



HAL
open science

L'usage de la donnée médicale : Contribution à l'étude du droit des données

Agathe Voillemet

► **To cite this version:**

Agathe Voillemet. L'usage de la donnée médicale : Contribution à l'étude du droit des données. Droit. Université Polytechnique Hauts-de-France, 2022. Français. NNT : 2022UPHF0011 . tel-03696956

HAL Id: tel-03696956

<https://theses.hal.science/tel-03696956>

Submitted on 16 Jun 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THESE DE DOCTORAT
délivrée par l'UNIVERSITE POLYTECHNIQUE HAUTS-DE-FRANCE
et l'INSA HAUTS-DE-FRANCE

Pour obtenir le grade de Docteur en Droit
Présentée et soutenue publiquement par
Agathe VOILLEMET
Le 10 mars 2022 à Lille.

Ecole doctorale :

École Doctorale Polytechnique Hauts-de-France (ED PHF).

Unités de recherche :

Laboratoire de Recherche Sociétés & Humanités (LARSH).

Centre de recherche sur les relations entre le risque et le droit (C3RD).

L'USAGE DE LA DONNEE MEDICALE.
CONTRIBUTION A L'ETUDE DU DROIT DES DONNEES.

JURY

Co-directeurs de thèse :

Monsieur Julien ICARD, Professeur des universités, Université Paris II Panthéon-Assas.

Madame Lina WILLIATTE-PELLITTERI, Professeur des universités, Université Catholique de Lille.

Membres du jury :

Madame Lucie CLUZEL-METAYER, Professeur des universités, Université Paris Nanterre, Présidente du jury.

Monsieur Thibault DOUVILLE, Professeur des universités, Université de Caen Normandie, Rapporteur.

Madame Johanne SAISON-DEMARS, Professeur des universités, Université de Lille, Examineur.

Monsieur François VIALLA, Professeur des universités, Université de Montpellier, Rapporteur.

Remerciements

Plus qu'un exercice académique, la thèse de doctorat est une épreuve de vie sans nul autre pareil. Mes pensées vont aux personnes qui m'ont accompagnée et soutenue, à un instant, ou tout au long de ce chemin téméraire.

Mes remerciements sont d'abord adressés à mes co-directeurs de thèse. Ma profonde reconnaissance est témoignée à Lina Williatte-Pellitteri qui, à mes yeux, incarne bien d'autres qualités que celle de directrice de ma thèse. Je la remercie de m'avoir donné l'ambition d'entreprendre ces travaux, d'en avoir assuré la responsabilité, et de m'avoir confortée dans cette voie académique. Ce fût un véritable enchantement d'évoluer à ses côtés, tant sur le plan humain que sur le plan scientifique. Ma gratitude va tout autant à Julien Icard qui m'a fait l'honneur de m'accorder sa confiance en m'offrant l'opportunité de m'engager vers la recherche en sciences juridiques. Je lui sais gré de sa disponibilité et de ses précieux conseils bienveillants et avisés.

Mes remerciements se dirigent ensuite vers les membres du jury qui m'accordent le privilège de leur considération et de leur présence. C'est avec la plus grande distinction que je remercie les professeurs Lucie Cluzel-Metayer, Thibault Douville, Johanne Saison-Demars et François Vialla d'avoir accepté de juger ces travaux.

Après, je tiens à exprimer mon attachement aux professionnels du Centre hospitalier de Valenciennes ainsi qu'à leurs partenaires. Ce fût un réel enrichissement de contribuer, à leurs côtés, au développement du virage numérique en santé et de l'innovation à partir de l'exploitation des données médicales des patients. L'application pratique de la théorie juridique et nos regards croisés ont amplement alimenté les réflexions que j'ai menées dans le cadre de ces travaux de thèse. Et je les remercie grandement pour cela.

Du fond du cœur, je remercie finalement mes proches d'avoir cru en moi comme personne. Par vos encouragements sans faille, votre aide logistique ou votre implication intellectuelle, vous m'avez procuré les moyens et la force nécessaires pour mener ce travail à terme.

Sommaire

PREMIERE PARTIE : LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AU PROFIT DE SA PRISE EN CHARGE SANITAIRE47

TITRE 1 : LA FORMALISATION DES DONNEES MEDICALES AU SEIN DES DOSSIERS MEDICAUX DU PATIENT 49

Chapitre 1 : Les contours des données personnelles colligées dans les dossiers médicaux du patient..... 53

Chapitre 2 : La limitation des droits du patient sur les données personnelles colligées dans ses dossiers médicaux 97

TITRE 2 : LA COMMUNICATION DES DONNEES MEDICALES FORMALISEES DANS LES DOSSIERS MEDICAUX DU PATIENT 155

Chapitre 1 : L'accès du patient aux données médicales générées lors de sa prise en charge sanitaire 157

Chapitre 2 : L'accès des professionnels aux données médicales du patient 207

DEUXIEME PARTIE : LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AU BENEFICE DE LA COLLECTIVITE 283

TITRE 1 : LA DETERMINATION DU STATUT ET DU REGIME APPLICABLES A LA DONNEE MEDICALE 285

Chapitre 1 : L'extrapatrimonialité de la donnée médicale 287

Chapitre 2 : La valorisation économique du traitement de la donnée médicale extrapatrimoniale 343

TITRE 2 : LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AUX FINS D'INTERET PUBLIC DANS LE DOMAINE DE LA SANTE : LA RECHERCHE, L'INNOVATION ET LA SANTE PUBLIQUE..... 403

Chapitre 1 : La requalification des données médicales en données de recherche 405

Chapitre 2 : La lutte contre les menaces sanitaires par la datasurveillance 477

Principales abréviations

AIPD	Analyse d'impact sur la protection des données
AJDA	Actualité juridique Droit administratif
ALD	Affection longue durée
ANAES	Agence nationale d'accréditation et d'évaluation en santé
ANS	Agence du numérique en santé
ARS	Agence régional de santé
ASAP	Loi n°2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique
Ass. plén.	Assemblée plénière de la Cour de cassation
CA	Cour d'appel
CAA	Cour administrative d'appel
CADA	Commission d'accès aux documents administratifs
CCC	Revue Contrats Concurrence Consommation
CCE	Revue Communication Commerce électronique
Cons.	Considérant
Cons. Const.	Conseil constitutionnel
CCNE	Comité consultatif national d'éthique
CDFUE	Charte des droits fondamentaux de l'Union européenne
CDHP	Commission départementale des hospitalisations psychiatriques
CE	Conseil d'Etat
CEDH	Cour européenne des droits de l'homme
CEPD	Contrôleur européen de la protection des données

CESREES	Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé
chron.	Chronique
Cf.	Se reporter à
CI-SIS	Cadre d'interopérabilité des Systèmes d'information de Santé
Civ.	Chambre civile de la Cour de cassation
CJUE	Cour de justice de l'Union européenne
CNCDH	Commission nationale consultative des droits de l'homme
CNIL	Commission nationale de l'informatique et des libertés
CNAM	Caisse nationale d'assurance maladie
CNNum	Conseil national du numérique
CNOM	Conseil national de l'Ordre des médecins
CNPEN	Comité national pilote d'éthique du numérique
CNRTL	Centre national de ressources textuelles et lexicales
CPAM	Caisse primaire d'assurance maladie
CPP	Comité de protection des personnes
Crim.	Chambre criminelle de la Cour de cassation
D.	Recueil Dalloz
DC	Commission départementale des hospitalisations psychiatriques
DGOS	Direction générale de l'offre de soins
DMP	Dossier médical partagé
ed.	Edition
ENS	Espace numérique de santé
et al.	Et autres
Gd. Ch.	Grande chambre

G29	Groupe de travail de l'article 29 de la directive n° 95/46/CE sur la protection des données
HAS	Haute autorité de santé
Ibid.	Dans le même passage du même ouvrage.
In	Dans
Infra	Ci-dessous
INSERM	Institut national de la santé et de la recherche médicale
JCP A	La Semaine Juridique Administrations et Collectivités territoriales
JCP G	La Semaine Juridique Édition Générale
JDSAM	Journal de droit de la santé et de l'assurance maladie
JORF	Journal officiel de la République française
JOUE	Journal officiel de l'Union européenne
LEPI	L'Essentiel Droit de la propriété intellectuelle
Loc. cit.	Dans l'ouvrage cité, à la même page
LPA	Les petites affiches
MERRI	Missions d'enseignement, de recherche, de référence et d'innovation
MR-004	Méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé
MSS	Messagerie sécurisée de santé
n°	Numéro
NIR	Numéro d'inscription au répertoire national d'identification des personnes physiques
Op. cit.	Dans l'ouvrage cité

p.	Page
RSC	Revue de science criminelle et de droit pénal comparé
RDS	Revue Droit & Santé
RDSS	Revue de droit sanitaire et social
RDT civ.	Revue trimestrielle de droit civil
RTD com.	Revue trimestrielle de droit commercial et de droit économique
Req.	Chambre des requêtes, Cour de cassation
RGDM	Revue générale de droit médical
RGPD	Règlement général sur la protection des données
RLDI	Revue Lamy droit de l'immatériel
s.	Suivant
SIGAPS	Système d'interrogation, de gestion et d'analyses des publications scientifiques
SNDS	Système national des données de santé
Supra	Ci-dessus
TA	Tribunal administratif
TIC	Technologies de l'information et de la communication
Vol.	Volume
VSM	Volet de synthèse médicale du dossier médical partagé

INTRODUCTION GENERALE

« *La matière médicale fait partie des grandes causes justifiant un régime particulier pour le droit sur les données personnelles.* »¹.

1. Aussi surprenant que cela puisse paraître, l'usage de la donnée médicale est une réalité amorcée dès l'Antiquité et développée au Moyen-Âge. Hippocrate, Galien, Avicenne ou encore Averroès consignaient, au sein de l'observation médicale², les particularités physiologiques qu'ils relevaient lors de l'auscultation du malade. En ces périodes historiques, ces médecins philosophes traitaient manuellement les informations médicales du patient à l'aide de fichiers manuscrits. Les premiers dossiers médicaux étaient ainsi constitués. Ce travail de formalisation des données médicales du patient a participé à la métamorphose de la médecine. Jusqu'à l'apogée de la Grèce Antique, la médecine du Paléolithique, du Mésolithique voire du Néolithique n'était fondée que sur le mysticisme. La maladie était imputée aux esprits malfaisants. Seuls des guérisseurs, élus par les divinités, détenaient le pouvoir de libérer les souffrances. Ces thaumaturges ne s'adressaient qu'à l'esprit du malade dans l'espoir de le délivrer des forces maléfiques³. A compter du IV^{ème} siècle avant Jésus-Christ, la croyance médicale a laissé place à la science médicale établie sur la pratique et l'expérimentation cliniques. La mise en données du corps humain a alors permis de soigner à l'appui d'informations biologiques probantes et de partager les connaissances médicales à des fins d'enseignement et de recherche⁴. C'est ainsi que « *la médecine antique a façonné la médecine occidentale, qu'elle a dégagée de la magie pour la faire entrer dans une perspective scientifique* »⁵. Depuis, le traitement de la donnée médicale est consubstantiel à la délivrance d'actes de prévention, de diagnostic ou de soins ainsi qu'aux progrès médicaux.

¹ SAINT PAU (J.-C.), *Droits de la personnalité*, LexisNexis, 2013, p. 632.

² L'observation médicale est document de travail rédigé par le médecin. Ce document comporte les informations recueillies lors des différentes étapes de la consultation : l'anamnèse et l'examen clinique constitué de l'inspection, de la palpation, de la percussion et de l'auscultation.

³ Encyclopédie Larousse, *Histoire de la médecine*. Disponible en ligne sur le site [www.larousse.fr]. Consulté le 11 avril 2022.

⁴ ZORN-MACREZ (C.), *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, Presses universitaires de Nancy, 2010, p. 22.

⁵ LECA (A.), LUNEL (A.), SANCHEZ (S.), *Histoire du droit de la santé*, LEH, 2014, p. 21.

L'usage de la donnée médicale est donc observé comme un fait ancestral au fondement de l'Art – scientifique et technique – médical⁶.

2. Alors que la mise en données du corps humain précède de loin l'informatique, l'avènement de l'ère numérique a bouleversé les capacités d'exploitation de la donnée médicale du patient. D'une part, l'informatisation des dossiers médicaux favorise la production, à chaque seconde, d'un volume considérable d'informations intimes. D'autre part, les outils numériques permettent l'analyse de ces mégadonnées dont la massivité est mise au service du malade et, plus généralement, de la science et de la santé publique. Si la donnée médicale demeure l'outil essentiel à la prise en charge sanitaire du patient, elle constitue désormais le socle sur lequel repose le système de santé dans son ensemble⁷. Certainement, la viabilité de la société numérique⁸, qui intègre inévitablement le domaine de la santé, dépend du traitement des données personnelles des individus, et donc des données médicales du patient. Fortement impacté par la révolution numérique, le domaine de la santé connaît actuellement une mutation à laquelle il ne peut échapper⁹.

3. Le système de santé traditionnel se transforme activement en un système numérisé qui suscite autant de méfiance que d'espérance. Cette évolution, engendrée par l'apparition de nouveaux outils technologiques, est à l'origine de la *santé numérique*. Cette notion, relativement moderne, englobe « *tous les domaines où les technologies de l'information et de la communication sont mises au service de la santé* »¹⁰. Plus connues sous l'acronyme « TIC », ces technologies renvoient aux télématiques. Elles sont des outils de support qui permettent le traitement et la transmission des données au moyen de l'électronique et du

⁶ VIALLA (F.), *Non progredi est regredi ?*, In BROSSET (E.), GAMBARDELLA (S.), NICOLAS (G.), *La santé connectée et « son » droit : approches de droit européen et de droit français*, Presses Universitaires d'Aix-Marseille, 2017, p. 49.

⁷ MOUNCIF-MOUNGACHE (M.), *La place de la santé dans le règlement sur les données personnelles*, In ESPESSON-VERGEAT (B.), *Innovation juridique et transversalité des politiques liées au numérique, à la santé et aux territoires*, Actes du colloque organisé le 28 septembre 2017 à la Faculté de droit de Saint-Etienne, LEH, 2018p. 85 à p. 93.

⁸ Voir : COMPIEGNE (I.), *La société numérique en question(s)*, Editions Sciences Humaines, 2010.

⁹ ESPESSON-VERGEAT (B.), *Quel regard en droit européen sur l'innovation juridique en matière de santé ?*, In ESPESSON-VERGEAT (B.), *Innovation juridique et transversalité des politiques liées au numérique, à la santé et aux territoires*, op. cit., p. 113.

¹⁰ SAFON (M.-O.), *La e-santé. Télésanté, santé numérique ou santé connecté*, Synthèses & Bibliographies, Institut de recherche et de documentation en économie de la santé, octobre 2021.

numérique¹¹. Le champ de la santé numérique concerne donc l'ensemble des services sanitaires qui implique un traitement automatisé de données. Le traitement d'une information est une notion considérablement large définie à l'article 4.2 du Règlement général sur la protection des données¹² (RGPD). Sous ce terme, le législateur européen inclue toute opération informatique ou manuscrite effectuée sur une donnée à caractère personnel. Il peut notamment s'agir de leur collecte, de leur structuration, de leur conservation, de leur consultation, de leur utilisation, de leur communication, de leur modification, de leur interconnexion ou encore de leur destruction. Si l'on s'en tient à cette définition, la santé numérique intègre toute activité qui suppose une action effectuée sur des données personnelles à l'aide des technologies numériques. Concrètement, elle comprend tant les dossiers de santé électroniques, que la télésanté ou l'aide à la décision médicale.

4. A l'aune de ces définitions, nous pouvons affirmer que le système de santé numérisé repose exclusivement sur le traitement automatisé des données sanitaires. Plus spécifiquement, le numérique en santé repose indispensablement sur une ressource essentielle : la donnée médicale. L'usage étant défini comme le fait de se servir de quelque chose afin de satisfaire un besoin¹³, nous pouvons affirmer que les opportunités qu'offre le numérique en santé dépendent essentiellement de l'usage des informations médicales du patient.

En premier lieu, les bénéfices du virage numérique en santé profitent personnellement au patient. D'une part, le traitement de ses données médicales, au moyen des TIC, permet de pratiquer une médecine devenue préventive, prédictive, participative, personnalisée, pertinente et de parcours¹⁴. Les actes sanitaires sont prodigués en présentiel ou en distanciel, en amont de la maladie et de façon ciblée en considération des caractéristiques propres au patient. D'autre part, la circulation de la donnée médicale, au moyen des télécommunications, facilite la dispensation des services de soins de santé dans le cadre d'un parcours interactif,

¹¹ Définition proposée par le dictionnaire de la bibliothèque numérique de droit de la santé et d'éthique médicale.

¹² Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JOUE* L 119/1, 4 mai 2016.

¹³ Définition du substantif « usage » proposé par le Centre nationale de ressources textuelles et lexicales (CNRTL). Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 05 janvier 2022.

¹⁴ Dite médecine des « 6P ».

coordonné et incluant à la fois le patient et l'ensemble des professionnels impliqués. La qualité et l'efficacité des soins réalisés en sont améliorées. A l'heure de la science et de la médecine des données, la donnée médicale constitue l'infrastructure du soin¹⁵.

En second lieu, cette évolution disruptive bénéficie à la collectivité. Le développement des technologies permet le traitement informatique des mégadonnées médicales nécessaires à l'accélération de la recherche et de l'innovation en santé. Il devient alors possible de déployer et d'entraîner des solutions numériques en santé, de promouvoir, d'identifier et d'anticiper la gestion des risques sanitaires, ou encore d'élaborer des politiques de santé pertinentes. L'usage de la donnée médicale du patient présente donc des enjeux considérables, pour l'avenir de la Santé, dans l'intérêt particulier du patient ainsi que dans l'intérêt général de la communauté. Il en ressort que les données médicales « *sont le matériau de recherche de base pour les scientifiques [...] C'est pourquoi leur exploitation représente une opportunité de première importance* »¹⁶.

5. Compte tenu de ce qui précède, la dématérialisation de la donnée médicale facilite son accessibilité et son usage simultanés par une multitude d'acteurs concourant à la santé individuelle du patient comme à la santé collective de la population. La donnée médicale, intimement personnelle au patient, comporte donc une dimension collective pour la préservation de la santé de tous et de chacun. Si la donnée médicale du patient se cristallisait au sein du colloque singulier, l'efficacité d'une médecine de parcours globalisé en serait affectée et le progrès de la science médicale resterait figé.

Toutefois, le colloque singulier, consacré par le célèbre médecin Georges Duhamel¹⁷, constitue le sacerdoce de la relation médicale. Henri Péquignot y voyait « *une espèce de duo qui ne comporte dans le silence du cabinet que deux personnages : le médecin et le malade* »¹⁸. Ce Professeur de médecine exposait ainsi la nature bilatérale et confidentielle de

¹⁵ Voir : BERANGER (J.), BOUADI (R.), *Approche éthico-juridique de l'usage des données médicales à caractère personnel*, Les Cahiers du numérique, vol. 10, 2014, n°02, p. 94.

¹⁶ 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.

¹⁷ DUHAMEL (G.), *Les excès de l'étatisme et les responsabilités de la médecine*, Revue des Deux Mondes, 1934, n°02, p. 277 à p. 299 ; DUHAMEL (G.), *Paroles de médecin*, Du Rocher Monaco, 1946.

¹⁸ PÉQUIGNOT (H.), *Médecine et mode moderne : l'écran des techniques entre le médecin et le malade*, Paris, Les éditions de minuit, 1953, p. 7.

la relation entre le professionnel de santé et le patient. L'illustration la plus significative de cet axiome revient à Louis Portes. Il considérait que « *tout acte médical normal n'est, ne peut être, ne doit être qu'une confiance qui rejoint librement une conscience* »¹⁹. Néanmoins, il est primordial de noter qu' « *il n'y a pas de médecine sans confiance, de confiance sans confiance et de confiance sans secret* »²⁰. La relation médicale se concrétise donc par la rencontre d'une confiance et d'une conscience marquée sous le sceau du secret. Dès lors, toute donnée médicale générée dans le cadre du colloque singulier devient secrète. Bruno Py ne manque pas de rappeler que « *tout secret est, par nature, un obstacle à la libre circulation de l'information* »²¹. En conséquence, les données médicales du patient produites par un professionnel de santé ne peuvent, par principe, sortir du cadre de la relation sanitaire.

Cependant, les informations médicales *confiées* au professionnel de santé perdent leur caractère *secret* dès l'instant où il devient impossible d'identifier directement le patient auxquelles elles se rapportent. La pseudonymisation²² comme l'anonymisation²³ des données médicales du patient promeuvent alors leur diffusion par delà le colloque singulier. Partant, le traitement de la donnée médicale a pour effet de faire « *basculer le statut de l'information d'une relation interindividuelle ou intersubjective [...] en une relation collective, sociale, par défaut* »²⁴. Si la transformation du système de santé vers le numérique en santé bouleverse évidemment les fondements de la pratique médicale²⁵, cette évolution a particulièrement modifié le rapport que le patient entretient avec sa *donnée médicale à caractère personnel* et, consécutivement, les droits fondamentaux dont il dispose à son égard.

¹⁹ PORTES (L.), *À la recherche d'une éthique médicale*, Paris, Masson & Cie, 1964, p. 163.

²⁰ *Op. cit.* p. 131.

²¹ PY (B.), *Secret professionnel*, In VIALLA (F.) *Les grandes décisions du droit médical*, LGDJ, 2^e ed. 2014, p. 305.

²² L'article 4.5 du RGPD définit la pseudonymisation 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, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

²³ Cf. Paragraphe 366.

²⁴ LE REUN (R.), *Les métamorphoses numériques de l'hôpital. Le soignant et l'information sans papiers*, Ethique et santé, 2019, n°16, p. 45.

²⁵ LUCAS (J.), *Quelle déontologie pour les médecins à l'heure du numérique ?*, In POIROT-MAZÈRES (I.), *Santé, numérique et droit-s*, Presses de l'Université Toulouse 1 Capitole, 2018, p. 167 à p. 175.

6. La donnée médicale personnelle est devenue une source d'information particulière dont l'exploitation est impérieusement nécessaire pour la prise en charge sanitaire du patient, pour l'amélioration de la santé publique et, *in fine*, pour la croissance économique du secteur de la santé. Alors que le patient est perçu comme l'unique source de données médicales, il se trouve dépossédé de sa chose intime (**Paragraphe 2**). Il existe donc des points perpétuels de tension entre l'autodétermination informationnelle du patient envers sa donnée médicale, l'incontournable utilité de cet instrument sanitaire par-delà le colloque singulier, et le nécessaire renforcement de la protection de cet élément immatériel et confidentiel issu du corps humain (**Paragraphe 3**). Pourtant, la donnée médicale ne bénéficie d'aucun encadrement juridique permettant de considérer ses spécificités, ses enjeux, et les risques inhérents à sa création comme à son usage. Pour l'heure, seul le droit à la protection des données personnelles, articulé avec le droit des personnes malades²⁶, permet d'encadrer le traitement générique des données concernant la santé. Seulement, la conciliation de ces régimes juridiques est un exercice qui se révèle aussi complexe qu'incertain. Il en advient que le cadre juridique entourant l'usage des données médicales apparaît véritablement obscur²⁷ (**Paragraphe 1**).

7. Néanmoins, il est utile de préciser que, ces dernières années, des thèses de doctorat ont apporté des éclairages particuliers sur le droit à la protection des données à caractère personnel. Certains auteurs se sont attachés à démontrer que la finalité de ce droit ne se réduisait pas à la protection des données personnelles, mais à leur libre circulation dans les limites d'une police administrative spéciale²⁸. D'autres ont exploré la protection des données personnelles à travers leur qualification²⁹, la fondamentalisation de ce droit³⁰, ou encore

²⁶ Tels qu'initiés par la loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF*, 5 mars 2002, texte n° 1.

²⁷ BERANGER (J.), BOUADI (R.), *op. cit.*, p. 93 ; BENSAMOUN (A.), *Le règlement général sur la protection des données : aspects institutionnels et matériels*, Mare & Martin, 2020.

²⁸ OCHOA (N.), *Le droit des données personnelles : une police administrative spéciale*, Catherine TEITGEN-COLLY (dir.), Thèse de Doctorat, Droit, Université Paris I, 2014.

²⁹ LESAULNIER (F.), *L'information nominative*, Pierre CATALA (dir.), Thèse de Doctorat, Droit, Université Paris II, 2005 ; EYNARD (J.), *Les données personnelles, quelle définition pour un régime de protection efficace ?*, Michalon, 2013 ; ALLIOT (S.), *Essai de qualification de la notion de données à caractère personnel*, Nathalie MARTIAL-BRAZ (dir.), Thèse de Doctorat, Droit, Université de Franche-Comté, 2018.

³⁰ DEBAETS (E.), *Le droit à la protection des données à caractère personnel. Recherche sur un droit fondamental*, Bertrand MATHIEU (dir.), Thèse de Doctorat, Droit, Université Paris I, 2014 ; CHAMBARDON (N.), *L'identité numérique de la personne humaine : contribution à l'étude du droit fondamental à la protection des données à caractères personnel*, Édith JAILLARDON (dir.), Thèse de Doctorat, Droit, Université Lyon II,

l'effectivité et l'efficience de la matière³¹. Par ailleurs, quelques auteurs ont examiné l'impact des nouvelles technologies de l'information et de la communication sur la protection des données personnelles³². De façon spécifique, des thèses de Doctorat ont porté sur les données personnelles concernant la santé. Alors que certains auteurs ont axé leurs travaux sur la réutilisation des mégadonnées de santé³³, d'autres ont préféré se concentrer sur leur circulation dans le cadre de la pratique médicale³⁴. En outre, quelques contributeurs se sont interrogés sur la brûlante question de leur propriété³⁵.

Malgré ces analyses approfondies, aucun travail ne paraît livrer un éclairage sur les particularités de la donnée médicale, et moins encore sur la portée de ses usages. Le constat d'une carence textuelle et jurisprudentielle justifie alors une étude théorique prospective. Ainsi, les présents travaux ont pour objet de démontrer l'incomplétude du droit positif aux particularités de la donnée médicale et prétendent à concevoir un cadre juridique qui lui serait dédié. Pendant que la sacralisation de la donnée médicale affirmerait sa sauvegarde, son usage serait également favorisé par la redéfinition des prérogatives et des obligations que le patient disposerait à son égard.

2018 ; KOUMPLI (C.), *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, Otto PFERSMANN (dir.), Thèse de Doctorat, Droit, Université Paris I, 2019.

³¹ VERGNOLLE (S.), *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, Jérôme PASSA (dir.), Thèse de Doctorat, Droit, Université Paris II, 2020.

³² LE CLAINCHE (J.), *L'adaptation du droit des données à caractère personnel aux communications électroniques*, Jean FRAYSSINET (dir.), Thèse de Doctorat, Droit, Université Montpellier I, 2008 ; LANNA (M.), *La protection des données à caractère personnel à l'épreuve de l'automesure connectée*, Camille BROUELLE, Lucie CLUZEL-METAYER (dir.), Thèse de Doctorat, Droit, Université Paris II, 2019.

³³ GUITTET (L.), *La transparence des données issues des bases médico-administratives. Pour une ouverture des bases de données respectueuse de la vie privée*, Guillaume ROUSSET (dir.), Thèse de Doctorat, Droit, Université Lyon III, 2019 ; LUTUN (A.), *Le Bigdata en santé, richesse et conditions d'accès*, Anne DEBET (dir.), Thèse de Doctorat, Droit, Université Paris V, 2021.

³⁴ ZORN-MACREZ (C.), *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, Presses universitaires de Nancy, 2010 ; BRASSELET (R.), *La circulation de la donnée à caractère personnel relative à la santé*, Bruno PY (dir.), Thèse de doctorat, Droit, Université de Lorraine, 2018 ; OLECH (V.), *Le secret médical et les technologies de l'information et de la communication*, Bruno PY (dir.), Thèse de doctorat, Droit, Université de Lorraine, 2019.

³⁵ CAVALIER (M.), *La propriété des données de santé*, Marion GIRER (dir.), Thèse de Doctorat, Droit, Université Lyon III, 2016.

Paragraphe 1 : L'absence de protection juridique spécifique à la donnée médicale

8. L'objet de cet étude porte sur les *données médicales*. Seulement, cette espèce particulière de données ne bénéficie d'aucune reconnaissance juridique. En l'état actuel du droit positif, la donnée médicale personnelle est catégorisée parmi les données personnelles concernant la santé. Par conséquent, le régime juridique applicable aux données personnelles de santé s'applique, par défaut, aux données médicales personnelles (**B**). Bien que cette classification ne soit pas erronée, elle paraît insuffisamment assortie à cette sous-catégorie de données personnelles relatives au patient. Avant de concevoir un encadrement juridique adéquat aux particularités de la donnée médicale, il apparaît essentiel de lui offrir une définition fidèle à ses caractéristiques (**A**).

A) Les caractéristiques de la donnée médicale personnelle

9. La donnée médicale pourrait simplement être assimilée aux informations concernant la santé des individus. Toutefois, cette conception ne permet pas d'en considérer la singularité. Il nous revient alors la tâche de déterminer l'objet de la présente thèse en lui consacrant une acception ainsi qu'une signification distinctive.

10. En premier lieu, la donnée médicale constitue une *donnée à caractère personnel* lorsqu'elle se réfère au patient duquel elle émane. Par définition, une donnée à caractère personnel concerne toute information se rapportant à une personne physique identifiée ou identifiable, dénommée *personne concernée*³⁶. Une personne concernée par une information peut être identifiée directement, notamment par ses noms et prénoms ; ou indirectement par référence à un identifiant, à un pseudonyme ou à des éléments propres à son identité qui la rendent identifiable³⁷. Autrement dit, une donnée est à *caractère personnel* lorsqu'elle révèle des renseignements attachés à un individu. Les substantifs féminins *donnée* et *information* étant entendus comme des synonymes par le législateur européen, une donnée médicale est donc une information personnelle au patient lorsqu'elle lui est rattachée de quelque façon

³⁶ Article 4.1 du RGPD.

³⁷ Article 4.1 du RGPD ; DE TERWANGNE (C.), *Définitions clés et champ d'application du RGPD*, In DE TERWANGNE (C.) et ROSIER (K.), *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie*, Larcier, 2018, p. 61.

que ce soit. Bien que certains auteurs considèrent que la donnée se distingue de l'information par la transformation qu'elle subit pour être traitée informatiquement³⁸, les termes *information* et *donnée* seront indistinctement employés tout au long de ces travaux.

11. En revanche, il est fondamental de distinguer les données médicales *personnelles* des données médicales *anonymes*. Alors que toute donnée médicale *nominative* ou *pseudonymisée* est considérée comme à *caractère personnel* en ce qu'elle permet de caractériser la personne concernée, une donnée médicale *anonyme* ne permet irréversiblement l'identification du patient qui en est à l'origine. Dans cette dernière hypothèse, il n'y a « *pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes* »³⁹. A travers la protection des données personnelles, le Droit s'attache à protéger la personne concernée par le traitement de ses informations. Lorsque les données ne se rapportent à aucun individu, il n'y a donc aucune personne physique à préserver. A l'inverse, les données médicales concernant un patient identifié ou identifiable sont soumises au droit à la protection des données personnelles.

12. Parmi les données à caractère personnel, les informations observées comme *neutres* ont rapidement été opposées aux informations appréciées comme *sensibles*. Avant l'adoption de la première loi Informatique et Libertés du 6 janvier 1978⁴⁰, différentes catégories de données personnelles étaient déjà distinguées selon leur nature, leur sensibilité et les risques que leur traitement pouvait engendrer pour les libertés et les droits fondamentaux de la personne concernée. En effet, la Commission informatique et libertés, créée à la demande du Premier ministre Pierre Messmer⁴¹ à la suite de la polémique relative au projet « S.A.F.A.R.I »⁴², a différencié les données à caractère personnel selon leur degré d'intimité. Alors chargée de proposer au Gouvernement des mesures visant à garantir que l'informatique et le traitement des fichiers à caractère personnel se développeraient dans le respect de la vie

³⁸ DE LAMBERTERIE (I.), *Qu'est ce qu'une donnée de santé ?*, In *Le droit des données de santé*, Actes du colloque de l'Association française de droit de la santé organisé à Paris le 25 mars 2004, RGDM, 2004, n°04, p. 13.

³⁹ Considérant 26 du RGPD.

⁴⁰ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, 7 janvier 1978.

⁴¹ Décret n°74-938 du 8 novembre 1974 portant création de la commission informatique et libertés, *JORF*, 13 novembre 1974.

⁴² Voir : le site [www.senat.fr/evenement/archives/D45/context.html]. Consulté le 27 novembre 2021.

privée, des libertés individuelles et des libertés publiques, cette Commission proposait de soumettre ces traitements à des principes généraux applicables en fonction de la nature des données traitées. Parmi ces règles, elle suggérait d'interdire l'enregistrement de certaines données examinées comme sensibles afin de protéger la vie privée et l'intimité des individus contre toute forme de discrimination⁴³. C'est alors que les *données de santé* ont été progressivement additionnées à la liste des données de nature sensible⁴⁴ avant que leur définition ne soit consacrée, en 2016, par le législateur européen.

13. Selon l'article 4.15 du RGPD, les données concernant la santé correspondent aux « *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* ». Concrètement, le trente-cinquième considérant de ce règlement explique que sont des données de santé celles « *qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée* ». L'étendue de cette définition permet d'englober toute information personnelle relative à un état de santé nonobstant la source dont elle provient et le contexte de sa génération. Ainsi, des données indiquant le poids et la taille d'une personne, ses performances physiques et intellectuelles ou la qualité de son sommeil, collectées à partir d'objets connectés de bien-être, peuvent être qualifiées de données de santé lorsqu'elles révèlent, à elles seules ou en étant croisées avec d'autres données, des informations relatives à la santé de l'intéressé⁴⁵. Également, doit être considérée comme une donnée de santé, l'unique information portant sur un handicap, sur l'inscription en vue de bénéficier des services de soins de santé ou encore sur l'identifiant national de santé. La définition de la donnée de santé par le RGPD élargit « *sensiblement la définition de donnée concernant la santé puisqu'elle se réfère à une*

⁴³ Rapport de la commission informatique et liberté, rédigé par Bernard Tricot, 27 juin 1975, La documentation française, p. 47.

⁴⁴ En particulier par l'article 9 de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOUE* n° L 281, 23 novembre 1995 ; et par l'article 2 de la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n°182, 7 août 2004, texte n° 2.

⁴⁵ LANNA (M.), *La protection des données à caractère personnel à l'épreuve de l'automesure connectée*, Camille BROUELLE, Lucie CLUZEL-METAYER (dir.), Thèse de Doctorat, Droit, Université Paris II, 2019, p. 131.

« *personne* » et non à un « *patient* » »⁴⁶. Par surcroît, cette définition étend son « *spectre aux données du corps humain dans son ensemble et non aux activités prévues dans le domaine médical* »⁴⁷.

14. Alors que la catégorie des données concernant la santé apparaît considérablement vaste, elle comporte des sous-catégories de données sensibles telles que les données génétiques⁴⁸, les données biométriques⁴⁹ ainsi que les données médicales. En second lieu, les données médicales correspondent donc à des données sensibles concernant la santé. En revanche, toute donnée concernant la santé ne constitue pas nécessairement une donnée médicale⁵⁰. Ainsi que le constate Thibault Douville, « *la notion de données concernant la santé se distingue de la notion de données de santé au sens du Code de la santé publique, qui désigne les données relatives à la prise en charge d'un patient par un professionnel ou un établissement de santé, la première étant une catégorie englobant la seconde* »⁵¹. Les données de santé entretiennent donc, avec les données médicales, un rapport de genre à espèce. Bien que les données médicales constituent une sous-catégorie de données de santé, elles méritent indéniablement une analyse spécifique en raison de leur nature particulière.

15. Certes, les données médicales sont vaguement considérées au premier alinéa de l'article L.1111-7 du code de la santé publique⁵². Néanmoins, ni le droit européen, ni le droit national ne leur concèdent une définition juridique assortie d'un statut *ad hoc*. Pourtant, les données médicales correspondent spécifiquement aux conditions biologiques, physiques et psychiques d'une personne humaine recueillies et produites par un professionnel de santé à l'occasion de la dispensation d'un acte sanitaire. Il en advient que la donnée médicale correspond à un élément immatériel, généré dans un contexte médical, par un professionnel de santé exceptionnellement autorisé à attenter à l'intégrité corporelle du patient sous réserve

⁴⁶ PAULIN (B.), *Trois conseils sur le traitement des données de santé*, In *Droit des données personnelles*, Dalloz, 1^{ère} ed., novembre 2019, p. 90.

⁴⁷ *Ibid.*

⁴⁸ Article 4.13 du RGPD.

⁴⁹ Article 4.14 du RGPD

⁵⁰ DE LAMBERTERIE (I.), *op. cit.*, p. 19.

⁵¹ DOUVILLE (T.), *Droit des données à caractère personnel*, Gualino, 2020, p. 81.

⁵² Ces dispositions encadrent le droit d'accès aux informations médicales du patient.

de son consentement⁵³. La donnée médicale ne peut donc émaner que d'un patient ; c'est-à-dire d'une *personne malade* relevant directement d'une prise en charge sanitaire⁵⁴. Etant donné que l'objet de cette étude porte sur les données médicales, le sujet en est logiquement le patient, en tant que personne concernée par le traitement de ses informations intimes.

En considération de ce qui précède, les données médicales peuvent être définies comme les *éléments immatériels du corps humain du patient*. S'il ne fait aucun doute que les données médicales révèlent l'état de santé du patient, elles comportent des particularités inhérentes aux modalités de leur production et aux informations qu'elles renferment. En conséquence, cette sous-catégorie de données apparaît supérieurement sensible à la catégorie des données de santé à laquelle elles appartiennent. De toute évidence, le patient entretient un lien singulier, personnel et profondément intime avec sa donnée médicale. Alors, si l'individu dispose sur son corps d'un droit naturel et souverain⁵⁵, le patient dispose-t-il d'une autonomie similaire à l'égard de l'usage de ses données médicales ?

B) L'application d'un régime de droit commun à une donnée médicale particulière

16. Après avoir eu l'opportunité de définir la notion de donnée médicale, il convient d'examiner les régimes juridiques qui lui sont applicables. Manifestement, aucune règle de droit n'encadre spécifiquement son traitement. Pour cause, la donnée médicale n'est encore assortie d'aucun statut juridique qui lui est propre. Par défaut, l'usage de la donnée médicale est encadré par le droit à la protection des données (1). Par ailleurs, la donnée médicale est également protégée par le droit au secret médical⁵⁶. Plus qu'une obligation de secret professionnel, il consacre un véritable droit à la confidentialité des éléments de la vie privée du patient (2).

⁵³ Article 16-3 du code civil.

⁵⁴ TABUTEAU (D.), DOMINIQUE (M.), *Les droits des personnes malades*, In BOURDILLON (F.), *Traité de santé publique*. Lavoisier, 2016, p. 148.

⁵⁵ EL RHRIB-LOUH (H.), *L'autonomie médicale des personnes en situation d'incapacité*, Françoise DEKEUWER-DEFOSSEZ (dir.), Thèse de doctorat, Droit, Université de Lille, juin 2012, p. 20.

⁵⁶ Article L.1110-4 du code de la santé publique.

1. L'application du droit à la protection des données personnelles

17. En l'état actuel du droit, les données médicales correspondent à des données concernant la santé. En l'absence de consécration juridique particulière, le régime applicable au traitement des données de santé encadre également le traitement des données médicales. Seulement, le régime dévolu aux données concernant la santé est prescrit par les dispositions de l'article 9 du RGPD, lesquelles organisent uniformément le traitement de toute donnée considérée comme *sensible*. Les données de santé – et implicitement les données médicales – ne sont donc envisagées « *qu'à travers le régime général dérogatoire prévu pour les données sensibles* »⁵⁷. Afin de leur garantir une protection ultime, ce règlement européen affirme le principe d'interdiction de traitement des données sensibles⁵⁸. Par principe, le traitement des données de santé – ainsi que des données médicales – est donc interdit.

A titre dérogatoire, le législateur européen autorise néanmoins leur usage lorsque le traitement poursuit l'une des dix finalités énumérées à l'article 9.2 du RGPD. Ainsi, l'utilisation d'une donnée sensible est permise lorsqu'elle apparaît absolument nécessaire à l'accomplissement d'une finalité exceptionnellement autorisée par le législateur européen. Cette exigence permet de limiter l'ingérence dans l'intimité de la vie privée des personnes concernées. En effet, les données sensibles révèlent des informations protégées par le droit au respect de la vie privée institué à l'article 9 du code civil et à l'article 8 de la Convention européenne des droits de l'homme. Ce droit au respect de la vie privée est constitué de plusieurs composantes dont l'état civil, l'image, la vie familiale, amoureuse, spirituelle, les opinions, les correspondances, le patrimoine, le domicile ou encore l'état de santé. Par analogie, le champ des données sensibles, comprenant « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale* »⁵⁹, les données génétiques, les données biométriques, les données concernant la santé et les données concernant la vie ou l'orientation sexuelle, correspond aux éléments appartenant au champ de la vie privée. Le traitement des données sensibles peut donc

⁵⁷ MARTIAL-BRAZ (N.), *Données traitées – Données de santé*, In MARTIAL-BRAZ (N.), ROCHFELD (J.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, p. 91.

⁵⁸ Article 9.1 du RGPD.

⁵⁹ *Ibid.*

fortement attenter à l'intimité des personnes concernées, notamment lorsque ces informations fondent des décisions prises à leur encontre. Cependant, ces données sensibles ne peuvent pas être exclues de tout traitement. Dans l'hypothèse où la finalité de leur usage est indispensable pour les besoins énumérés à l'article 9.2 du RGPD, cette nécessité prévaudra sur le principe d'interdiction de leur traitement. C'est ainsi que le règlement européen concède le traitement des données de santé – et donc des données médicales – dans le cadre « *de la prise en charge sanitaire* »⁶⁰ de la personne concernée ou « *pour des motifs d'intérêt public dans le domaine de la santé publique* »⁶¹.

18. En complément du régime dérogatoire dédié aux données sensibles, l'entité qui désire mettre en œuvre un traitement de données à caractère personnel doit respecter les obligations de droit commun édictées par le RGPD. Ces règles communes de protection s'appliquent indistinctement à toute catégorie des données personnelles indépendamment de leur éventuelle sensibilité.

19. D'abord, tout traitement de données à caractère personnel ne peut être licitement mis en œuvre qu'à la condition d'être juridiquement fondé sur l'une des six *bases légales* exhaustivement et précisément énumérées à l'article 6 du RGPD. Egalement dénommée *fondement juridique*, une base légale correspond à une situation juridique inflexible permettant de justifier la licéité d'un traitement de données personnelles. En pratique, la détermination de la base légale « *d'un traitement de données est fait par le responsable de traitement* »⁶², c'est-à-dire l'entité publique ou morale qui détermine les finalités et les moyens du traitement⁶³. Au demeurant, le choix entre les six bases légales énoncées à l'article 6 du RGPD « *s'opère en particulier en fonction des finalités du traitement* »⁶⁴ et de ses spécificités. Il doit donc exister une concordance entre la finalité du traitement et son fondement juridique. Aussi, chaque finalité de traitement doit être juridiquement fondée sur une base légale appropriée. Lorsqu'un traitement de données personnelles poursuit plusieurs finalités, chacune de ces finalités doit alors reposer sur une base légale qui lui est propre.

⁶⁰ Article 9.2 h) du RGPD.

⁶¹ Article 9.2 i) du RGPD.

⁶² DOUVILLE (T.), *Droit des données à caractère personnel, op. cit.*, p. 111.

⁶³ Article 4.7 du RGPD.

⁶⁴ DOUVILLE (T.), *loc. cit.*

Compte tenu de ce qui précède, tout traitement de donnée personnelle concernant la santé peut être légalement autorisé aux conditions cumulatives qu'il soit fondé sur l'une des six bases légales prévues à l'article 6 du RGPD, et qu'il poursuive l'une des dix finalités dérogatoires de l'article 9.2 du RGPD. Bien qu'elles soient étroitement liées, il est donc important de distinguer les notions de *base légale* du traitement et de *finalité* du traitement. Les possibilités d'exploiter des données de santé – et des données médicales – paraissent donc limitées par ces deux obligations présentées comme des gardes fou garantissant la légitimité de leur traitement.

20. Ensuite, tout traitement de données personnelles doit être conforme aux principes généraux et essentiels qui gouvernent leur protection⁶⁵. C'est ainsi que les informations se rapportant à une personne concernée ne peuvent être traitées que « *de manière licite, loyale et transparente* »⁶⁶ à l'égard de la personne concernée. Leur traitement ne peut être mis en œuvre que pour « *des finalités déterminées, explicites et légitimes* »⁶⁷. Si les données personnelles collectées doivent être « *exactes* »⁶⁸, seules les informations « *adéquates, pertinentes et limitées à ce qui est nécessaire* »⁶⁹ à la finalité du traitement ne peuvent être utilisées. Afin de prévenir leur détournement, elles ne peuvent être conservées que pendant une durée n'excédant pas celle essentielle à l'accomplissement de l'objectif du traitement⁷⁰. En définitive, le responsable d'un traitement doit « *garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées* »⁷¹. L'ensemble de ces principes visent à encadrer toute utilisation de données à caractère personnel dans l'intention de leur assurer une sécurisation effective. En effet, tout responsable d'un traitement de données

⁶⁵ Article 5 du RGPD.

⁶⁶ Article 5.1 a) du RGPD.

⁶⁷ Article 5.1 b) du RGPD.

⁶⁸ Article 5.1 d) du RGPD.

⁶⁹ Article 5.1 c) du RGPD.

⁷⁰ Article 5.1 e) du RGPD.

⁷¹ Article 5.1 f) du RGPD.

personnelles doit respecter les obligations de protection des données personnelles et des personnes concernées dès sa conception et par défaut⁷².

21. Force est d'observer que le RGPD ne consacre aucun statut spécifique à aucune catégorie particulière de données sensibles. Effectivement, le législateur européen assure la sauvegarde des données à caractère personnel, neutres et sensibles, en déterminant les exigences juridiques auxquelles doivent satisfaire leurs usages. Si les données médicales étaient spécifiquement reconnues par le législateur européen, elles incorporeraient la liste des données considérées comme sensibles. Dès lors, elles seraient soumise au régime dérogatoire applicable aux données sensibles d'une part, et aux exigences générales de protection des données personnelles d'autre part. La consécration de la donnée médicale à l'échelle européenne n'emporterait donc aucune conséquence sur le niveau de protection qu'elles méritent particulièrement de recevoir.

22. La protection des données personnelles est principalement régie par le RGPD, entré en vigueur dans l'ordre juridique français le 25 mai 2018 sans qu'aucune transposition n'eut été nécessaire. Toutefois, le législateur européen a offert certaines marges de manœuvre aux États membres de l'Union européenne. Cette démarche de compromis était nécessaire pour « *emporter l'adhésion des Etats qui s'opposaient au choix du règlement uniforme comme outil normatif pour encadrer le droit de la protection des données à caractère personnel* »⁷³. Ces derniers sont donc autorisés à introduire des conditions ou des limitations supplémentaires aux règles de protection fixées par le RGPD⁷⁴, notamment en ce qui concerne le traitement des données sensibles⁷⁵. C'est ainsi que la loi Informatique et Libertés modifiée⁷⁶ a consacré une section spécifique aux « *traitements de données à caractère*

⁷² Article 25 du RGPD.

⁷³ MARTIAL-BRAZ (N.), *Présentation de la loi française et articulation des textes français et européens*, In MARTIAL-BRAZ (N.), ROCHFELD (J.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, p. 23.

⁷⁴ Considérant 10 du RGPD.

⁷⁵ Article 9.5 du RGPD.

⁷⁶ Telle que modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *JORF* n°288, 13 décembre 2018.

personnel dans le domaine de la santé »⁷⁷ composée de deux sous-sections : l'une comportant des « *dispositions générales* »⁷⁸, et l'autre des « *dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé* »⁷⁹.

Seulement, « *le champ d'application de ce régime [particulier] ne recouvre pas l'ensemble des traitements de données de santé* »⁸⁰. En réalité, « *la plupart des traitements de données de santé sont mêmes exclus de ce régime* »⁸¹. En effet, les « *dispositions générales* »⁸² relatives aux traitements de données personnelles dans le domaine de la santé avertissent que cette section introduit des conditions supplémentaires au RGPD pour les seuls traitements présentant une *finalité d'intérêt public*⁸³. La loi Informatique et Libertés modifiée écarte donc expressément l'application de cette section particulière⁸⁴ aux « *traitements [de données de santé] nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé* »⁸⁵. Autrement dit, le dispositif particulier introduit par la loi nationale ne semble s'adresser qu'aux responsables des traitements de données de santé poursuivant une finalité concourant à la santé publique. En effet, le droit national n'a imposé des formalités particulières pour les seuls traitements présentant des motifs d'intérêt public dans le domaine de la santé, telles que l'autorisation de la Commission nationale de l'informatique et des libertés (CNIL) en amont de leur réalisation⁸⁶. Pour cause, il est « *apparu nécessaire, à la fois pour des raisons de santé publique et des besoins de plus grande innovation des systèmes de santé notamment connectés, de pouvoir ouvrir davantage l'accès aux très importantes bases de données*

⁷⁷ Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

⁷⁸ Sous-section 1 de la Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

⁷⁹ Sous-section 2 de la Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

⁸⁰ DOUVILLE (T.), *Droit des données à caractère personnel, op. cit.*, p. 359.

⁸¹ *Ibid.*

⁸² Sous-section 1 de la Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

⁸³ Article 66 I de la loi Informatique et Libertés modifiée.

⁸⁴ Article 65 1° de la loi Informatique et Libertés modifiée.

⁸⁵ Article 44 1° de la loi Informatique et Libertés modifiée.

⁸⁶ Article 66 III de la loi Informatique et Libertés modifiée.

constituées dans le domaine de la santé »⁸⁷ tout en renforçant leur protection eu égard à leur très grande sensibilité.

23. Alors que le législateur européen protège généralement les données concernant la santé en raison de leur nature sensible, le législateur français n'encadre spécifiquement l'usage de cette catégorie de données personnelles que dans le cas où leur traitement poursuit une finalité inscrite dans le domaine de la santé collective⁸⁸. En d'autres termes, la protection particulière des données de santé n'est concédée par le droit national qu'en raison du contexte sanitaire dans lequel leur traitement s'inscrit. Il en advient que le régime particulier prescrit par la loi Informatique et Libertés modifiée ne concède aucun statut propre à la donnée de santé, et moins encore à la donnée médicale. Pourtant, la donnée médicale mérite un encadrement juridique dès sa génération et indépendamment des circonstances de ses potentielles utilisations.

2. L'application du droit à la confidentialité de la vie privée du patient

24. Bien que la loi Informatique et Libertés modifiée n'édifie aucune condition particulière au traitement des informations du patient dans le cadre de ses soins, ce contexte sanitaire emporte la protection des données médicales au titre des droits des malades consacrés par la loi du 4 mars 2002⁸⁹. En effet, la prise en charge sanitaire est un espace sanctuarisé devant être préservé de toute indiscretion. C'est pourquoi toute information relative au patient, dont les professionnels intervenant dans le système de santé ont connaissance à l'occasion de l'exercice de leurs fonctions, est protégée par le *secret médical*⁹⁰. Ainsi, toute personne prise en charge par un professionnel intervenant dans le système de santé a droit au respect de sa vie privée et du secret des informations qui la concernent⁹¹. Il convient de rappeler que la qualification des données médicales dépend de l'environnement dans lequel ces informations sont créées⁹². Il a été précisé que les données

⁸⁷ MARTIAL-BRAZ (N), *Données traitées – Données de santé*, *op. cit.*, p. 87 à p. 88.

⁸⁸ Article 66 I de la loi Informatique et Libertés modifiée.

⁸⁹ Loi n° 2002-303 du 4 mars 2002, *loc. cit.*

⁹⁰ Article L.1110-4 du code de la santé publique.

⁹¹ *Ibid.*

⁹² LANNA (M.), *op. cit.*, p. 121.

médicales correspondaient aux éléments immatériels du corps humain du patient générés à l'occasion de sa prise en charge sanitaire⁹³. En tant qu'informations personnelles au patient, les données médicales, générées dans ce contexte thérapeutique, entrent alors dans le champ de protection de l'article L.1110-4 du code de la santé publique. Il en résulte que la donnée médicale personnelle fait l'objet d'une double protection fondée sur le droit à la protection des données personnelles et sur le droit au secret médical⁹⁴.

25. Le secret médical est une notion juridique source de confusion en raison de ses différentes acceptions. Bruno Py a constaté que « *les auteurs traitent de la question en choisissant tantôt l'expression de secret médical, tantôt l'expression de secret professionnel. Plusieurs utilisent alternativement les deux formules, les considérant à l'évidence comme des synonymes* »⁹⁵. Il nous appartient alors de préciser la terminologie qui sera employée au sein de la présente étude.

Depuis l'adoption de la loi du 4 mars 2002 relative aux droits des malades, le *secret médical* présente une dualité. D'une part, le *secret médical* constitue une obligation professionnelle établie à l'article L.1110-4 du code de la santé publique et sanctionnée à l'article 226-13 du code pénal. Par l'effet de la loi, les professionnels intervenant dans le système de santé sont soumis au silence à l'égard de toutes les informations personnelles relatives au patient obtenues lors de l'exercice de leur profession. Le manquement à cette obligation de se taire a pour effet d'engager la responsabilité pénale du dépositaire du secret professionnel. Pour cause, « *le délit de violation du secret professionnel est institué non seulement dans l'intérêt général, pour assurer la confiance qui s'impose dans l'exercice de certaines professions, mais également dans l'intérêt des particuliers, pour garantir la sécurité des confidences que ceux-ci sont dans la nécessité de faire* »⁹⁶. Le secret professionnel médical participe ainsi à l'instauration de la confiance, que le patient se doit d'accorder aux professionnels intervenant dans le système de santé, préalablement à la

⁹³ Cf. Paragraphe 15.

⁹⁴ HERVEG (J.), VERHAEGEN (M.-N.), POULLET (Y.), *Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé*, Revue de droit de la santé, 2002, p. 62.

⁹⁵ PY (B.), *Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel*, RDS, 2013, n°50 hors-série, p. 165

⁹⁶ ZORN-MACREZ (C.), *op. cit.* p. 85 à p. 86.

révélation de son intimité corporelle et de ses confidences⁹⁷. Tout au long de ce travail, l'expression *secret professionnel médical* désignera l'obligation légale à laquelle sont astreints les professionnels qui en sont dépositaires. Au demeurant, nous serons en droit de nous demander si le concept actuel du secret professionnel médical est encore approprié à la transformation numérique du système de santé⁹⁸.

Le *secret médical* n'est plus uniquement conçu comme une obligation de secret professionnel. Xavier Bioy, Anne Laude et Didier Tabuteau le considèrent « *comme un véritable droit du patient* »⁹⁹. D'autre part, le *secret médical* constitue donc un droit subjectif du patient. Sous ce prisme humaniste, le secret médical est analysé comme un élément de la protection de la vie privée appartenant aux droits de la personnalité¹⁰⁰. En effet, « *le droit au respect du secret médical apparaît ainsi comme une illustration du droit à la vie privée particulièrement adapté aux informations médicales, personnelles et confidentielles que les professionnels de santé sont amenés à connaître et à collecter dans le cadre de la relation de soins* »¹⁰¹. A ce titre, le *secret médical* s'entend comme un droit à la confidentialité qui bénéficie spécifiquement au patient à l'égard des informations qui entrent dans sa « *sphère d'intimité* »¹⁰². Il en ressort que le droit au secret médical et le droit à la protection des données personnelles ont pour point commun leur rattachement au droit au respect de la vie privée¹⁰³. En ce sens, la Cour européenne des Droits de l'Homme a eu l'occasion de juger que « *la protection des données à caractère personnel, et spécialement des données médicales, revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention* »¹⁰⁴. Le droit au secret médical

⁹⁷ PY (B.), *Le secret professionnel*, L'Harmattan, 2005 ; Crim., 19 novembre 1985, n° 83-92813, *Bull. crim.*, n°364 ; Crim., 8 avril 1998, n°97-83656, *Bull. crim.*, n° 138 ; D., 1999, n° 43, p. 381, obs. J. Penneau ; Dr. pén., 1998, comm. 113, M. Véron.

⁹⁸ BERANGER (J.), BOUADI (R.), *op. cit.*, p. 108 ; TRUCHET (D.), *Le secret médical, obligation obsolète ou exigence actuelle*, In Mélanges en l'honneur de Michel Bélanger, *Modernité du droit de la santé*, LEH, 2017, p. 317 à p. 328.

⁹⁹ BIOY(X.), LAUDE (A.), TABUTEAU (D.), *Droit de la santé*, 4^e ed., PUF, 2020, p. 295.

¹⁰⁰ *Ibid.*

¹⁰¹ BIOY(X.), LAUDE (A.), TABUTEAU (D.), *Droit de la santé*, 4^e ed., PUF, 2020, p. 295.

¹⁰² CARBONNIER (J.), *Droit civil*, Vol. 1, 14e ed, Presses universitaires de France, 1982, p. 341.

¹⁰³ CLEMENT-FONTAINE (M.), *L'union du droit à la protection des données à caractère personnel et du droit à la vie privée*, Légipresse, 2018, n°356, p. 19 à p. 24.

¹⁰⁴ CEDH, 27 août 1997,74/1996/693/885, *aff. M.S. c. Suède*, cons. 41 : AJDA, 1998, n° 01, p. 37, chron. J.-F. Flauss ; D., 2000, n° 24, p. 521, note I. Laurent-Merle.

apparaît alors comme une prérogative accordée au patient pour protéger sa vie privée. Tout au long de ce travail, l'expression *secret médical* renverra à ce droit de la personnalité accordé spécialement au patient par l'article L.1110-4 du code de la santé publique.

26. Si les données médicales personnelles sont enfermées dans le silence du colloque singulier, quel est l'intérêt, pour le patient concerné, de disposer d'un droit à la confidentialité à l'égard des éléments immatériels de son corps humain ? Le premier avantage réside dans la possibilité, pour la personne concernée, de demander la réparation en justice de toute atteinte à sa vie privée¹⁰⁵. Le second avantage tient aux prérogatives que le droit au respect de la vie privée offre aux individus. Sur le fondement de l'article 9 du code civil¹⁰⁶, la personne concernée peut, de sa propre initiative, déconfidentialiser les informations relevant de sa vie privée comme, à l'inverse, écarter les tiers de sa sphère secrète de vie afin d'être laissée tranquille¹⁰⁷.

27. Il résulte de ce qui précède que le droit au respect de la vie privée doit s'interpréter comme le pouvoir de maîtriser et de contrôler ses informations personnelles afin d'assurer son droit à la tranquillité¹⁰⁸. Nous retrouvons ici les « *trois facettes* » de la vie privée dégagées par Antoinette Rouvroy et Yves Poullet¹⁰⁹. La première facette consiste en l'opacité de la sphère intime : la personne bénéficie de la possibilité de conduire la vie qu'elle souhaite mener à l'abri des regards indiscrets¹¹⁰. La deuxième facette consiste en une autonomie décisionnelle : l'existence individuelle de la personne est protégée contre l'interférence des tiers dans l'expression de ses choix et de ses actions¹¹¹. La troisième facette de la vie privée consiste au pouvoir de contrôle de l'individu sur les informations qui le concernent : c'est-à-dire en une autodétermination informationnelle objectivée par les droits que la personne

¹⁰⁵ CARBONNIER (J.), *op. cit.*, p. 343.

¹⁰⁶ SAINT-PAU (J.-C.), *L'article 9 du code civil : matrice des droits de la personnalité*, Recueil Dalloz, 1999, p. 541.

¹⁰⁷ CARBONNIER (J.), *op. cit.*, p. 341.

¹⁰⁸ NIETO (A.), *La vie privée à l'épreuve de la relation de soin*, François VIALLA (dir.), Thèse de Doctorat, Droit, Université de Montpellier, 2017, p. 233.

¹⁰⁹ ROUVROY (A.), POULLET (Y.), *Le droit à l'autodétermination informationnelle et la valeur du développement personnel: une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie*, In BENYKHELF (K.), TRUDEL (P.), *Etat de droit et virtualité*, Thémis, Montréal, p. 192 à p. 209.

¹¹⁰ *Ibid.*

¹¹¹ *Ibid.*

concernée détient sur ses données personnelles¹¹². Réciproquement, le droit à la protection des données personnelles est un moyen de garantir la vie privée des personnes concernées¹¹³.

En somme, « *le traitement informatisé des données du patient se construit autour d'un axe fondamental : le respect de sa vie privée. Ce principe s'inscrit tant dans la nécessité de maintenir la confiance des citoyens dans le système des soins de santé, que dans la reconnaissance de leur droit à l'autodétermination informationnelle* »¹¹⁴. La portée de l'autodétermination informationnelle du patient est devenue une question capitale à l'aube de la numérisation du système de santé¹¹⁵. S'il n'est pas question d'attenter à la confidentialité des données intimes du patient, il convient néanmoins de s'interroger sur le pouvoir que le patient détient à l'égard de ces matériaux dont l'usage est indispensable à la protection de la santé individuelle et collective. Pour cause, la *protection de la santé* est un objectif à valeur constitutionnel¹¹⁶ qui « *revêt un caractère hybride : protection de l'intérêt général à travers la santé publique, protection des intérêts individuels à travers la santé de chacun* »¹¹⁷. La mise en œuvre de cet objectif, qui constitue par ailleurs un droit fondamental¹¹⁸, peut légitimer une réduction des droits et des libertés individuels¹¹⁹. Il importe alors de trouver un équilibre entre les prérogatives du patient sur sa donnée médicale et les besoins de son exploitation pour l'intérêt particulier de sa prise en charge sanitaire

¹¹² *Ibid.*

¹¹³ Cons. Const., Décision n°2012-652 DC, 22 mars 2012, cons. 8 : JCP A, 2012, act. 232 ; RLDI, 2012, n° 83, 2783, obs. L. Costes ; AJDA, 2012, p. 623, note R. Grand ; Cons. Const., Décision n°2013-675 DC, 9 octobre 2013, cons. 26 : JCP A, 2014, 2018, etu. M. Verpeaux ; JCP G, 2013, n° 44-45, 1143 ; JCP A, 2013, n° 42, act. 800 ; Cons. Const., Décision n°2013-681, 5 décembre 2013, cons. 27 : JCP G, 2013, n° 52, 1365, obs. C. Tukov ; JCP A, 2013, n° 51, act. 951, obs. R. Bourrel ; JCP G, 2013, n° 05, doct. 152, étu. M. Verpeaux ; Cons. Const., Décision n°2014-690 DC, 13 mars 2014, cons. 51 ; Cons. Const., Décision n°2018-765 DC, 12 juin 2018, cons. 47.

¹¹⁴ HERVEG (J.), VERHAEGEN (M.-N.), POULLET (Y.), *op. cit.*, p. 58.

¹¹⁵ FOEGLE (J.-P.), *Le "droit" à l'autodétermination informationnelle et les réseaux numériques*, In ENCINAS DE MUNAGORI (R.), BENSAMOUN (A.), BROSSET (E.), COHENDET (M.-A.), *Sciences et droits de l'homme*, Mare & Martin, 2017, p. 85 à p. 103 ; BARBE (V.), *La garantie du droit au respect de la vie privée face au fichier* », In EDDAZI (F.), MAUCLAIR (S.), *Le fichier*, Actes du colloque organisé les 26 et 27 novembre 2015 par le Centre de recherche juridique Pothier de l'Université d'Orléans, LGDJ, p. 87 et s.

¹¹⁶ Cons. Const., Décision n° 93-325 DC, 13 août 1993 : D., 1994, n° 13, p. 111, obs. D. Maillard Desgrées du Loû ; Dr. soc., 1994, n° 01, p. 69, étude J.-J. Dupeyroux et X. Prétot ; RFDA, 1993, n° 05, p. 871, note B. Genevois ; Rev. crit. DIP, 1994, n° 01, p. 01, ét. D. Turpin ; Cons. Const., Décision n° 90-283 DC, 8 janvier 1991 : RDSS, 1991, n°02, p. 204, J.-S. Cayla ; AJDA, 1991, n° 05, p. 382, comm. P. Wachsmann.

¹¹⁷ MEMETEAU (G.), GIRER (M.), *Cours de droit médical*, 5e ed., LEH, 2016, p. 685.

¹¹⁸ Cf. Paragraphe 329.

¹¹⁹ Cf. Paragraphe 332.

comme pour l'intérêt général de la société. Eu égard à ces enjeux, l'autodétermination informationnelle du patient à l'égard de sa donnée médicale constituera la clé de voute de cette étude. Autrement dit, ces travaux seront centrés autour des droits et des devoirs que le patient détient réellement et concrètement à l'égard des éléments immatériels de son corps humain. La présente thèse apportera donc une perspective sectorielle du droit des données sous l'angle de l'autodétermination informationnelle du patient concerné par l'usage de sa donnée médicale.

Paragraphe 2 : La réduction de l'autodétermination informationnelle du patient

28. Si la donnée médicale nécessite un encadrement juridique particulier, c'est notamment afin de compenser la restriction de la maîtrise et du contrôle du patient envers les éléments immatériels de son corps humain. Dans un contexte sanitaire individuel et collectif, l'usage de la donnée médicale semble présenter un caractère impérieux (**A**). En effet, les données médicales du patient constituent également des outils sanitaires à l'égard desquels le patient concerné ne peut exercer l'ensemble des droits dont il bénéficie sur ses données à caractère personnel (**B**).

A) Le caractère obligatoire du traitement de la donnée médicale

29. A titre exceptionnel, tout traitement de données sensibles est autorisé lorsque son objectif poursuit l'une des finalités dérogatoires énumérées à l'article 9.2 du RGPD¹²⁰. Si le droit à la protection des données personnelles interdit l'utilisation des informations liées à la vie intime des personnes concernées, il existe dix situations dans lesquelles la mise en œuvre d'un traitement de données sensibles est autorisée. Ce principe d'interdiction ne pouvait certainement pas présenter un caractère absolu. Dans certaines situations, l'utilisation des informations se rapportant à la vie privée des personnes concernées est en effet requise.

En premier lieu, l'article 9.2 du RGPD précise que tout traitement de données sensibles peut être réalisé dans l'hypothèse où la personne concernée a donné son

¹²⁰ Cf. Paragraphe 17.

consentement explicite pour une finalité spécifique dont elle a été préalablement informée¹²¹. Bien que le consentement ne traduit pas « *toujours une pleine et consciente acceptation [...] des conditions de traitement* »¹²², il revient à accorder à la personne concernée la maîtrise de l'usage de ses informations intimes. Cependant, le consentement à l'usage de ses données sensibles ne constitue pas l'unique exception au principe d'interdiction de leur traitement. Il existe neuf autres dérogations qui n'exigent pas l'acceptation de l'intéressé. En effet, il subsiste des situations où l'usage des données sensibles se révèle indispensable nonobstant l'importance de leur sensibilité ou la volonté de la personne concernée. Ainsi, le traitement des données médicales du patient – en leur qualité de données sensibles – est exceptionnellement autorisé dans le cadre de sa prise en charge sanitaire¹²³, ou lorsqu'il est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique¹²⁴ tels que la recherche et l'innovation dans le domaine de la santé et la protection contre les menaces sanitaires. De la même façon, parmi les six bases légales sur lesquelles un traitement de données personnelles doit indispensablement reposer¹²⁵, le consentement ne constitue que l'un des fondements juridiques appuyant sa licéité. Sauf à ce que l'opération de traitement ne constitue une obligation légale pour le responsable de traitement, ces deux utilisations dérogatoires des données médicales du patient reposent tantôt sur les intérêts légitimes du professionnel de santé ou de l'innovateur en santé¹²⁶, tantôt sur une mission de service public dont est investi l'établissement de santé¹²⁷.

30. Qu'ils soient mis en œuvre au bénéfice du patient ou dans l'intérêt de la collectivité, ces traitements de données médicales du patient ne semblent jamais reposer sur son consentement. Il en advient que dans ces deux contextes, l'exploitation de la donnée médicale personnelle présente un caractère péremptoire. Cette impériosité coïncide avec la transformation du système de santé numérique à laquelle la société ne peut échapper. La santé individuelle comme la santé collective reposent dorénavant sur le traitement de l'information

¹²¹ Article 9.2 a) du RGPD.

¹²² MARTIAL-BRAZ (N), *Base de traitement – Consentement*, In MARTIAL-BRAZ (N.), ROCHFELD (J.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, p. 143.

¹²³ Article 9.2 h) du RGPD.

¹²⁴ Article 9 .2 i) du RGPD.

¹²⁵ Cf. Paragraphe 19.

¹²⁶ Article 6.1 f) du RGPD.

¹²⁷ Article 6.1 e) du RGPD.

médicale. D'une part, « *l'utilisation de systèmes d'information est désormais un accessoire indispensable à la réalisation de la mission de soins* »¹²⁸ pluridisciplinaire. D'autre part, le développement des dispositifs de santé numérique dépend intrinsèquement de l'innovation en santé, laquelle s'appuie indispensablement sur l'exploitation de la donnée médicale du patient. La donnée médicale personnelle doit donc être partagée pour la prise en charge sanitaire du patient comme pour le progrès de la santé publique.

31. Si le patient conservait une portion de la maîtrise de sa donnée médicale, il devrait alors en permettre l'exploitation. Véritablement, « *la rupture culturelle que nous nous proposons de comprendre n'est-elle pas celle qui va changer définitivement notre rapport à l'information et faire de cette métamorphose la porte d'entrée dans une nouvelle culture numérique ?* »¹²⁹. Le patient, en tant que membre d'une société, doit être mobilisé dans la mutation sociétale induite par l'ère de l'information et du numérique. Il en résulte que le patient aurait davantage le devoir de favoriser l'exploitation des éléments immatériels de son corps humain que la possibilité de renoncer à leur traitement. Pourtant, la donnée médicale émane d'une personne en état de vulnérabilité alors qu'elle se livrait, en toute confiance, à un professionnel de santé soumis au secret professionnel médical. Seulement, plus une donnée est sensible, moins l'interdiction de son traitement ne semble pouvoir être levée par la personne concernée. Autrement dit, plus l'information est sensible, plus son usage doit poursuivre un caractère impérieux. Si le patient ne semble pouvoir déterminer de l'usage de sa donnée médicale, qu'en est-il des droits dont il dispose sur cet élément immatériel de son corps humain ?

B) La restriction des prérogatives du patient à l'égard de sa donnée médicale

32. Le droit à la protection des données personnelles concède une pluralité de prérogatives que les individus peuvent détenir sur les informations qui les concernent. Il est offert, aux personnes concernées, les droits d'accéder à leurs données personnelles¹³⁰, de les

¹²⁸ ANS, *TIC & Santé*. Disponible en ligne sur le site [esante.gouv.fr]. Consulté le 28 novembre 2021.

¹²⁹ LE REUN (R.), *op. cit.*, p. 47.

¹³⁰ Article 15 du RGPD.

rectifier¹³¹, de les effacer¹³², d'en demander la portabilité¹³³, d'en limiter le traitement¹³⁴, de s'opposer à leur utilisation¹³⁵, et de donner des directives sur leur sort après leur décès¹³⁶. Il en résulte que toute personne concernée par un traitement de données personnelles bénéficie théoriquement de leur maîtrise et de leur contrôle. Cette maîtrise et ce contrôle des données personnelles par la personne concernée correspond au concept de *l'autodétermination informationnelle* dégagé en 1983 par la Cour constitutionnelle fédérale allemande¹³⁷. Pauline Türk explique qu'il « *correspond à l'affirmation d'un droit de la personne à être placée en capacité de disposer librement de ses données personnelles et des informations numériques qui la concernent, et de maîtriser leur utilisation* »¹³⁸. Ainsi, le *Selbstbestimmungsrecht* consiste au droit, pour chaque individu, de décider de l'emploi des informations le concernant. Cette faculté conditionne le caractère démocratique de nos sociétés¹³⁹. Elle octroie, aux personnes concernées, la liberté de déterminer leurs conditions d'existence et leur assure une autonomie de décision¹⁴⁰. A titre d'exemple, le patient devrait pouvoir décider de consulter un professionnel de santé sans que cette liberté ne soit conditionnée par la crainte que ses données médicales ne soient divulguées à des tiers. Si le patient ne conservait pas le contrôle des éléments immatériels de son corps humain, il pourrait, par peur qu'ils lui échappent, renoncer aux soins. D'une certaine façon, l'autodétermination informationnelle entre en résonance avec le droit au respect de la vie privée et, conséquemment, avec le droit à la confidentialité des éléments intégrant la sphère intime de l'individu. Certainement, si le patient n'avait pas la garantie que le secret professionnel médical était préservé, il pourrait

¹³¹ Article 16 du RGPD.

¹³² Article 17 du RGPD.

¹³³ Article 20 du RGPD.

¹³⁴ Article 18 du RGPD.

¹³⁵ Article 21 du RGPD.

¹³⁶ Article 85 de la loi Informatique et Libertés modifiée.

¹³⁷ Cour constitutionnelle fédérale allemande, 15 décembre 1983.

¹³⁸ TÜRK (P.), *L'autodétermination informationnelle : un droit fondamental émergent ?*, Dalloz IP / IT, 2020, n°11, p. 616.

¹³⁹ *Ibid.*

¹⁴⁰ MARTIAL-BRAZ (N.), *Le renforcement des droits de la personne concernée*, Dalloz IP/IT, 2017, n° 05, p. 254.

faire le choix, pour préserver la confidentialité de ses informations intimes, de se soustraire au système de santé.

Le concept de l'autodétermination informationnelle a été repris et affirmé par le droit français, au premier article de la loi Informatique et Libertés, et se concrétise à travers les droits que la personne concernée détient sur ses données personnelles en vertu du RGPD. En effet, les dispositions de la loi nationale énoncent que « *les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant [...] s'exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi* »¹⁴¹. En somme, les droits octroyés par le RGPD à la personne concernée objectivent le principe de l'autodétermination informationnelle de la personne concernée. Néanmoins, tous les droits relatifs aux données personnelles ne sont pas identiquement ni systématiquement applicables. En effet, l'étude des dispositions relatives aux droits des personnes concernées permet de constater que l'existence et l'exercice de certains sont « *frappés d'incertitude* »¹⁴².

33. L'ensemble des droits énumérés sont conçus de façon générique afin de s'appliquer, par défaut, à toute personne concernée ainsi qu'à toute donnée à caractère personnel. Néanmoins, toutes les prérogatives concédées aux personnes concernées n'ont pas toujours vocation à s'appliquer. En premier lieu, Thibault Douville souligne que « *la nature de la base juridique du traitement a une incidence sur les droits reconnus à la personne concernée* »¹⁴³. En effet, l'existence des droits consacrés par le RGPD varie en fonction de la base légale sur laquelle le traitement est fondé¹⁴⁴. Assurément, l'exercice de certains droits de la personne concernée pourrait contrarier la réalisation d'un traitement dont la licéité repose sur un fondement juridique contraignant. Par exemple, lorsqu'un traitement de données personnelles prend sa source dans une obligation légale incombant au responsable de traitement¹⁴⁵, l'exercice des droits d'opposition au traitement et d'effacement des données

¹⁴¹ Article 1^{er} de la loi Informatique et Libertés modifiée.

¹⁴² MARTIAL-BRAZ (N.), *Le renforcement des droits de la personne concernée*, op. cit., p. 258.

¹⁴³ DOUVILLE (T.), *Droit des données à caractère personnel*, op. cit, p. 111.

¹⁴⁴ Cf. Paragraphe 33.

¹⁴⁵ Article 6.1 c) du RGPD.

personnelles ferait échec à l'exécution de sa réalisation. En second lieu, l'existence des droits consacrés par le RGPD fluctue en fonction de la finalité du traitement des données personnelles¹⁴⁶. En effet, l'exercice des droits de la personne concernée pourrait contrevenir à l'accomplissement de l'objectif du traitement. A titre d'illustration, l'effectivité du droit à l'effacement des données personnelles compromettrait les traitements nécessaires « *à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* »¹⁴⁷. C'est ainsi que le droit à la protection des données personnelles module l'exercice de chaque droit, indifféremment octroyé aux personnes concernées, en fonction des situations objectives énumérées aux articles 6.1 et 9.2 du RGPD.

34. Tandis que le droit à la protection des données personnelles conçoit des restrictions aux droits de la personne concernée en considération du contexte du traitement, ni le législateur européen, ni le droit national ne prennent compte la nature de la donnée personnelle traitée. Pourtant, les caractéristiques de la donnée médicale tendent directement à impacter les droits qui sont restrictivement reconnus au patient. Il en advient que les droits dont le patient devrait bénéficier lorsque sa donnée médicale est exploitée dans le cadre de sa prise en charge sanitaire, ou dans le domaine de la santé publique, se trouveraient inconciliables avec les caractéristiques qui lui sont propres. En effet, la donnée médicale, en tant qu'instrument sanitaire généré par le professionnel de santé, doit demeurer intègre et immuable. Le patient ne devrait donc intervenir ni sur la structure, ni sur la substance des éléments immatériels de son corps humain. Alors, le patient disposerait de moins de droits sur sa donnée médicale que la personne concernée sur sa donnée de santé. Pourtant, la donnée médicale est profondément rattachée au patient qui en est la source. Il apparaîtrait donc légitime que le patient détienne l'entière maîtrise des éléments qui le concernent intimement¹⁴⁸.

35. Il apparaît que les droits dont le patient dispose à l'égard de sa donnée médicale se trouvent fortement limités et que les prérogatives qui lui subsistent se révèlent chimériques. Cette dépossession est-elle compatible avec le droit fondamental à la protection des données

¹⁴⁶ Cf. Paragraphe 33.

¹⁴⁷ Article 17.3 d) du RGPD.

¹⁴⁸ DEBIES (E.), *Big data de santé et autodétermination informationnelle : quelle articulation possible pour une innovation protectrice des données personnelles ?*, Revue française d'administration publique, 2018, vol. 3 n° 167, p. 573.

à caractère personnel¹⁴⁹ ? En pratique, la donnée médicale constitue un instrument sanitaire au service du droit fondamental à la protection de la santé individuelle et collective¹⁵⁰. Il en advient un conflit entre des droits fondamentaux de valeur juridique égale. Les enjeux liés à l'usage de la donnée médicale au profit de la Santé bouleversent donc les rapports entre le patient et sa chose intime.

Bien que l'usage de la donnée médicale soit généralement encadré par le droit à la protection des données personnelles, ce cadre juridique lui apparaît insuffisamment adapté. Ce régime générique ne tient compte ni des particularités endogènes aux éléments immatériels issus du corps humain du patient, ni des risques que son usage impérieux engendre sur la protection des données et des personnes concernées, ni des perturbations que son utilité entraîne sur les droits fondamentaux des individus.

Paragraphe 3 : La réglementation spécifique à la donnée médicale du patient

36. La donnée médicale du patient constitue à la fois un élément immatériel de son corps humain et un outil sanitaire indispensable à sa prise en charge médicale, à la santé publique ainsi qu'à la recherche et à l'innovation en santé. Par surcroît, la donnée médicale comporte des utilités notamment fondamentales à l'avancement de la transition numérique du système de santé, à la conception des médicaments et des dispositifs médicaux, et au développement économique de cet écosystème. Alors que la donnée médicale n'a longtemps intéressé que le professionnel de santé dans le cadre d'une relation médicale bipartite, elle « *est aujourd'hui devenue un enjeu majeur de société* »¹⁵¹. En raison de ses utilités, la donnée médicale est désormais prise en compte par les concepteurs de dispositifs numériques en santé, par l'industrie pharmaceutique, par les *data analysts* en profilage et *marketing*, par les *data brokers*, ou encore par les cybercriminels¹⁵². Outre l'économie produite à l'occasion du traitement de la donnée médicale, ses utilités lui confèrent une certaine valeur financière. Il en advient que la

¹⁴⁹ Article 8 de la Charte des droits fondamentaux de l'Union européenne, *JOUE* C 326/391, 26 octobre 2012.

¹⁵⁰ Article 35 de la Charte des droits fondamentaux de l'Union européenne, *JOUE* C 326/391, 26 octobre 2012 ; Alinéa 11 du Préambule de la Constitution de 1946 ; Cons. Const., Décision n° 74-54 DC, 15 janvier 1975.

¹⁵¹ MORLET-HAÏDARA (L.), *Les usages du big data en santé et les exigences du respect des droits des patients*, Revue Pratique de la Prospective et de l'innovation, 2019, n° 02, p. 37.

¹⁵² Voir : DOUVILLE (T.), *Les droits des personnes concernées en cas de transmission de leurs données à caractère personnel*, Revue Lamy Droit de l'Immatériel, 2018, n° 153, p. 33.

donnée médicale présente des intérêts qui en font un objet de convoitise et qui tendent naturellement à la qualifier de *bien*.

Au siècle de l'information et de l'électronique, comment résister à l'appropriation de la donnée médicale, à son consumérisme et à l'exploitation de l'ensemble des informations qu'elle peut révéler sur son hôte ? Bien que la donnée médicale soit un instrument séduisant pour les acteurs de la santé, du numérique, de la finance ou des assurances, il n'en demeure pas moins qu'il s'agit d'un élément immatériel provenant du corps humain du patient. Tant son usage que son appropriation exposent le patient concerné à un asservissement de sa personne ainsi qu'à des atteintes à ses droits et ses libertés fondamentaux. Par le simple fait de son existence, la donnée médicale comporte donc des risques qu'il convient de prévenir¹⁵³.

37. En réponse aux risques intrinsèques à la donnée médicale, il conviendrait de lui allouer une protection adaptée et proportionnée aux enjeux en péril. Si le patient n'avait pas la garantie que les éléments immatériels de son corps humain, générés à l'occasion de sa prise en charge sanitaire, ne seraient ni divulgués, ni détournés, ni vendus, d'aucun n'accorderait plus sa confiance au système de santé. Parce qu'elle a été recueillie ou produite dans un cadre sanitaire marqué par le colloque singulier, et qu'elle touche directement à la dignité et à l'intégrité du patient concerné, la donnée médicale mérite une consécration juridique authentique. La notion de donnée médicale doit certainement être déterminée pour garantir aux personnes une protection cohérente de ces éléments immatériels du corps humain, et pour déterminer la portée de leur autodétermination informationnelle à leur égard en fonction de leur usage.

38. De toute évidence, la question de la conciliation entre l'indispensable exploitation de la donnée médicale et la nécessaire sacralisation de sa protection se pose alors foncièrement. Qu'advient-il de la relation entre le patient et sa donnée médicale ? Quelle place occupera-t-il dans un écosystème numérique qui dépend indéfectiblement de l'usage de sa chose intime ? Si l'imprécision et la complexité du Droit ne permet actuellement pas de sécuriser la facilitation du traitement de la donnée médicale du patient, ni de déterminer les

¹⁵³ Sur les menaces liés aux nouveaux usages numériques : DALLE (D.), QUEMENER (M.), WIERRE (C.), *Quels droits face aux innovations numériques ? Législation, jurisprudences et bonnes pratiques du cyberspace - Défis et protections face aux dérives du numériques*, Gualino, 2020.

prérogatives qu'il détient effectivement à son égard, le Droit pourrait offrir des solutions sur la base des garanties juridiques fondamentales auxquelles il n'est pas ici question de renoncer. Certainement, si un statut authentiquement protecteur était concédé à la donnée médicale, sa circulation et son utilisation pourraient être favorisées grâce à l'affirmation de sa sanctuarisation. Toutefois, si la donnée médicale pouvait être exploitée dans le respect de la dignité du patient concerné et en toute confidentialité, il n'empêche que le droit au respect de la vie privée permet ordinairement à l'individu « *de s'opposer à toute intrusion non consentie dans sa sphère intime* »¹⁵⁴. C'est pourquoi il apparaît tout aussi nécessaire de redéfinir les prérogatives que le patient détient effectivement sur sa donnée médicale à la lumière de la définition octroyée à cette chose originale d'une part, et des enjeux que son exploitation comporte d'autre part.

39. Alors que ces travaux s'attacheront à spécifier un statut propre à la donnée médicale, ils tâcheront également de redéterminer les contours de l'autodétermination informationnelle du patient en considération de ses usages. Pour y parvenir, l'ensemble des branches du droit seront mobilisées. Au carrefour du droit des données et du droit de la santé, le sujet de la présente thèse porte sur des matières juridiques transversales qui entretiennent des liens étroits avec le droit supranational, européen et français, ainsi qu'avec les différentes sous-branches du droit privé et du droit public. En effet, le droit des données est édicté par des normes européennes foisonnantes¹⁵⁵ qui harmonisent un cadre de droit commun et qui entrent en résonance avec de multiples règles de droit interne. Le droit civil des personnes assure la protection des données personnelles par les droits de la personnalité, pendant que le droit de la propriété mobilière restreint leur appréhension par quiconque. Par ailleurs, le droit des contrats borde les conventions d'usage entre les détenteurs et les futur utilisateurs des

¹⁵⁴ HENNETTE-VAUCHEZ (S.), ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, Dalloz, 4^{ème} ed., 2020, p. 448 ; CARBONNIER (J.), *op. cit.*, p. 342 ; LOISEAU (G.), *Le droit des personnes*, 2^e ed., Ellipses, 2020, p. 251.

¹⁵⁵ Dont principalement : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JOUE* L 119/1, 4 mai 2016 ; Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *JOUE* L 303/59, 28 novembre 2018 ; Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données, 2020/0340 COD, 25 novembre 2020 ; Proposition de 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 (règlement sur les données), 2022/0047 COD, 23 février 2022.

données médicales¹⁵⁶ alors que le droit de la propriété intellectuelle administre la valorisation des résultats de leur traitement. Le droit des données se rapporte également au droit administratif lorsque les informations personnelles ou anonymes ont été générées par une personne morale investie d'une mission de service public. Le cas échéant, l'usage de la donnée médicale se trouve régi par les règles d'accès aux documents administratifs et de réutilisation des informations publiques. Le droit des données apparaît donc marqué par la fragmentation de son corpus juridique.

De la même façon, le droit de la santé et le droit médical transcendent les clivages traditionnels des disciplines juridiques. Ces droits hybrides sont réunis au sein du code de la santé publique, dont les dispositions organisent notamment l'accès aux données médicales pour la prise en charge sanitaire du patient et leur réutilisation pour des motifs d'intérêt public dans le domaine de la santé.

Ce corpus, aussi varié qu'abondant, engendre un certain flou juridique lorsqu'il s'agit de déterminer les régimes juridiques applicables aux différents usages de la donnée médicale. L'une des difficultés majeures de ces travaux se trouve dans l'articulation du droit privé et du droit public, du droit du numérique et du droit de la santé. Toutefois, les différentes branches du droit civil et du droit administratif offrent un terrain d'expérimentation particulièrement riche et diversifié pour construire des propositions *sui generis* relatives à l'usage de la donnée médicale.

40. Pour construire ces propositions, il apparaissait essentiel de distinguer les données médicales en leur concédant une définition spécifique¹⁵⁷. C'est donc à la lumière des caractéristiques de cet élément immatériel du corps humain que la portée de l'autodétermination informationnelle du patient sera analysée. Les cas d'usage de la donnée médicale étant limitativement concédés¹⁵⁸, cette étude s'articulera logiquement autour des prérogatives du patient lorsqu'elle est générée et traitée à des fins de prise en charge médicale, puis lorsqu'elle est réutilisée à des fins d'intérêt public dans le domaine de la santé.

¹⁵⁶ Sur les rapports entre le droit du numérique et le droit privé, voir : NETTER (E.), *Numérique et grandes notions du droit privé*, CEPRISCA, 2019.

¹⁵⁷ Cf. Paragraphe 15.

¹⁵⁸ Cf. Paragraphe 17.

En premier lieu, nous examinerons donc le rapport que le patient entretient avec sa donnée médicale lorsqu'elle est traitée dans le cadre de sa prise en charge sanitaire (**Première partie**). A cette occasion, nous révélerons que la personne concernée aurait le devoir de promouvoir la communication des éléments immatériels de son corps humain. Générés par les professionnels de santé dans un contexte médical, ils constituent assurément les matériaux essentiels à la dispensation des services de soins de santé.

En second lieu, nous analyserons le rapport que le patient entretient avec sa donnée médicale lorsqu'elle est traitée au bénéfice de la collectivité (**Seconde partie**). En l'occurrence, nous dévoilerons que tout citoyen aurait le devoir de placer les éléments immatériels de son corps humain à la disposition des acteurs concourant à la protection de la santé collective. Certainement, les activités connexes à la santé publique sont principalement fondées sur la réutilisation des données médicales des membres de la société.

Que l'usage de la donnée médicale profite directement ou indirectement au patient concerné, nous démontrerons que les droits qu'il devrait détenir sur celle-ci s'avèrent fortement circonscrits. A l'inverse, le patient aurait davantage de devoirs à son égard : la donnée médicale devient quérable à l'image d'une créance du système de santé numérique à l'encontre du patient. La protection de la donnée médicale mérite alors d'être renforcée par l'édification d'un encadrement juridique spécifique et, subséquentement, par l'identification de l'autodétermination informationnelle que le patient concerné dispose réellement à son égard.

PREMIERE PARTIE :

LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AU PROFIT DE SA PRISE EN CHARGE SANITAIRE

41. Des données de santé, et plus spécifiquement des données médicales, sont générées à l'occasion de toute prise en charge sanitaire. En effet, ces informations singulièrement intimes sont recueillies et produites par les professionnels intervenant dans le système de santé dès la prise du rendez-vous médical et lors de la dispensation d'actes de prévention, de diagnostic ou de soins. Cette collection d'informations médicales est indispensable à la délivrance des services de soins de santé. Certainement, la prise en charge sanitaire du patient repose nécessairement sur leur consultation, leur utilisation et leur analyse par les professionnels y concourant. En tant qu'outil technique de la science médicale, il est apparu fondamental que les données médicales du patient soient tracées, regroupées et disponibles au sein d'un support identifié. C'est pourquoi les données médicales, générées à l'occasion de la prise en charge sanitaire du patient, doivent être formalisées, rassemblées et conservées au sein de fichiers sécurisés et confidentiels communément appelés « dossiers médicaux » (**Titre 1**). Ces fichiers peuvent être définis comme l'« *élément dynamique constitué pour être le support de l'ensemble des informations recueillies à l'occasion de la prise en charge du patient* »¹⁵⁹. Alors formalisée au sein d'un support tangible, la donnée médicale issue du corps humain du patient devient accessible tant au patient concerné qu'aux professionnels concourant à sa prise en charge sanitaire (**Titre 2**). Certainement, la donnée médicale du patient a vocation à circuler.

¹⁵⁹ ANAES, *Evaluation des pratiques professionnelles dans des établissements de santé, Dossier Du Patient : Réglementation et recommandations*, juin 2003, p. 4. Disponible sur le site [www.has-sante.fr]. Consulté le 1^{er} décembre 2021.

TITRE 1 :

LA FORMALISATION DES DONNEES MEDICALES AU SEIN DES DOSSIERS MEDICAUX DU PATIENT

« Le dossier est une mémoire écrite des informations cliniques, biologiques, diagnostiques et thérapeutiques d'un malade, à la fois individuelle et collective, constamment mise à jour ».

Pr Francis Roger-France.

42. Un dossier médical, réunissant l'ensemble des données médicales du patient, est obligatoirement constitué pour chacune de ses prises en charge au sein d'un établissement de santé ou au cabinet d'un médecin¹⁶⁰. Ces dossiers sont alors conservés au sein de l'établissement de santé ou du cabinet médical dans lequel le patient a bénéficié d'actes sanitaires¹⁶¹. Ces dossiers médicaux apparaissent plus exactement comme des dossiers relatifs aux soins. Pour un même patient, il existe donc autant de dossiers de soins que de structures de santé dans lesquelles il a été médicalement pris en charge. En outre, les données médicales générées lors de la prise en charge sanitaire du patient peuvent être intégrées au sein de dossiers numériques supplémentaires aux dossiers de soins, dont le plus notoire est le Dossier Médical Partagé (DMP). A l'inverse des dossiers de soins, le DMP est un dossier numérique rattaché au patient, indépendamment de ses éventuelles prises en charge médicales. En tant que carnet de santé numérique, le DMP est accessible, au moyen de l'Internet, à l'ensemble des professionnels de santé concourant à la prise en charge du patient, quels que soient leur mode et leur lieu d'exercice. Bien que ces différents dossiers soient qualifiés de « dossiers médicaux », le dossier de soins se distingue du DMP. Le fait que le patient soit titulaire d'un DMP ne dispense donc pas chaque établissement ou professionnel de santé d'établir un dossier de soins pour tout patient pris en charge¹⁶².

¹⁶⁰ Article R.1112-2 du code de la santé publique ; Article R.4127-45 du code de la santé publique.

¹⁶¹ Article R.1112-7 du code de la santé publique.

¹⁶² Article R.1111-40 du code de la santé publique.

43. Ces opérations de collecte, d'enregistrement, de structuration et de conservation des données médicales du patient au sein d'un fichier idoine correspondent exactement à la définition de la notion de *traitement* telle que définie à l'article 4 du RGPD. Autrement dit, la formalisation des données médicales du patient au sein d'un dossier médical constitue un traitement de données personnelles. C'est ainsi que ce *traitement* doit répondre à l'ensemble des dispositions juridiques du droit à la protection des données personnelles, dont aux six principes essentiels prescrits à l'article 5 du RGPD¹⁶³. Parmi ces « *principes relatifs au traitement des données à caractère personnel* »¹⁶⁴, le professionnel intervenant dans le système de santé doit veiller à respecter le principe de minimisation¹⁶⁵ lors de la génération des données médicales du patient. En vertu de ce principe, seules les données personnelles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées peuvent être régulièrement collectées. Afin d'en assurer le respect, il est primordial de déterminer les catégories de données devant être formalisées au sein des différents dossiers médicaux du patient. Il convient donc d'étudier avec précision les contours des données qui y sont colligées (**Chapitre 1**).

44. La délimitation des données consignées au sein des dossiers médicaux est un exercice crucial pour l'exercice des droits du patient sur ses données médicales. D'une part, l'identification des données colligées au sein des dossiers médicaux du patient permet de distinguer les éléments immatériels à l'égard desquels il détient effectivement des droits. D'autre part, la détermination des données personnelles inscrites dans les dossiers médicaux du patient permet de discerner les droits qui lui sont véritablement reconnus à leur égard. Seulement, les droits consacrés par le RGPD et leurs conditions d'exercice s'entendent de façon générique eu égard à la base légale du traitement¹⁶⁶. Certainement, les règles de droit commun du RGPD ne tiennent pas compte des spécificités inhérentes à la nature des données traitées, ni au domaine dans lequel leur traitement intervient. Par suite, l'articulation des droits conférés par le RGPD avec le droit de la santé et les spécificités de la donnée médicale exige des compromissions. Il en résulte que l'application des dispositions du droit de la santé et les caractéristiques de la donnée médicale tendent à restreindre la portée des droits du

¹⁶³ Cf. Paragraphe 20.

¹⁶⁴ Article 5 du RGPD.

¹⁶⁵ Article 5.1 c) du RGPD.

¹⁶⁶ Cf. Paragraphe 33.

patient sur les éléments immatériels de son corps humain contenus dans ses dossiers médicaux (**Chapitre 2**).

Chapitre 1 :

Les contours des données personnelles colligées dans les dossiers médicaux du patient

45. Toute donnée médicale recueillie et produite à l'occasion de la prise en charge sanitaire du patient doit être impérativement formalisée au sein de ses dossiers médicaux. Toutefois, comme l'a justement remarqué Dominique Giocanti, il existe un certain nombre de termes renvoyant à différentes sortes de dossiers médicaux, répondant eux-mêmes à des utilités, des logiques, des formes et des règles juridiques différentes¹⁶⁷. Compte tenu du principe de minimisation des données¹⁶⁸, les informations médicales incluses dans ces différents dossiers doivent donc être distinguées en fonction de leur pertinence au regard des objectifs respectivement poursuivis par les différents dossiers médicaux dont le patient est titulaire. Dans l'intention de lever la confusion entourant le terme général de « dossier médical », il paraît opportun de différencier les dossiers de soins constitués à l'occasion de la prise en charge médicale¹⁶⁹, des dossiers numériques supplémentaires participant à la coordination des soins. A cet effet, il convient de périmétrer les catégories de données médicales consignées au sein des dossiers de soins constitués à l'initiative des établissements et des professionnels de santé d'une part (**Section 1**) ; et de caractériser les catégories de données médicales renseignées au sein du DMP d'autre part (**Section 2**). Afin de préciser la sémantique utilisée tout au long de ces travaux, le terme « dossiers médicaux » englobera tant les dossiers de soins que le Dossier Médical Partagé.

¹⁶⁷ GIOCANTI (D.), *Les différentes acceptions des termes "dossier médical" et, dans ce contexte, situation du dossier hospitalier*, RGDM, 2010, n° 37, p. 164.

¹⁶⁸ Article 5.1 c) du RGPD.

¹⁶⁹ S'il convient de distinguer les dossiers de soins du dossier médical partagé, il est important de préciser que les dossiers de soins sont majoritairement informatisés.

Section 1 : Les dossiers de soins constitués à l'initiative des professionnels et des établissements de santé

46. Les données médicales du patient sont principalement générées par les professionnels de santé à l'occasion de la dispensation d'actes de prévention, de diagnostic et de soins. En d'autres termes, la prise en charge sanitaire du patient constitue une source de production de données médicales (**Paragraphe 1**). Une fois recueillies et produites, l'ensemble de ces données doivent être intégrées au sein des dossiers de soins du patient : celui conçu par les établissements de santé et celui créé par les professionnels de santé exerçant à titre individuel (**Paragraphe 2**).

Paragraphe 1 : Les données médicales générées lors de la prise en charge médicale du patient

47. Les données médicales du patient sont recueillies et produites, à différents niveaux, par l'ensemble des professionnels intervenant dans le système de santé, en secteur public comme en secteur privé, en médecine hospitalière comme en médecine de ville. En premier lieu, les données médicales collectées par les professionnels intervenant dans le parcours de soins sont directement fournies par le patient lui-même. Autrement dit, le patient est d'abord observé comme l'informateur des données relatives à sa santé, alors recueillies par les professionnels intervenant dans le cadre de sa prise en charge sanitaire (**A**). En second lieu, les données médicales du patient sont produites, au cours de la prise en charge médicale, par les professionnels débiteurs des services de soins de santé. Dans cette hypothèse, le patient constitue une source de production d'éléments médicaux immatériels. Ces données, issues de la pratique médicale, peuvent être qualifiées de données cliniques et, le cas échéant, de données génétiques (**B**). L'ensemble des données médicales nécessaires à la prise en charge sanitaire du patient, bien qu'elles ne présentent pas le même degré d'intimité, sont toutes de nature extrêmement sensible. La notion de donnée de santé apparaît donc comme une grande catégorie de données à caractère personnel, subdivisée en sous-groupe de données médicales et génétiques dont la sensibilité est toujours avérée.

A) Les données médicales recueillies auprès du patient

48. Tout accès au système de santé repose initialement sur les données de santé fournies par le patient ou, lorsqu'il se trouve hors d'état de s'exprimer, par un tiers. Traduites en données médicales, ces éléments permettent d'orienter et de contextualiser la prise en charge sanitaire qui s'ensuivra.

49. En premier lieu, les informations médicales du patient peuvent être déduites ou recueillies au moment de la prise du rendez-vous médical auprès d'un secrétariat idoine ou du professionnel de santé concerné. En effet, les informations collectées lors de l'inscription du patient en vue de bénéficier de services sanitaires sont déjà considérées comme des informations concernant la santé¹⁷⁰, voire comme des données médicales. Tel est notamment le cas lorsque le secrétaire médical interroge le patient sur le motif de la consultation, le traduit techniquement en des termes médicaux et oriente ainsi un diagnostic potentiel. Toutefois, eu égard au principe de minimisation des données, seules les informations strictement pertinentes et nécessaires à la prise du rendez-vous médical ne peuvent être collectées. C'est pourquoi le Conseil national de l'Ordre des médecins (CNOM) et la CNIL recommandent qu'aucune information relative à la santé du patient ne soit renseignée lorsque « *la consultation ne nécessite pas de préparation au préalable ou la réservation d'outils spécifiques* »¹⁷¹. Bien entendu, la finalité de la prise d'un rendez-vous médical consiste à planifier l'agenda du professionnel de santé en attribuant des créneaux de rendez-vous médicaux à des patients identifiés. A moins que la consultation sanitaire exige la mise en place d'un dispositif particulier, le motif du rendez-vous médical ne devrait donc pas être communiqué à ce stade de la prise en charge du patient.

Au demeurant, l'unique information relative à la consultation d'un professionnel de santé constitue, à elle seule, une donnée intime pouvant conduire à des discriminations à l'encontre du patient concerné. L'information relative à la prise d'un rendez-vous médical peut sembler anodine lorsqu'un individu consulte occasionnellement un médecin généraliste. Cette seule information ne permet pas de présupposer l'état de santé de l'intéressé.

¹⁷⁰ Considérant 35 du RGPD.

¹⁷¹ CNOM, CNIL, *Guide pratique sur la protection des données personnelles*, juin 2018, p. 13. Disponible sur le site [www.cnil.fr]. Consulté le 1^{er} décembre 2021.

Assurément, tout à chacun est amené à consulter un médecin généraliste : le patient en excellente santé pour l'obtention d'un certificat médical d'aptitude à une compétition sportive, le patient ayant contracté un virus saisonnier ou encore le patient atteint d'une blessure musculaire accidentelle. Dès lors, son éventuelle divulgation n'engendrerait que peu de risque pour sa vie privée dans la mesure où cette information, n'étant que peu révélatrice, n'est pas véritablement exploitable à son encontre. Néanmoins, dans certains cas, la simple information d'un rendez-vous médical suffit à insinuer des informations relatives à la santé du patient. La régularité des rendez-vous chez un médecin généraliste comme la ponctualité d'une consultation chez un médecin spécialiste laissent présumer que le patient concerné souffre de problèmes de santé spécifiques. La révélation de ces consultations médicales pourrait fonder des décisions discriminatoires à l'encontre de l'intéressé. Par exemple, si préalablement à un recrutement, un employeur avait connaissance qu'une candidate consultait un médecin spécialisé en reproduction, il pourrait écarter sa candidature alors même qu'elle ne se trouverait pas en état de grossesse. Dans cette situation, la femme qui n'est pas enceinte, mais qui cherche à procréer, se trouve moins bien protégée que la femme en état de grossesse. D'une part, la femme qui candidate à un emploi n'est pas tenue de révéler son état de grossesse¹⁷². D'autre part, quand bien même l'employeur en avait connaissance, il lui serait interdit de prendre l'état de grossesse en considération pour refuser de l'embaucher¹⁷³. Bien qu'elle ne constitue pas une donnée médicale au sens de la présente étude, la révélation de l'information portant sur une consultation sanitaire¹⁷⁴ permet d'inférer un état de santé passé, présent ou à venir, pouvant porter atteinte aux droits et libertés du patient concerné.

50. En second lieu, les données médicales du patient sont générées par les professionnels de santé au cours de la consultation sanitaire. Que la prise en charge soit effectuée en présentiel ou à distance au moyen des technologies de l'information et de la communication, tout examen clinique doit débiter par un interrogatoire conduit par le professionnel de

¹⁷² Article L.1225-2 du code du travail.

¹⁷³ Article L.1225-1 du code du travail.

¹⁷⁴ Il convient d'englober toutes sortes de consultations d'ordre sanitaire : médicales, chirurgicales, dentaires, maïeutiques, etc.

santé¹⁷⁵. En amont de tout examen physique ou complémentaire, il lui appartient de recueillir les informations notamment relatives au motif de la consultation, aux symptômes ressentis, aux antécédents médicaux, chirurgicaux, allergiques et familiaux, aux traitements pharmaceutiques, à l'histoire de la maladie, ou encore, au mode de vie du patient. L'ensemble de ces informations est directement collecté par le professionnel de santé auprès du patient ou de son représentant légal, oralement ou à l'aide d'un questionnaire remis à la personne concernée. Ces informations brutes, formulées par le patient, sont traduites en des termes médicaux et consignées au sein de l'observation médicale rédigée par le professionnel de santé : elles deviennent des données médicales. C'est alors que l'observation médicale doit être implémentée dans le dossier de soins du patient. Ces éléments immatériels aident à l'orientation de l'examen clinique et à l'établissement du diagnostic médical. Les données médicales recueillies auprès du patient présentent ainsi un caractère fondamentalement utile et particulièrement sensible.

B) Les données médicales produites par les professionnels de santé

51. Après avoir recueilli l'ensemble de ces renseignements, le professionnel de santé produit des données médicales au cours de l'examen physique du patient. A cette occasion, il reporte les données biologiques qu'il constate par le geste médical, ou qu'il relève au moyen d'un dispositif médical (thermomètre, tensiomètre, etc.), au sein de l'observation médicale intégrée dans le dossier de soins du patient. Lorsque la prise en charge a lieu à distance, notamment lors d'une téléconsultation de télésanté, l'examen physique peut être effectué au moyen de dispositifs médicaux connectés dont les mesures de biométrie médicale sont envoyées au téléconsultant. A titre d'exemple, les cabines de téléconsultation médicale¹⁷⁶ comportent différents instruments de mesure connectés dont une balance et une toise, un oxymètre, un stéthoscope ou encore un électrocardiogramme. Ces informations, converties en données médicales, retranscrivent une condition clinique et biologique provenant directement du corps humain du patient. Il en advient que ces données cliniques

¹⁷⁵ La sémiologie médicale consiste en l'étude des signes cliniques relevés à l'occasion de l'examen clinique du patient. L'examen clinique se déroule en deux étapes : d'abord par l'interrogatoire, ensuite par l'examen physique du patient.

¹⁷⁶ La téléconsultation médicale est un acte de télémédecine défini à l'article R.6316-1 1° du code de la santé publique comme l'acte médical « qui a pour objet de permettre à un professionnel médical de donner une consultation à distance à un patient ».

constituent la retranscription de la physiologie propre à une personne. Elles tendent à formaliser, en une information concrète, une condition physique intrinsèque et naturelle de la personne humaine. En conséquence, les données médicales issues de la pratique clinique touchent au plus profond de l'intimité du patient et se trouvent profondément attachées à la personne de laquelle elles sont issues.

52. Outre la retranscription d'éléments physiques effectués par le professionnel de santé, les données médicales du patient peuvent directement provenir d'une substance corporelle. En effet, les données médicales peuvent être produites à l'occasion de l'analyse d'échantillons biologiques humains tels que du sang, des fluides, des tissus et cellules, des micro-organismes, etc. Les résultats biologiques des éléments du corps humain, prélevés par culture, biopsie ou frottis sur le patient, sont indubitablement des données médicales. De surcroît, ces éléments humains peuvent être examinés comme des données « *relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique* »¹⁷⁷ dès lors que leur analyse porte sur « *des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou [...] d'un autre élément permettant d'obtenir des informations équivalentes* »¹⁷⁸. Bien que toute donnée médicale ne constitue pas forcément une donnée génétique, à l'inverse, toute donnée génétique constitue une donnée médicale ou, à tout le moins, une donnée de santé. A l'évidence, les données génétiques « *donnent des informations uniques sur la physiologie ou l'état de santé* »¹⁷⁹ de la personne concernée. Les données médicales résultant des échantillons biologiques prélevés sur le patient apparaissent donc singulièrement intimes. A ce titre, elles mériteraient une protection équivalente au principe à valeur constitutionnelle de sauvegarde de la dignité du corps humain¹⁸⁰. Plus généralement, les données médicales, en raison de leur origine, pourraient être soumises à un régime juridique analogue à celui concédé aux éléments du corps humain qu'elles retranscrivent¹⁸¹.

53. Par ailleurs, les données médicales peuvent être produites à l'image du corps humain du patient. Ainsi, les photographies prises à l'occasion d'un acte de soins de santé et les

¹⁷⁷ Considérant 34 du RGPD.

¹⁷⁸ *Ibid.*

¹⁷⁹ CNIL, *Les données génétiques*, La documentation française, 6 septembre 2017, présentation.

¹⁸⁰ Cons. Const., décision n°94-343/344 DC du 27 juillet 1994.

¹⁸¹ Cf. Paragraphe 357.

clichés d'un examen d'imagerie médicale sont à compter parmi cette sous-catégorie de données de santé. Assurément, ces représentations reflètent littéralement le corps humain du patient et conduisent à l'élaboration des diagnostics médicaux, voire à des pronostics vitaux.

54. Il résulte qu'en matière de prise en charge médicale, les sources de production des données médicales sont variées et invariablement sensibles. Que les données médicales soient peu ou prou intimes, il n'en demeure pas moins qu'elles sont toutes, quel que soit leur niveau, profondément attachées à la vie intime du patient et potentiellement discriminantes. C'est pourquoi, le traitement des données médicales recueillies et produites à l'occasion de l'examen clinique du patient doit être explicitement et légitimement nécessaire à sa prise en charge sanitaire¹⁸². De surcroît, en tant qu'opérations de traitement à part entière, le recueil et la production des données médicales à l'occasion de l'examen clinique du patient doivent être limités à ce qui apparaît nécessaire à sa prise en charge sanitaire¹⁸³. Force est d'observer que la prise en charge sanitaire constitue, à titre dérogatoire, une autorisation de traitement des données médicales du patient¹⁸⁴. Si le législateur européen autorise exceptionnellement le traitement des données médicales du patient pour cette finalité, c'est parce que toute prise en charge médicale suppose que les informations médicales du patient soient d'abord collectées, puis analysées et traitées par des professionnels de santé. De toute évidence, n'importe quel professionnel de santé ne peut prévenir une pathologie, établir un diagnostic, dispenser des soins ou encore prescrire une thérapeutique qu'en se fondant sur les données médicales, propres à chaque patient, qu'il aura générées au cours de l'examen clinique et des examens paracliniques.

55. En raison de leur nature infiniment sensible et confidentielle, les données médicales du patient doivent faire l'objet d'une sécurisation matérielle par la mise en œuvre de mesures techniques et organisationnelles par le responsable de traitement¹⁸⁵ et, le cas échéant, son sous-traitant¹⁸⁶. Cette sécurisation matérielle doit prioritairement passer par la formalisation et l'intégration des données médicales du patient au sein d'un dossier de soins qui lui est

¹⁸² Article 5.1 b).

¹⁸³ Article 5.1 c) du RGPD.

¹⁸⁴ Article 9.2 h) du RGPD.

¹⁸⁵ Articles 25 et 32 du RGPD.

¹⁸⁶ Article 28 du RGPD.

rattaché. Par essence, un dossier de soins peut donc être considéré comme un dispositif de sécurisation des données médicales du patient, à condition bien-sûr que la constitution de ce dossier, en tant que traitement de données sensibles, réponde à l'ensemble des mesures de protection édictées par le RGPD. Ces éléments immatériels doivent donc être structurés et intégrés dans des fichiers manuscrits ou numérisés appelés « dossiers médicaux » et élaborés conformément au droit à la protection des données personnelles. Certainement, la constitution et l'alimentation d'un dossier médical constitue un traitement de données personnelles confidentielles.

Paragraphe 2 : L'intégration des données médicales du patient au sein d'une pluralité de dossiers de soins

56. Toute donnée médicale ne peut avantageusement être stockée qu'au sein d'un dossier éponyme. D'une part, le regroupement des informations médicales du patient au sein d'un dossier constitué à son effigie lui offre une réelle visibilité sur l'emplacement réel de ses informations immatérielles. D'autre part, cette formalisation permet de réduire les risques d'identitovigilance et, pour le professionnel de santé, d'assurer un suivi et une continuité dans la prise en charge médicale du patient. Cependant, il n'en demeure pas moins qu'en pratique, les données médicales attachées à un même patient peuvent être disséminées à travers une multitude de supports papiers ou numérisés. Face à cette obscurité, comment s'assurer qu'elles sont effectivement reportées au sein d'un dossier *ad hoc* ? Pour répondre à cette interrogation, encore faut-il déterminer les dossiers de soins existants, ainsi que le périmètre des données devant y être intégrées. Deux typologies de dossiers de soins constitués à l'occasion de toute prise en charge médicale sont communément utilisées : le dossier médical hospitalier constitué par les établissements de santé (**A**) et les fiches d'observation personnelles tenues par le médecin (**B**). Au cœur de ces dossiers, ne seront pas formalisées l'entièreté des données issues de la télésanté (**C**), ni les notes personnelles prises par le professionnel de santé (**D**).

A) *Le dossier médical hospitalier*

57. Alors que le contenu du premier dossier hospitalier a été déterminé par un décret du 30 mars 1992¹⁸⁷, les députés chargés d'étudier le projet de loi relatif aux droits des malades et à la qualité du système de santé avaient constaté que le contenu et la qualité des dossiers médicaux hospitaliers demeuraient variables d'un établissement de santé à l'autre¹⁸⁸. Malgré l'élargissement progressif du contenu minimal du dossier hospitalier, son périmètre actuel reste toujours incertain. Si le dossier médical hospitalier, constitué pour toute personne prise en charge dans un établissement de santé, doit tout au moins contenir les éléments énumérés à l'article R.1112-2 du code de la santé publique, un dossier de soins ne peut être ni exhaustif, ni restrictif.

58. D'abord, le dossier médical hospitalier doit être constitué d'une première partie regroupant l'ensemble des données médicales générées au cours du séjour hospitalier ou lors des consultations médicales externes dispensées au sein de l'établissement de santé¹⁸⁹. Le pouvoir exécutif a spécifié que ce premier volet devait comporter : la lettre du médecin qui est à l'origine de la consultation ou, en cas d'admission, la lettre de liaison¹⁹⁰ ; les motifs d'hospitalisation ; la recherche d'antécédents et de facteurs de risques ; les conclusions de l'évaluation clinique initiale ; le type de prise en charge prévu et les prescriptions effectuées à l'entrée ; la nature des soins dispensés et les prescriptions établies lors de la consultation externe ou du passage aux urgences ; les informations relatives à la prise en charge en cours d'hospitalisation : état clinique, soins reçus, examens para-cliniques, notamment d'imagerie ; les informations sur la démarche médicale ; le dossier d'anesthésie ; le compte rendu opératoire ou d'accouchement ; le consentement écrit du patient pour les situations où il est requis sous cette forme ; la mention des actes transfusionnels pratiqués sur le patient et, le cas échéant, la copie de la fiche d'incident transfusionnel ; les éléments relatifs à la prescription médicale, à son exécution et aux examens complémentaires ; le dossier de soins

¹⁸⁷ Décret n°92-329 du 30 mars 1992 relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santé publics et privés et modifiant le code de la santé publique.

¹⁸⁸ EVIN (C.), CHARLES (B.), DENIS (J.-J.), *Rapport n°3263 fait au nom de la commission des affaires culturelles, familiales et sociales sur le projet de loi relatif aux droits des malades et à la qualité du système de santé n°3258*, Assemblée Nationale, Vol. I, Titre 1^{er} Démocratie sanitaire, 26 septembre 2001, p. 31.

¹⁸⁹ Article R.1112-2 1° du code de la santé publique.

¹⁹⁰ Cf. Paragraphe 295.

infirmiers ou, à défaut, les informations relatives aux soins infirmiers ; les informations relatives aux soins dispensés par les autres professionnels de santé ; les correspondances échangées entre professionnels de santé ; et les directives anticipées ou, le cas échéant, la mention de leur existence ainsi que les coordonnées de la personne qui en est détentrice¹⁹¹. Ensuite, au sein d'une deuxième partie, le dossier médical hospitalier doit rassembler, les données médicales établies à la fin du séjour, dont la lettre de liaison remise à la sortie du patient¹⁹² ; la prescription de sortie et les doubles d'ordonnance de sortie ; les modalités de sortie en cas d'hospitalisation (domicile, autres structures) ; ainsi que la fiche de liaison infirmière¹⁹³. Finalement, dans un troisième volet, le dossier médical hospitalier doit réunir les informations relatives à la santé du patient qui ont été recueillies auprès de tiers n'intervenant pas dans sa prise en charge sanitaire ainsi que les éventuelles informations médicales concernant les tiers¹⁹⁴.

59. Le périmètre du dossier médical hospitalier, ainsi délimité par les dispositions de l'article R.1112-2 du code de la santé publique, n'est pas restrictif mais extensif. En effet, la lettre de cette disposition réglementaire indique que « *ce dossier contient au moins les éléments* » susmentionnés. Bien qu'il semble considérable, ce regroupement des données médicales et de santé ne constitue que le contenu minimal du dossier médical hospitalier. Cela signifie que ce fichier peut consigner des informations et documents supplémentaires à ceux inventoriés par le pouvoir exécutif. Pour autant, toute donnée personnelle relative au patient ne doit être incluse au sein de ce dossier. En effet, les mesures de protection des données à caractère personnel impliquent de minimiser les données faisant l'objet d'un traitement. Si toute donnée médicale ne peut inmanquablement être insérée qu'au sein d'un dossier médical, seules les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la prise en charge sanitaire du patient peuvent y être implémentées. En conséquence, toute information personnelle pertinente pour la prise en charge sanitaire du patient peut être reportée dans son dossier médical hospitalier, quand bien même elle ne saurait appartenir à la grande catégorie des données concernant la santé. Dans le respect du

¹⁹¹ *Ibid.*

¹⁹² *Cf.* Paragraphe 295.

¹⁹³ Article R.1112-2 2° du code de la santé publique.

¹⁹⁴ *Cf.* Paragraphes 241 à 250.

principe de minimisation des données¹⁹⁵, toute information familiale, sexuelle, raciale ou encore professionnelle pourrait donc être colligée au sein du dossier médical hospitalier du patient si tant est qu'elle se révèle nécessaire à la finalité du traitement, à savoir, sa prise en charge sanitaire. Au surplus des données médicales, le dossier d'un patient peut contenir des données ne relevant pas du champ de la santé. Le périmètre des données incluses dans le dossier médical hospitalier est donc à la fois étendu et limité à toutes données absolument nécessaires à la prise en charge sanitaire du patient et, particulièrement, à la production des services de soins de santé.

60. Outre ces données sanitaires, l'article R.1112-3 du code de la santé publique annonce que « *le dossier comporte l'identification du patient* ». Dans une instruction du 7 juin 2013, la Direction générale de l'offre de soins (DGOS) a indiqué que « *le recueil de l'identité est l'une des toutes premières étapes de la prise en charge du patient* »¹⁹⁶. Cette identification doit être observée comme un dispositif de sécurité et de qualité de la prise en charge médicale, mais aussi comme une mesure de protection des données à caractère personnel. Préalablement à la formalisation des éléments immatériels du patient dans son dossier médical hospitalier, le professionnel de santé doit vérifier l'adéquation entre son identité et le dossier qui lui est rattaché. Afin d'éviter que deux patients homonymes puissent présenter la même identité, la DGOS considère que les traits stricts d'identification permettant d'identifier le plus sûrement une personne physique sont le nom de naissance, éventuellement le nom usuel, la date de naissance et le sexe¹⁹⁷. La définition des traits d'identification des patients par les établissements de santé doit être précisée au sein de leur politique d'identitovigilance et, spécifiquement, au sein des procédures d'identification et de rapprochement des identités¹⁹⁸. Cette démarche vise à prévenir les risques sanitaires et les évènements indésirables pour la santé du patient consécutifs à une erreur liée à son identification. Effectivement, l'identitovigilance peut être définie comme « *un dispositif permanent et systémique de surveillance, de détection, d'alerte, de correction, de prévention*

¹⁹⁵ Article 5.1 c) du RGPD.

¹⁹⁶ Instruction DGOS/MSIOS n°2013-281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins, Bulletin officiel Santé, Protection sociale, Solidarité n°2013/8, 15 septembre 2013.

¹⁹⁷ *Ibid.*

¹⁹⁸ DGOS, *Programme Hôpital numérique. Boîte à outils pour l'atteinte des pré-requis – Fiches pratiques*, Fiche pratique n°1, octobre 2012, p. 7 à p. 14. Disponible en ligne sur le site [solidarites-sante.gouv.fr]. Consulté le 1^{er} décembre 2021.

des risques et des erreurs liés au processus d'identification des patients »¹⁹⁹. Cette démarche vise également à prévenir les violations des données personnelles caractérisées par la perte de leur confidentialité. Assurément, la fiabilité de l'identification des dossiers médicaux hospitaliers permet alors d'éviter qu'un patient accède à des données personnelles qui ne le concernent pas²⁰⁰.

61. En complément de son identification, les données administratives du patient devraient contenir ses coordonnées. Dans le contexte de l'obligation d'information des risques liés à l'acte médical ou paramédical, les dispositions de l'article L.1111-2 du code de la santé publique énoncent que « *lorsque, postérieurement à l'exécution des investigations, traitements ou actions de prévention, des risques nouveaux sont identifiés, la personne concernée doit en être informée [par le professionnel de santé], sauf en cas d'impossibilité de la retrouver.* ». De la même manière, « *les médecins hospitaliers sont tenus de communiquer aux patients les informations, concernant leur état de santé, dont ils ont eu connaissance après leur sortie* »²⁰¹. Pour parvenir à ces fins, le dossier médical hospitalier devrait indispensablement comporter les informations permettant de situer et de contacter le patient. A ce titre, devraient être collectés son adresse postale, son adresse électronique et son numéro de téléphone. En effet, seule l'impossibilité de retrouver le patient permet d'exonérer les professionnels de santé de l'obligation précitée²⁰². Seulement, pour tenter de retrouver une personne, encore faut-il posséder ses coordonnées. A défaut, cette abstention peut constituer une faute de nature à engager la responsabilité du service hospitalier et engendrer une perte de chance de guérison pour le patient²⁰³. Par ailleurs, le renseignement des coordonnées du patient apparaît indispensable à la délivrance de l'information individuelle préalable à l'éventuelle réutilisation de ses données médicales à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé²⁰⁴.

¹⁹⁹ WEKA, *L'identitovigilance*, Fiche pratique n°6927. Disponible en ligne sur le site [www.weka.fr]. Consulté le 06 avril 2020.

²⁰⁰ Cf. Paragraphe 196.

²⁰¹ CE, 2 septembre 2009, n°292783, *M^{me} Peignien*, Rec. Lebon T. ; D., 2009, n° 34, p. 2283, C. De Gaudemont ; ADJA, 2009, n° 29, p. 1581, C. Biget ; RDSS, 2010, n° 01, p. 104, note F. Dieu.

²⁰² *Ibid.*

²⁰³ *Ibid.*

²⁰⁴ Cf. Paragraphes 487 s.

B) Les fiches d'observation personnelles

62. Indépendamment des dossiers médicaux hospitaliers, l'article 45 du code de déontologie médicale prévoit que tout médecin doit tenir « *pour chaque patient une fiche d'observation qui lui est personnelle* ». Compte tenu de la portée juridique des dispositions du code de déontologie médicale²⁰⁵, chaque médecin devrait constituer une fiche d'observation personnelle à chaque patient. Les données médicales du patient, recueillies et produites lors de son examen clinique par tout médecin exerçant en milieu hospitalier, en groupement, ou à titre individuel, devraient donc être reportées au sein d'une fiche d'observation. Cela signifie que les données médicales du patient pris en charge au sein d'un établissement de santé devraient être colligées dans son dossier médical hospitalier, mais également au sein des fiches d'observation tenues par chacun des médecins l'ayant pris en charge. Néanmoins, en pratique, la fiche d'observation personnelle constitue exclusivement le dossier de soins du médecin exerçant en dehors du secteur hospitalier. La fiche d'observation personnelle doit donc être distinguée des notes personnelles prises par le médecin, lesquelles ne peuvent comporter aucun élément relatif aux décisions diagnostiques et thérapeutiques²⁰⁶.

63. Contrairement au dossier médical hospitalier, la fiche d'observation personnelle n'est soumise à aucun formalisme, ni à aucun contenu minimal. Les dispositions déontologiques indiquent seulement que toute fiche d'observation doit comporter « *les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques* »²⁰⁷. De la même façon, un fichier comportant l'ensemble des informations de santé nécessaires aux *décisions diagnostiques et thérapeutiques* doit être constitué pour chaque patient pris en charge dans un centre de santé²⁰⁸. Lorsque le patient est pris en charge dans une structure de santé non hospitalière, la fiche d'observation personnelle prend ainsi la forme d'un dossier commun à l'ensemble des professionnels de santé y exerçant. Il en résulte que « *la traçabilité des actions effectuées*

²⁰⁵ Les dispositions du code de déontologie médicale s'appliquent à tout médecin quel que soit son mode d'exercice.

²⁰⁶ Cf. Paragraphe 72.

²⁰⁷ Article R.4127-45 du code de la santé publique.

²⁰⁸ Article D.6323-5 alinéa 1 du code de la santé publique

dans le cadre de la prise en charge de chaque patient »²⁰⁹ tend à garantir la coordination de son parcours de santé dans le périmètre d'une telle structure.

64. L'absence de formalisme et de structuration des fiches d'observation personnelles ne permet pas d'assurer que l'ensemble des données médicales relatives à un patient pris en charge par un médecin y soit bien reporté. Même si ces fiches peuvent comporter toutes données personnelles adéquates, pertinentes et limitées à ce qui est nécessaire à la prise en charge sanitaire du patient, seules les informations minimisées à cette finalité doivent, pour le moins, y être intégrées. Alors que la fiche d'observation personnelle constitue le dossier de soins du patient pris en charge en médecine de ville, son contenu minimum semble modique par rapport à celui du dossier médical hospitalier. De surcroît, la pratique révèle que les médecins généralistes n'alimentent pas systématiquement les fiches d'observation personnelles – et donc les dossiers de soins – de leurs patients. Ces carences représentent une source de risque tant pour la prise en charge médicale du patient, que pour la protection de ses données personnelles et des droits qu'il détient sur celles-ci. Où les données médicales du patient seraient-elles importunément stockées si elles n'étaient pas retranscrites au sein de sa fiche d'observation personnelle, au demeurant conçue dans le respect du droit à la protection des données personnelles ? Comment pourrait-il y accéder ? Aucun élément ne permet, au patient concerné, de vérifier l'emplacement de données dispersées ou égarées. Pour autant, à l'exemple de la télésurveillance médicale²¹⁰, toute donnée médicale ne doit pas systématiquement être implémentée dans le dossier de soins du patient. Certainement, seules les informations pertinentes et limitées à ce qui est nécessaire à la prise en charge sanitaire du patient peuvent y être insérées. A défaut, la donnée médicale doit être détruite²¹¹.

C) La formalisation des données médicales générées à l'occasion de la télésanté

65. La télésanté, qui correspond aux services sanitaires délivrés au moyen des technologies de l'information et de la communication, est composée de la télémedecine et du télésoin. Tandis que « *le télésoin est une forme de pratique de soins à distance* »²¹², « *la*

²⁰⁹ Article D.6323-5 alinéa 3 du code de la santé publique.

²¹⁰ Cf. Paragraphe 67.

²¹¹ Cf. Paragraphe 145.

²¹² Article L.6316-1 du code de la santé publique.

télé médecine est une forme de pratique médicale à distance »²¹³ composée de cinq actes : la téléconsultation qui permet au médecin de donner une consultation à distance, la téléexpertise qui permet au médecin de s'enquérir de l'avis d'un professionnel médical spécialisé, la télésurveillance médicale qui permet le suivi du patient par l'interprétation de ses données de santé recueillies *via* un dispositif médical, la téléassistance médicale qui permet à un médecin d'assister un autre médecin dans la réalisation d'un acte, et la réponse médicale qui est apportée dans le cadre de la régulation médicale²¹⁴.

Même si la dispensation des actes sanitaires en présentiel requiert l'analyse des données médicales tout au long de la prise en charge du patient, la télé médecine repose davantage sur la transmission et la circulation de celles-ci. Quel que soit le type d'acte de télé médecine, les données médicales du patient, qui se trouve à distance du médecin, doivent lui parvenir au moyen d'un dispositif de télécommunication. C'est pourquoi tout acte de télé médecine doit être réalisé dans des conditions garantissant l'accès des professionnels médicaux aux données médicales nécessaires à la réalisation de cet acte²¹⁵. Assurément, la télé médecine repose d'abord sur la collecte des données médicales du patient, puis sur leur transmission au médecin intéressé. Aussi, comme tout acte médical, les actes de télé médecine sont une source de production de données médicales. Par suite, ces éléments immatériels recueillis ou produits à cette occasion doivent être colligés au sein du dossier de soins du patient.

66. En ce sens, les dispositions réglementaires encadrant les conditions de réalisation des actes de télé médecine imposent d'intégrer, dans le dossier de soins du patient, des éléments relatifs à cette forme de pratique médicale à distance. En vertu de l'article R.6316-4 du code de la santé publique, le compte rendu de la réalisation de l'acte, les prescriptions médicamenteuses effectuées dans le cadre de l'acte de télé médecine, l'identité des professionnels de santé participant à l'acte, la date et l'heure de l'acte et, le cas échéant, les incidents techniques survenus au cours de l'acte doivent être distinctement consignés dans le dossier de soins du patient ; en l'occurrence le dossier médical hospitalier ou la fiche d'observation personnelle. Il en advient que le dossier de soins du patient doit, le cas échéant,

²¹³ Article L.6316-2 du code de la santé publique.

²¹⁴ Article R.6316-1 du code de la santé publique.

²¹⁵ Article R.6316-3 du code de la santé publique.

contenir un volet spécifique à la télésanté. Si la liste des éléments spécifiques à la télémédecine semble être impérative et exhaustive, aucune disposition n'interdit d'y intégrer des données supplémentaires au périmètre défini par l'article susvisé. A moins qu'elle ne fasse l'objet d'une suppression, toute donnée médicale générée lors de la dispensation d'un acte de télésanté ne peut être conservée qu'au sein d'un dossier de soins.

67. En matière de télémédecine, la question de l'intégration des données médicales du patient dans son dossier de soins se pose particulièrement pour la télésurveillance médicale. En effet, la télésurveillance médicale consiste en l'interprétation, à distance, des données nécessaires au suivi médical du patient. Dans ce contexte, les données médicales du patient sont généralement recueillies par un dispositif médical connecté, parfois analysées par un algorithme générant des alertes paramétrables en fonction d'une norme de référence, et transmises au médecin chargé de suivre le patient.

Par exemple, en matière de télésurveillance glycémique, l'intégralité des mesures du taux de glucose propres à un patient peuvent être enregistrées sur une plateforme web, *via* un glucomètre connecté, à laquelle le médecin a accès pour l'interprétation des données médicales et le suivi du patient. Cette plateforme web, bien qu'elle collecte les données glycémiques du patient, ne constitue pas un dossier médical. En effet, il s'agit seulement d'un logiciel qualifié de dispositif médical, d'un moyen permettant la réalisation de l'acte de télésurveillance médicale. La question qui se pose est de savoir si l'ensemble des données médicales, recueillies quotidiennement pour chaque patient, doivent être enregistrées au sein de son dossier médical hospitalier ou de sa fiche d'observation personnelle ? Il convient de préciser que des centaines de mesures concernant le taux de glucose des patients inclus par un même médecin sont générées quotidiennement par la télésurveillance glycémique. En pratique, la formalisation et l'intégration journalière de ces quantités de données médicales dans les dossiers de soins peut rapidement s'avérer irréalisable. Pourtant, il est nécessaire de rappeler que les données médicales du patient ne peuvent être stockées qu'au sein d'un dossier idoine et ne doivent aucunement subsister sur une plateforme web. En solution, il paraît alors indispensable de filtrer les données glycémiques à consigner au sein du dossier de soins du patient. Assurément, il est concrètement impossible d'y intégrer l'intégralité des données produites dans ce cadre.

Afin de définir les données glycémiques à insérer dans le dossier de soins du patient télésurveillé, il convient d'appliquer le principe de minimisation des données²¹⁶. En conséquence, seules les données glycémiques pertinentes, adéquates et limitées à ce qui est nécessaire à la prise en charge médicale et au suivi du patient télésurveillé peuvent être traitées et introduites dans ce dossier. Parmi le nombre considérable de données glycémiques recueillies, seules les données qui ont justifié une action et une modification de la prise en charge médicale devraient donc être incluses dans le dossier médical hospitalier ou la fiche d'observation personnelle au patient télésurveillé. Quant aux autres données n'ayant pas de plus-value médicale, elles devraient faire l'objet d'une destruction dans la mesure où elles ne présentent aucune pertinence pour la prise en charge médicale du patient. Cette démonstration est évidemment duplicable pour tout acte de télésurveillance médicale et, plus largement, pour l'ensemble des actes de télémédecine et de télésoin.

68. Alors que la destruction des données médicales générées à l'occasion d'un acte de télémédecine constitue une obligation réglementaire lorsqu'elles n'apparaissent pas nécessaires à la finalité du traitement²¹⁷, cette suppression pourrait attenter à l'établissement de *la preuve* en matière de responsabilité médicale. En effet, dans un procès civil ou administratif, « *il incombe à chaque partie de prouver [...] les faits nécessaires au succès de sa prétention* »²¹⁸. Il appartient donc au patient victime d'un dommage consécutif à un acte de prévention, de diagnostic ou de soins, d'apporter la preuve de l'existence d'un préjudice, d'une faute et d'un lien de causalité entre les deux²¹⁹. De toute évidence, Dominique Chagnollaud De Sabouret atteste qu'il « *ne suffit pas d'alléguer des faits, encore faut-il prouver leur existence afin que s'établisse la certitude* »²²⁰. Si la preuve de ces trois conditions d'engagement de la responsabilité médicale peut être rapportée par tout moyen²²¹, le dossier de soins constitue l'ultime élément de preuve permettant de caractériser l'existence d'une faute médicale ou d'un aléa thérapeutique. Assurément, le juge recherche

²¹⁶ Cf. Paragraphe 43.

²¹⁷ Article 17.1 a) du RGPD.

²¹⁸ GUINCHARD (S.), DEBARD (T.), *Lexique des termes juridiques 2021-2022*, 29^e ed., Dalloz, août 2021, p. 819.

²¹⁹ Article 1240 du code civil.

²²⁰ CHAGNOLLAUD DE SABOURET (D.), *Dictionnaire élémentaire du droit*, 2^e ed., Dalloz, août 2016, p. 83.

²²¹ Article 1358 du code civil.

principalement leur caractérisation à travers les données formalisées dans le dossier de soins du patient. Si « *la preuve joue un rôle central en conditionnant le succès des prétentions des parties* »²²², le dossier de soins représente la pierre angulaire de la responsabilité médicale. La formalisation des données médicales du patient dans son dossier de soins permet donc de cristalliser l'existence de faits et, ainsi, d'en apporter la preuve. Seulement, comment apporter la preuve d'une éventuelle faute de télésurveillance médicale lorsque les données médicales générées par le dispositif médical connecté ont été jugées inutiles eu égard au principe de minimisation des données et, en conséquence, détruites ?

Selon l'adage latin *idem est non esse aut non probari*, ce qui n'existe pas ne peut être prouvé. Par suite, le patient victime d'une faute de télésurveillance médicale ne peut apporter la preuve de l'existence d'un indicateur biologique, clinique ou psychologique qui aurait nécessité une intervention médicale²²³ dès lors que le professionnel de santé a considéré que cet indicateur n'était pas pertinent dans le cadre de la télésurveillance médicale, et qu'il ne méritait pas d'être consigné dans son dossier de soins. Force est d'observer que l'interprétation subjective de ce principe essentiel de la protection des données personnelles comporte des écueils. Le principe de minimisation des données traitées à l'occasion d'un acte de télémédecine, *a fortiori* de télésurveillance médicale, pourrait conduire à supprimer toute trace d'élément pouvant fonder une décision médicale et, par conséquent, toute preuve d'une éventuelle faute médicale nécessaire à l'engagement de la responsabilité du professionnel de santé. Convient-il de privilégier le principe de minimisation des données au risque de laisser un préjudice sans réparation ? Ou faut-il privilégier la conservation de l'ensemble des données médicales générées à l'occasion d'un acte de télémédecine au risque de violer le droit à la protection des données ? Si Maryse Deguergue rappelle l'« *obligation d'ordre administratif* »²²⁴, pour les professionnels de santé, de tracer l'intervention de téléconsultation ou de télésurveillance dans le dossier du patient, nous attestons que seules les données ayant conduit à une décision médicale doivent être consignées dans le dossier de soins du patient²²⁵.

²²² CHAGNOLLAUD DE SABOURET (D.), *loc. cit.*

²²³ Arrêté du 4 octobre 2019 relatif à l'expérimentation de télésurveillance médicale des patients transplantés hépatiques, *JORF*, 12 octobre 2019.

²²⁴ DEGUERGUE (M.), *Télémédecine et responsabilités*, RDSS, 2 mars 2020, p. 33.

²²⁵ Cf. Paragraphe 72.

69. Le principe de minimisation des données de télémédecine étant favorisé²²⁶, comment le patient peut-il apporter la preuve d'une faute médicale et, plus particulièrement, de télésurveillance médicale ? S'il advient que le patient télésurveillé a subi un préjudice en lien avec la pathologie pour laquelle il était télésurveillé, et que ce préjudice pouvait être prévenu par l'interprétation des données médicales collectées par le dispositif médical connecté, une présomption simple de faute de télésurveillance médicale pourrait être instaurée. Au moyen d'une logique de probabilité, le mécanisme de la présomption permet de déduire un fait inconnu d'un fait connu²²⁷. Le patient serait alors dispensé de la charge probatoire d'un fait générateur dont l'existence s'avérerait matériellement inexistante. La charge probatoire pesant sur le professionnel de santé, il lui appartiendrait, pour se dédouaner, d'apporter la preuve de l'absence de faute médicale. Sans être circonscrit aux infections nosocomiales²²⁸, le mécanisme des présomptions de faute en matière de dommage médical est couramment employé tant par le juge civil que le juge administratif. En effet, Caroline Grossholz indique que « *le juge peut inférer la faute de la nature du dommage, de son caractère anormal, en estimant que sa survenance révèle qu'une faute a été commise, même si l'on ignore dans quelles circonstances* »²²⁹, qu'il s'agisse d'un défaut dans l'organisation et le fonctionnement du service ou d'un défaut dans l'exécution d'un acte de soins²³⁰.

Toutefois, l'éventuelle présomption d'une faute de télésurveillance médicale doit tenir compte des particularités inhérentes à l'interprétation, à distance, des données médicales des patients télésurveillés. Il convient de préciser que les téléprofessionnels de santé ne peuvent, à chaque instant, procéder à l'analyse des données et des alertes transmises quotidiennement par le dispositif médical connecté. Il apparaît indispensable que le service médical hospitalier, ou le médecin indépendant mettant en œuvre l'acte de télésurveillance, définisse une organisation relative à la gestion et à l'analyse des données de télémédecine. A

²²⁶ Cf. *supra*.

²²⁷ CHAGNOLLAUD DE SABOURET (D.), *op.cit.*, p. 84.

²²⁸ Voir : GROSSHOLZ (C.), *Hôpitaux : régimes de responsabilité et de solidarité. La responsabilité pour faute*, Répertoire de la responsabilité de la puissance publique, Dalloz, février 2018, actu. juin 2021, § 227 et § 228.

²²⁹ GROSSHOLZ (C.), *op. cit.*, § 229 ; CAA Paris, 24 mars 1998, n°96PA02373, *Assistance publique -Hôpitaux de Paris, M. B...*, Inédit Rec. Lebon ; Dr. adm. 1998, p. 292.

²³⁰ GROSSHOLZ (C.), *loc. cit.* ; CE, 12 octobre 1983, n°37768, *Mme Rolland et autres*, Rec. Lebon, 1983, p. 855 ; CE, 1^{er} mars 1989, n°67255, *Époux Peyres*, Rec. Lebon, 1989, p. 65.

cet effet, il s'avère indispensable de fixer et de délimiter des moments hebdomadaires dédiés à l'interprétation des données de télésurveillance médicale et d'en informer le patient intéressé. A titre d'exemple, selon la société française de cardiologie « *la prise de connaissance des alertes [de télésurveillance des dispositifs électroniques cardiaques implantables] devrait être quotidienne, idéalement le matin, afin d'éviter tout retard dans la gestion des problèmes* »²³¹. Compte tenu de ce qui précède, la présomption simple de faute de télémédecine ne jouerait que si le dommage médical se produisait dans un délai raisonnable consécutif aux moments d'analyse déterminés, postérieurement à la destruction des données médicales du patient télésurveillé.

70. La télésanté comporte également le télésoin. Introduit par la loi d'organisation et de transformation du système de santé du 24 juillet 2019, le télésoin « *est une forme de pratique de soins à distance utilisant les technologies de l'information et de la communication. Il met en rapport un patient avec un ou plusieurs pharmaciens ou auxiliaires médicaux dans l'exercice de leurs compétences* »²³². Les conditions de mise en œuvre du télésoin correspondent à celles encadrant les activités de télémédecine²³³. Il en advient que toute donnée médicale produite à l'occasion de la télésanté ne peut être stockée qu'au sein d'un dossier idoine à condition qu'elle soit minimisée à la finalité du traitement et qu'elle présente une plus-value dans le cadre de la prise en charge médicale ou paramédicale du patient télésoigné.

D) Les notes personnelles prises par le professionnel de santé

71. Malgré la rédaction confusiogène de l'article 45 du code de déontologie médicale, les notes personnelles prises par le professionnel de santé ne peuvent se substituer ni au dossier médical hospitalier, ni à la fiche d'observation personnelle. Si toute donnée médicale ne peut être stockée qu'au sein du dossier de soins du patient, cela signifie que des données personnelles étrangères à la prise en charge médicale du patient peuvent être intégrées sur

²³¹ GUEDON-MOREAU (L.), *Guide de bonnes pratiques de télésurveillance des dispositifs électroniques cardiaques implantables*, Société française de cardiologie, 5 décembre 2019, p. 17. Disponible en ligne sur le site [<https://sfcardio.fr>]. Consulté le 20 août 2020.

²³² Article L.6316-2 du code de la santé publique.

²³³ Décret n° 2021-707 du 3 juin 2021 relatif à la télésanté, *JORF* n°128, 4 juin 2021, texte n° 15.

des supports variés et personnels au médecin. Effectivement, lors des travaux parlementaires préparatoires à la loi du 4 mars 2002, Bernard Kouchner précisait que « *rien n'interdit aux médecins de consigner des notes personnelles ailleurs que dans le dossier médical* »²³⁴. A l'occasion de la prise en charge sanitaire d'un patient, le professionnel de santé peut être amené à prendre des notes manuscrites ou dactylographiées relatives à son patient. Ces notes peuvent aider à contextualiser la prise en charge, servir d'ébauche ou de brouillon pour la démarche intellectuelle et scientifique conduite par le professionnel de santé ou encore d'aide-mémoire. Ces notes peuvent être considérées comme personnelles dans la seule mesure où elles « *ne sont pas destinées à être conservées, réutilisées ou le cas échéant échangées, parce qu'elles ne peuvent contribuer à l'élaboration et au suivi du diagnostic et du traitement ou à une action de prévention* »²³⁵. En ce sens, la CNIL et le CNOM ont affirmé que « *toutes les informations que votre patient a pu vous révéler, dans le cadre de vos échanges, ne doivent pas nécessairement intégrer son dossier. Seules celles qui sont utiles au suivi de votre patient peuvent être enregistrées et conservées.* »²³⁶.

72. *A contrario*, dès lors que ces notes personnelles ont contribué à l'élaboration et au suivi du diagnostic et du traitement, elles font, en raison de leur fonction, partie intégrante du dossier médical hospitalier ou de la fiche d'observation personnelle au patient²³⁷. François Vialla expose concrètement « *qu'il convient de distinguer les notes informelles ne reflétant que des postulats de travail de celles, formalisées, traduisant une véritable démarche diagnostique* »²³⁸. Ainsi, nous déduisons que les notes personnelles qui relatent des comportements et des propos non directement liés à la prise en charge médicale n'ont pas à être intégrées au dossier de soins du patient. Néanmoins, si les notes personnelles prises par le professionnel de santé ne peuvent être incluses dans le dossier de soins du patient, il n'en demeure pas moins qu'elles constituent un traitement de données à caractère personnel.

²³⁴ EVIN (C.), CHARLES (B.), DENIS (J.-J.), *Rapport n°3263, loc. cit.*

²³⁵ Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, *JORF* n°65 du 17 mars 2004, texte n° 16, p. 5206.

²³⁶ CNOM, CNIL, *Guide pratique sur la protection des données personnelles, loc. cit.*

²³⁷ CAA Paris, 30 septembre 2004, n°03PA01769 : RDS, 2015, n° 05, p. 201, obs. F. Vialla ; TA d'Amiens, 24 octobre 2013, n°1200264 ; TA de Melun, 16 octobre 2015, n°1504175.

²³⁸ VIALLA (F.), *La communication des informations personnelles au regard des dispositions de l'article L.1111-7 du code de la santé publique, Réflexions à propos de l'arrêt de la cour administrative d'appel de Paris du 30 septembre 2004*, RGDM, 2005, n°16, p. 207.

Préalablement à la prise de notes relatives au patient, le professionnel de santé doit, évidemment l'en informer, mais également s'assurer que ce traitement est conforme au cadre juridique applicable en matière de protection de données personnelles institué par le RGPD et la loi Informatique et Libertés.

73. Face à l'opacité de la traçabilité des données médicales dans le cadre de la prise en charge sanitaire, ne serait-il pas opportun de concevoir un dossier, structuré et organisé, rattaché à chaque patient tout au long de sa vie ? Quotidiennement, des milliers de données médicales sont produites par tout professionnel de santé, pour tout patient et à l'occasion de tout acte médical ou de soins. Il peut alors exister, pour un même patient, une pluralité de dossiers de soins comportant une certaine quantité de données médicales. Par suite, ces informations intimes et confidentielles se trouvent disséminées, selon leur fonction, à travers une multitude de supports papiers ou numériques, prenant la forme de dossiers ou de notes, sur l'ensemble du territoire national. En 2002, les députés rapportaient que beaucoup d'établissements de santé mettaient en place « *des groupes de travail pour réfléchir à la constitution d'un dossier médical unique, avec l'objectif que celui-ci permette bien de conserver toutes les pièces utiles à la santé d'un malade, sur toute sa vie, et que ces pièces soient aisément consultables par les praticiens et communicables à une autre équipe ou un autre établissement si nécessaire* »²³⁹. Cette ambition a été mise en œuvre par l'adoption, en 2004, du Dossier Médical Personnel devenu, en 2016, le Dossier Médical Partagé (DMP).

Section 2 : Le Dossier Médical Partagé intégré dans l'Espace numérique de santé

74. A l'instar du carnet de santé, le DMP peut être assimilé à un carnet de santé numérique, centralisant l'ensemble des informations médicales relatives à une personne physique tout au long de sa vie. Ce dossier médical numérique, créé systématiquement dès l'ouverture automatique de l'Espace numérique de santé²⁴⁰, est supplémentaire aux dossiers de soins du patient²⁴¹. Il intervient comme l'outil de partage des informations médicales du patient entre les professionnels intervenant à sa prise en charge sanitaire en vue de la

²³⁹ CAA Paris, 30 septembre 2004, n°03PA01769 : RDS, 2015, n° 05, p. 201, obs. F. Vialla ; TA d'Amiens, 24 octobre 2013, n°1200264,; TA de Melun, 16 octobre 2015, n°1504175.

²⁴⁰ Article L.1111-13 du code de la santé publique.

²⁴¹ Article R.1111-40 du code de la santé publique.

coordination, de la qualité et de la continuité de ses soins. Compte tenu du principe de minimisation des données édicté par le RGPD, le périmètre des données médicales qu'il contient doit être circonscrit à celles nécessaires à l'accomplissement de ces finalités (**Paragraphe 1**). Seulement, la quasi-totalité des données médicales générées à l'occasion de la prise en charge sanitaire du patient s'avèrent indispensables à la continuité et à la coordination de ses soins. L'intégralité des données médicales colligées dans ses dossiers de soins doivent-elles être reportées dans son DMP ? Afin d'éviter la répétition de l'alimentation de ces dossiers analogues, et de favoriser le décloisonnement des soins entre la ville et l'hôpital, il conviendrait de centraliser les données médicales relatives à la prise en charge sanitaire du patient en un dossier national et exclusif (**Paragraphe 2**). En ce sens, le DMP est affiché comme un dossier permettant de retrouver, au même endroit, toutes les informations de santé concernant un individu²⁴².

Paragraphe 1 : Le périmètre du contenu du Dossier Médical Partagé

75. La subsistance et la prospérité du DMP sont subordonnées à son alimentation. Certainement, l'ouverture automatique de ce carnet de santé numérique n'emporte pas son succès ; son utilité dépend du renseignement effectif des données médicales relatives à son titulaire par les professionnels intervenant à sa prise en charge sanitaire. A ce titre, chaque professionnel de santé a l'obligation d'y reporter les éléments diagnostiques et thérapeutiques nécessaires à la coordination de ses soins à l'occasion de chaque acte, consultation ou hospitalisation²⁴³ (**A**). En complément, ce carnet de santé numérique peut, de façon inédite, être complété par son titulaire (**B**). Le patient et les professionnels participant à sa prise en charge sanitaire sont donc placés au cœur de ce dossier médical numérique.

²⁴² C'est ainsi que l'Assurance maladie présente le Dossier Médical Partagé sur le site Ameli.fr à travers un article intitulé « *Tout savoir sur le Dossier Médical Partagé (DMP)* ». Disponible en ligne sur le site [<https://www.ameli.fr>]. Consulté le 02 avril 2020.

²⁴³ Article L.1111-15 du code de la santé publique.

A) Les données médicales renseignées par les professionnels intervenant à la prise en charge sanitaire du patient

76. Après plusieurs tentatives de déploiement du Dossier Médical Personnel²⁴⁴, la « loi Santé » de 2016²⁴⁵ a refondé ce carnet numérique en instaurant le Dossier Médical Partagé, dont la mise en œuvre s’est faite progressivement²⁴⁶. Ce dispositif numérique, appartenant au patient, a évolué vers un outil au service des professionnels assurant la coordination de sa prise en charge sanitaire. Malgré son déploiement sur l’ensemble du territoire national et la création délibérée de plus de 10 millions de DMP début 2021²⁴⁷, la loi « Ma Santé 2022 » a entériné sa création automatique pour l’ensemble des assurés sociaux²⁴⁸. Alors que tout bénéficiaire de l’Assurance maladie pouvait décider de créer son DMP jusqu’au 1^{er} juillet 2021, le législateur a substitué ce droit au consentement par un droit d’opposition à sa création automatique pour les personnes bénéficiaires de l’Assurance maladie et de l’aide médicale d’Etat²⁴⁹. Désormais, « *le dossier médical partagé [...] est intégré à l’espace numérique de santé [ENS] dont il constitue l’une des composantes* »²⁵⁰. Partant, « *l’ouverture automatique de l’espace numérique de santé, [...] emporte la création automatique du dossier médical partagé* »²⁵¹ sauf opposition de la personne concernée. L’existence du DMP doit donc être articulée avec la création de l’ENS²⁵². L’évolution de ce régime juridique marque un tournant dans la transition numérique de la santé enclenchée par la loi « Ma santé 2022 »²⁵³. Bien qu’il ne soit pas véritablement obligatoire, le DMP semble être affirmé

²⁴⁴ Article 3 de la loi n°2004-810 du 13 août 2004 relative à l’assurance maladie, *JORF* n°190, 17 août 2004, texte n° 2 ; Article 50 de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l’hôpital et relative aux patients, à la santé et aux territoires, *JORF* n°167, 22 juillet 2009, texte n° 1.

²⁴⁵ Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°22 du 27 janvier 2016, texte n° 1.

²⁴⁶ Après des phases d’expérimentations dans des départements pilotes de décembre 2016 à novembre 2018.

²⁴⁷ Assurance maladie, *Réussir ensemble mon espace santé*, Point presse du 29 avril 2021. Disponible en ligne sur le site [www.esante.gouv.fr]. Consulté le 19 novembre 2021.

²⁴⁸ Article 50 de la loi n°2019-774 du 24 juillet 2019 relative à l’organisation et à la transformation du système de santé, *JORF* n°172, 26 juillet 2019, texte n°3.

²⁴⁹ *Ibid.*

²⁵⁰ Article L.1111-13 du code de la santé publique.

²⁵¹ Article L.1111-14 alinéa 2 du code de la santé publique.

²⁵² PY (B.), OLECH (V.), *La loi 24 juillet 2019 et le virage numérique, le DMP de troisième génération et l’espace numérique*, Revue Droit & Santé, 2019, n° 92, p. 930 à p. 935.

²⁵³ Voir : PON (D.), COURY (A.), *Accélérer le virage numérique*, Stratégie de transformation du système de santé, Rapport final au nom du Ministère des Solidarités et de la Santé, 18 septembre 2018.

comme l’outil numérique central de la prise en charge sanitaire, en s’imposant tant au patient qu’aux professionnels chargés de l’alimenter²⁵⁴.

Concrètement, le DMP peut être défini « *comme un ensemble de services permettant aux professionnels de santé autorisés, de partager, sous forme électronique, les informations de santé utiles à la coordination des acteurs prenant en charge le patient* »²⁵⁵. Contrairement à un service de messagerie électronique permettant l’échange d’informations, le DMP a vocation à stocker les données médicales de son titulaire en vue de les partager. Il convient donc de délimiter les contours de ce dispositif numérique de coordination des soins et de dresser la liste des éléments immatériels pouvant y être intégrés.

77. Depuis la création du régime applicable au DMP²⁵⁶, le législateur énonce vaguement que ce dossier numérique doit notamment comporter l’ensemble des « *éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge* »²⁵⁷. Seulement, une quantité considérable de données médicales sont produites à l’occasion de la dispensation « *de chaque acte ou consultation* »²⁵⁸ sanitaires. Si l’ensemble de ces données, pour chacune des prises en charge du patient, devaient être intégrées au sein de son DMP, ce dispositif deviendrait impénétrable et inutilisable. Il appartient donc aux professionnels de santé le soin d’évaluer les données médicales à y reporter eu égard à l’unique indication relative à l’objectif poursuivi : la coordination de la prise en charge sanitaire. Seulement, ce qu’un professionnel de santé peut juger non pertinent à cette finalité au moment où il renseigne le DMP peut s’avérer crucial dans le cadre d’une prise en charge ultérieure. En effet, toute information médicale peut se révéler fondamentale à la coordination des services de soins de santé, *a fortiori* lorsque la prise en charge médicale est réalisée en urgence ou quand le patient se trouve hors d’état de s’exprimer. Des indications relatives aux antécédents médicaux, au groupe sanguin ou aux traitements médicaux dispensés peuvent se révéler capitales pour la survie du patient. Il est alors délicat, eu égard à la coordination et la

²⁵⁴ Cf. Paragraphe 123.

²⁵⁵ Ministère des Solidarités et de la Santé, *Dossier médical partagé (DMP)*, 16 février 2012, actu. 17 avril 2019. Disponible en ligne sur le site [www.solidarites-sante.gouv.fr]. Consulté le 12 février 2020.

²⁵⁶ Article 3 de la loi n°2004-810 du 13 août 2004, *loc. cit.*

²⁵⁷ Article L.1111-14 alinéa 1 du code de la santé publique.

²⁵⁸ *Ibid.*

continuité des soins, de ne pas intégrer l'ensemble des informations médicales concernant le titulaire du DMP. Dans l'espoir d'apporter plus de précisions quant au contenu de ce dossier numérique, le pouvoir exécutif a tenté d'éclaircir les catégories de données médicales à y intégrer. L'article R.1111-42 du code de la santé publique indique que le DMP contient « *les données relatives à la prévention, à la santé et au suivi médical, social et médico-social, afin de servir la coordination, la qualité et la continuité des soins, y compris en urgence* »²⁵⁹. A titre indicatif, il est mentionné que ces informations concernent notamment « *l'état des vaccinations, les synthèses médicales et paramédicales, les lettres de liaison visées [...], les comptes rendus de biologie médicale, d'examen d'imagerie médicale, d'actes diagnostiques et thérapeutiques, et les traitements prescrits* »²⁶⁰. Bien que ces mentions offrent quelques exemples d'éléments à y implémenter, ce semblant de précision ne permet pas de déterminer le contenu minimal de ce dispositif appelé à devenir essentiel pour la prise en charge sanitaire du patient.

A l'occasion d'un contentieux relatif aux droits sociaux opposant des soignants à une clinique privée, la cour d'appel de Toulouse a rappelé que « *la transmission des informations, nécessaire pour assurer la continuité des soins, fait partie intégrante des fonctions des personnels soignants* »²⁶¹. Si l'absence ou le manque d'informations nécessaires à la continuité des soins causait un préjudice au patient, la responsabilité du professionnel de santé pourrait alors être mise en cause. Afin de pallier cette imprécision législative, source de risque et de contentieux, la loi d'accélération et de simplification de l'action publique²⁶² (ASAP) a annoncé que les données médicales nécessaires à la coordination des soins devant être reportées dans le DMP seront listées par arrêté du ministre chargé de la santé. La liste réglementaire fixant les informations nécessaires à la continuité des soins devrait favoriser l'uniformisation du contenu de l'ensemble des DMP et, *de facto*, son efficacité pour la finalité qu'il poursuit. Par surcroît, cette délimitation devrait participer à la préservation du principe de minimisation des données médicales. Tandis que ces éléments recueillis ou produits à l'occasion de l'examen clinique du patient sont ordinairement reportés par le professionnel

²⁵⁹ Article R.1111-42 1° b) du code de la santé publique.

²⁶⁰ *Ibid.*

²⁶¹ CA Toulouse, ch. sociale, 15 juin 2012, n° 11/03433, JurisData n° 2012-018228.

²⁶² Article 98 de la loi n°2020-1525 du 7 décembre 2020 d'accélération et de simplification de l'action publique, *JORF* n°296, 8 décembre 2020, texte n°1.

de santé qui les a générés, « *ces données peuvent également être versées dans le dossier médical partagé par les services numériques en santé référencés au catalogue de l'espace numérique de santé* »²⁶³. Des dispositifs médicaux connectés peuvent, en effet, produire des données médicales et les intégrer dans le DMP sous réserve de l'interopérabilité de ces systèmes d'information.

En complément des éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins du patient, certains professionnels de santé doivent y reporter des données médicales particulières. D'abord, les professionnels de santé « *habilités des établissements de santé doivent reporter [...] un résumé des principaux éléments relatifs à ce séjour* »²⁶⁴. Ensuite, il appartient au médecin traitant d'y « *verser périodiquement, au moins une fois par an, une synthèse dont le contenu est défini par la Haute Autorité de santé* »²⁶⁵. Après, les données médicales du Dossier Pharmaceutique (DP) utiles à la coordination des soins du patient doivent être retranscrites au sein de son DMP. Finalement, les données médicales incluses dans le dossier médical en santé au travail pourront être reportées au sein du DMP si elles apparaissent nécessaires à la finalité de ce carnet de santé numérique²⁶⁶. Contrairement aux autres éléments immatériels intégrés dans le DMP, ces informations particulières ne pourront y être versées qu'avec l'autorisation de son titulaire²⁶⁷.

78. Alors que le DMP était originellement réservé aux professionnels de santé, le patient peut désormais autoriser des *non-professionnels de santé* à l'alimenter²⁶⁸. Cette nouveauté, introduite par la loi ASAP²⁶⁹, présuppose que le professionnel intervienne effectivement à la prise en charge sanitaire du patient et qu'il soit inscrit sur la liste exhaustive de l'article R.1110-2 du code de la santé publique²⁷⁰. Le cas échéant, le non-professionnel de santé doit veiller à n'y inscrire que les informations apparaissant strictement indispensables à la

²⁶³ Article R.1111-42 1° b) du code de la santé publique.

²⁶⁴ Article L.1111-14 alinéa 1 du code de la santé publique.

²⁶⁵ *Ibid.*

²⁶⁶ A compter du 1er janvier 2024 au plus tard.

²⁶⁷ Article 16 de la loi n°2021-1018 du 2 août 2021 pour renforcer la prévention en santé au travail, *JORF* n°178, 3 août 2021, texte n°2.

²⁶⁸ Article L.1111-17 III du code de la santé publique.

²⁶⁹ Article 98 de la loi n°2020-1525 du 7 décembre 2020, *op. cit.*

²⁷⁰ Cf. Paragraphe 261.

coordinations des soins du patient. Après avoir obtenu l'autorisation préalable du patient, « *l'alimentation ultérieure de son dossier médical partagé par ce même professionnel est soumise à une simple information de la personne prise en charge* »²⁷¹. Alors que certaines données péri-médicales, médico-sociales ou sociales pourraient être potentiellement utiles à la prise en charge sanitaire du patient, comment un non-professionnel de santé peut-il juger de la pertinence d'une information non médicale pour la continuité et la coordination des soins du patient ? Une mauvaise interprétation de l'adéquation d'une information confidentielle pour la coordination, la qualité et la continuité des soins pourrait contrevenir au principe de minimisation des données personnelles. Au demeurant, cette information inutile à l'accomplissement de ces finalités serait rendue accessible à une pluralité de professionnels qui ne devraient pas être amenés à en connaître. Néanmoins, la situation sanitaire étant unique à un patient, il apparaît nécessaire que les professionnels participant à sa prise en charge sanitaire apprécient subjectivement les données médicales recueillies et produites lors des actes sanitaires qui se trouvent spécifiquement nécessaires pour ses prises en charges ultérieures.

B) Les données renseignées par le titulaire du Dossier Médical Partagé

79. Contrairement aux dossiers de soins, le DMP peut contenir des informations renseignées directement par son titulaire ou, le cas échéant, par son représentant légal. Plus qu'un outil de coordination des soins, le DMP est également estampillé comme étant le dossier du patient. A ce titre, il bénéficie de la possibilité de l'alimenter.

80. Le DMP étant un dossier unique à chaque assuré social, son titulaire doit renseigner ses données administratives et ses coordonnées²⁷². Avant qu'une donnée médicale ne puisse y être implémentée, l'identification du titulaire doit alors être assurée. Le professionnel doit ainsi vérifier que les documents versés au sein du DMP concernent effectivement le patient dont il assure la prise en charge sanitaire ou médico-sociale. Au titre des données administratives, figurent également l'identité et les coordonnées des représentants légaux du mineur, ainsi que celles relatives à la personne chargée de la mesure de représentation du

²⁷¹ Article L.1111-17 III du code de la santé publique.

²⁷² Article R.1111-42 1° a) du code de la santé publique.

majeur protégé²⁷³. Ces indications relèvent d'une importance particulière dans le cadre du consentement aux décisions concernant la santé du titulaire du DMP lorsqu'il juridiquement incapable. En effet, le professionnel de santé ne peut prendre les décisions médicales relatives au mineur qu'avec le consentement de ses représentant légaux²⁷⁴. Aussi, la personne chargée de la mesure de protection avec représentation relative au patient consent aux décisions médicales lorsque ce dernier est inapte à exprimer sa volonté²⁷⁵. L'inscription des informations relatives aux représentants légaux du patient permettent au professionnel de santé de s'assurer que les décisions médicales seront effectivement déterminées avec l'assistance de ses protecteurs. De cette façon, la protection de l'intégrité de son corps humain en est renforcée²⁷⁶.

81. En complément des données administratives obligatoires, le titulaire du DMP peut y renseigner des informations concernant les volontés relatives à la fin de sa vie dans le cas où il serait hors d'état de les exprimer. Le DMP peut ainsi comporter « *les données relatives à l'identité et les coordonnées de la personne de confiance* »²⁷⁷, « *les données relatives aux directives anticipées* »²⁷⁸ et « *les données relatives au don d'organes ou de tissus* »²⁷⁹. Bien que ces informations paraissent uniquement connexes à la santé de la personne concernée, elles revêtent d'une utilité pour la coordination de ses soins. En effet, le DMP est incontestablement un outil de démocratie sanitaire plaçant le patient au cœur de sa prise en charge médicale. Grâce au DMP, le patient devient un acteur et un coordonnateur des décisions médicales entourant la fin de sa vie. Le patient bénéficie de l'opportunité d'anticiper des situations délicates alors même qu'il ne serait plus en état d'exprimer ses choix et volontés. Seulement, certaines de ces indications semblent avoir une portée limitée dans la mesure où elles constituent un droit qui ne peut être exercé que sous certaines conditions formelles.

²⁷³ Article R.1111-42 2° du code de la santé publique.

²⁷⁴ Article L.1111-4 alinéa 7 du code de la santé publique.

²⁷⁵ Article L.1111-4 alinéa 8 du code de la santé publique.

²⁷⁶ Article 16-3 du code civil.

²⁷⁷ Article R.1111-42 3° du code de la santé publique.

²⁷⁸ Article R.1111-42 1° g) du code de la santé publique.

²⁷⁹ Article R.1111-42 1° f) du code de la santé publique.

82. En vertu de l'article L.1111-6 du code de la santé publique, toute personne majeure bénéficie du droit de désigner une personne de confiance. Eu égard à la structuration du DMP, cet outil semble être un moyen d'exercice de ce droit. En effet, le titulaire du DMP peut y renseigner les données relatives à la personne de confiance qu'il souhaite désigner. Cependant, le législateur a disposé que cette désignation devait être « *faite par écrit et cosignée par la personne désignée* »²⁸⁰. Assurément, la personne de confiance doit, d'une part, avoir connaissance des dernières volontés du patient et, d'autre part, accepter de les témoigner dans l'hypothèse où le patient se trouverait hors d'état de s'exprimer. Il paraît donc surprenant de pouvoir désigner unilatéralement, au moyen du DMP, une personne de confiance sans même qu'elle ne puisse accepter le poids de ce rôle. La valeur juridique des désignations de personnes de confiance réalisées à travers le DMP semble donc être remise en cause.

Seulement, dans les cas où le patient n'y a pas renseigné ses directives anticipées, il serait essentiel que les professionnels de santé puissent avoir connaissance de la désignation de ce témoin, notamment en cas de situation médicale critique. En effet, lorsque la personne est hors d'état d'exprimer sa volonté, aucune limitation ni arrêt des traitements ne peuvent être réalisés sans que « *les directives anticipées [n'aient été respectées] ou, à défaut, sans que la personne de confiance [...] ou, à défaut la famille ou les proches, aient été consultés* »²⁸¹. Il appert que le témoignage de la personne de confiance prime sur tout autre témoignage. Si le DMP permettait cette désignation conformément aux conditions légales, et si les patients y renseignaient effectivement les données relatives aux directives anticipées et à la personne de confiance, des situations conflictuelles analogues à l'affaire « Vincent Lambert » pourraient être évitées. Dans l'intention de se conformer aux conditions légales de la désignation de la personne de confiance, cette nomination devrait être effectuée au moyen d'un écrit manuscrit, numérisé et intégré dans le DMP par son titulaire. De cette façon, la personne désignée pourrait y apposer sa signature suivant les exigences de l'article L.1111-6 du code de la santé publique. Bien que le droit à la rédaction des directives anticipées et à la désignation de la personne de confiance existent indépendamment du DMP, l'intérêt de consigner ces informations au sein d'un dossier unique est de les rendre accessibles, en tout

²⁸⁰ Article L.1111-6 alinéa 1 du code de la santé publique.

²⁸¹ Article L.1111-4 alinéa 6 du code de la santé publique.

lieu et en tout temps, à tout professionnel de santé intervenant dans le cadre de la prise en charge médicale de la personne concernée.

83. Au surplus de ces informations analogues à la santé, le titulaire du DMP peut renseigner ses données médicales. Leur intégration par le titulaire de ce dossier numérique peut prendre la forme d'un texte libre ou d'un document téléchargé. Ainsi, ce dernier a la possibilité d'y insérer l'ensemble de ses documents médicaux produits antérieurement à l'ouverture de cet outil. Si le patient le souhaite, l'historique de sa santé pourra donc y être reporté. Dans le cadre de la coordination des soins, il serait pertinent que les professionnels de santé puissent avoir connaissance de l'antériorité médicale de la santé du patient. En effet, la prise en compte de certaines pathologies passées permet de prévenir le risque de survenance de pathologies futures. Il conviendrait alors d'encourager le titulaire du DMP à transférer l'ensemble de ses données cliniques formalisées antérieurement à la création de ce dossier dans la mesure où il semble le seul à pouvoir les y verser.

84. Compte tenu de l'analyse des données médicales colligées au sein du dossier de soins et du DMP, nous pouvons constater que leurs périmètres sont sensiblement identiques. Assurément, la majorité des données médicales recueillies et produites à l'occasion de la prise en charge sanitaire du patient – et donc nécessairement consignées au sein de ses dossier de soins – se montrent nécessaires à la coordination et à la continuité de son parcours de santé. Partant, elles devraient opportunément être reportées au sein du DMP. Il en advient que les professionnels de santé participant à la prise en charge sanitaire du titulaire du DMP devraient systématiquement y renseigner les données médicales générées à l'occasion de la délivrance des services de soins de santé. Il en résulte que les mêmes données médicales se trouveraient stockées au sein du dossier médical hospitalier ou de la fiche d'observation personnelle au patient, mais également dans son DMP. Or, ces multiples retranscriptions favorisent importunément la dissémination des données médicales du patient et tend véridiquement à décoordonner ses prises en charges sanitaires. A l'heure du virage numérique en santé, l'affirmation d'un unique dossier numérique centralisé pourrait devenir une solution à la limitation de ces innombrables traitements de données particulièrement sensibles.

Paragraphe 2 : La nécessaire centralisation des données relatives à la prise en charge médicale du patient en un dossier national et exclusif

85. Alors que nous pouvons dénombrer une pluralité de dossiers de soins, il existe pareillement une multitude de dossiers numériques partagés (A). Ces dossiers, supplémentaires aux dossiers de soins, ont exclusivement vocation à favoriser la coordination de la prise en charge sanitaire du patient entre l'ensemble des professionnels y participant. A cet effet, les éléments immatériels du corps humain du patient sont réunis et conservés sur une plateforme web, abritée auprès d'un hébergeur de données de santé certifié, à laquelle les personnes légalement habilitées peuvent accéder. Cependant, la pluralité et la disparité des dossiers numériques partagés pourraient nuire à leur utilité. En effet, s'il subsiste autant de dossiers numériques partagés que d'utilisateurs professionnels, les informations médicales relatives au patient ne pourront être centralisées en un seul et même endroit, accessible en tout temps et en tout lieu. Il apparaît donc incontournable d'affermir le rôle central du DMP (B).

A) La disparité des dossiers numériques partagés

86. Alors que l'instauration du DMP remonte au mois d'août 2004, sa généralisation à l'échelle nationale n'est intervenue qu'à compter de novembre 2018, et l'automatisme de son ouverture pour tout assuré social est advenue en janvier 2022. Pendant ce laps de temps, l'idée d'un dossier numérique partagé n'a pas demeuré sous le monopole étatique. Bien que le DMP soit un outil numérique public et national, Guillaume Monziols a très justement soulevé que son déploiement tardif a ouvert un boulevard aux solutions numériques privées et morcelées²⁸². En effet, depuis une décennie, tant les géants américains du web que les *start up* françaises ont investi le numérique au service de la santé. Le marché de la santé numérique étant en plein essor²⁸³, les acteurs privés ne cessent de proposer des services et des solutions

²⁸² MONZIOLS (G.), *Le dossier médical partagé face aux logiciels et applications mobiles du secteur privé*, RGDM, 2019, n° 27, p.154.

²⁸³ Voir : MOREAUX (R.), *Santé et numérique: un marché "en plein essor" au sein du pôle Cap Digital*, TicPharma, 22 juin 2018. Disponible en ligne sur le site [www.ticpharma.com]. Consulté le 13 février 2020 ; MOREAUX (R.), *Le marché mondial de la santé numérique estimé à 234,5 milliards de dollars en 2023*, TicPharma, 31 octobre 2019. Disponible en ligne sur le site [www.ticpharma.com]. Consulté le 13 février 2020.

variés, dont des dossiers numériques partagés²⁸⁴. Par conséquent, « *il existe, à l'heure actuelle, un nombre important de dossiers différents qui contiennent des données médicales de patient et qui sont utilisés pour leur suivi* »²⁸⁵. Les fournisseurs de solutions numériques sont donc multiples et les offres qu'ils proposent sont disparates. Or, cette diversification des offres numériques sur le marché de la santé va à l'encontre de l'objectif du partage de l'information médicale. Certainement, le législateur autorise le partage des données médicales du patient entre les professionnels qui participent à sa prise en charge dès lors qu'elles se révèlent « *strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social* »²⁸⁶. Seulement, comment garantir le partage d'une information médicale lorsque les dossiers numériques ne sont ni coordonnés, ni interopérables ? En pratique, les différentes solutions de dossiers numériques ne sont soumises à aucun référentiel de standardisation contraignant, ce qui complique considérablement leur interfaçage. Nonobstant le respect du cadre – facultatif - d'interopérabilité des systèmes d'information de santé (CI-SIS), l'adoption d'un dispositif national unique apparaît essentiel à la communication des données médicales.

87. Outre ces initiatives privées, des solutions publiques similaires au DMP émergent également. La stratégie de transformation du système de santé, consacrée par la loi Ma Santé 2022, est particulièrement axée sur le renforcement du numérique dans le système de santé. Dans cette dynamique, une feuille de route visant à accélérer ce virage numérique a été présentée par la ministre de la santé, Agnès Buzyn, le 25 avril 2019. Parmi les actions exposées, la troisième orientation présentée portait sur le déploiement de *services numériques socles* dont l'action 14 repose sur le programme « e-parcours ». Ce programme e-parcours vise à « *accompagner la transformation numérique du parcours de santé dans les territoires en appui des professionnels exerçant dans les secteurs sanitaires, médicosociaux et sociaux* »²⁸⁷ en leur offrant un bouquet de services numériques de coordination. En d'autres termes, ce programme fournit un outillage numérique régional dédié à la coordination des

²⁸⁴ Nous pouvons citer, à titre d'exemple non exhaustif, les solutions *MedicalCloud*, *Followmed*, ou encore *Yes Dr.*

²⁸⁵ TILMAN (L.), *L'utilisation des technologies de l'information et de la communication à l'hôpital face au droit*, Johanne SAISON-DEMARS (dir.), Thèse de doctorat, Droit, Université de Lille, 28 septembre 2017, p.161.

²⁸⁶ Article L.1110-4 III du code de la santé publique.

²⁸⁷ Ministère des Solidarités et de la Santé, *Le programme e-Parcours*, 25 juin 2019. Disponible en ligne sur le site [www.solidarites-sante.gouv.fr/]. Consulté le 23 février 2020.

parcours de santé²⁸⁸. A titre d'exemple, l'Agence régionale de santé des Hauts-de-France, associée au Groupement d'intérêt public « Sant& Numérique Hauts-de-France », a décliné cette feuille de route à l'échelle locale par le lancement d'un programme régional nommé « *Prédice : Ma santé Hauts de France* ». Prédice est une « *plateforme intégrée de collaboration, de services et d'interopérabilité des systèmes d'information en santé* »²⁸⁹ accessible aux professionnels de santé et aux usagers *via* « *un portail régional unique et sécurisé* »²⁹⁰. Elle a pour objectif le renforcement de la coordination du parcours de soins grâce au partage et à l'échange des informations médicales du patient, avec les professionnels des secteurs sanitaire, médico-social et social participant à sa prise en charge sur le territoire régional²⁹¹. Concrètement, la plateforme Prédice constitue un outil numérique de coordination des soins.

88. Alors que Prédice est officiellement présenté comme un dossier de coordination complémentaire au DMP, son déploiement pourrait supplanter le DMP à l'échelle régionale. Pourtant, le DMP est compté comme le premier des « services numériques socles » et l'affirmation de son déploiement était annoncée comme prioritaire aux autres actions visant à renforcer le virage numérique²⁹². D'ailleurs, la feuille de route du numérique en santé conseille de continuer à en « *promouvoir l'alimentation par les établissements de santé, les EHPAD, les biologistes, les radiologues et les médecins généralistes* »²⁹³ afin que son utilisation et son efficacité puissent devenir optimales. Avant de créer de nouvelles plateformes de coordination des soins, il conviendrait certainement d'avancer graduellement. En effet, il serait plus raisonnable d'attendre l'implantation effective du DMP sur l'ensemble du territoire national avant de soumettre un énième outil aux professionnels chargés de la prise en charge sanitaire du patient. La multiplicité des dossiers numériques élaborés par l'administration pourrait définitivement ralentir le déploiement et l'utilisation des outils numériques au service des patients et des acteurs du système de santé.

²⁸⁸ Instruction n°DGOS/PF5/2019/129 du 24 mai 2019 relative à la mise en œuvre du programme e-parcours.

²⁸⁹ ARS Hauts-de-France, *Plaquette de présentation Prédice*. Disponible en ligne sur le site [www.hauts-de-france.ars.sante.fr]. Consulté le 23 février 2020.

²⁹⁰ *Ibid.*

²⁹¹ *Ibid.*

²⁹² Instruction n° SG/DSSIS/DGOS/DGCS/CNAM/2018/72 du 13 mars 2018 relative à l'accompagnement en région de la généralisation du dossier médical partagé (DMP).

²⁹³ Ministère des Solidarités et de la Santé, *Avancement du « virage numérique en santé »*, décembre 2019, p.21.

89. De surcroît, les professionnels de santé ne semblent pas encore avoir adhéré au DMP. En 2019, il apparaissait que 46% des médecins généralistes le consultaient et que seulement 20% l'alimentaient²⁹⁴. Alors que certains professionnels de santé en ignorent même l'existence, ceux qui en ont connaissance estiment souvent que son alimentation constitue une tâche administrative trop chronophage et non valorisée. En ce sens, le syndicat Fédération des Médecins de France considère que l'alimentation de 1450 DMP représenterait plus de dix semaines de travail pour le médecin. En outre, ce syndicat réclame que la première alimentation du volet de synthèse médicale (VSM) du DMP soit rémunérée à hauteur d'une consultation complexe, voire très complexe²⁹⁵. Le travail que représente l'alimentation du DMP explique notamment l'absence d'alimentation des DMP créés.

Toutefois, dans la ferme intention d'appuyer la transformation numérique du système de santé – et surtout d'anticiper la prospérité de l'ENS –, l'avenant n°9 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie²⁹⁶ concède le financement progressif de l'usage du DMP. A ce titre, « *l'Etat mobilise un investissement historique pour soutenir financièrement les professionnels de santé dans leur équipement en solutions logicielles facilitant l'échange et le partage de données de santé entre les acteurs du parcours de soins et avec l'utilisateur* »²⁹⁷. Afin d'inciter les médecins de ville à renseigner le DMP, et plus particulièrement le VSM, « *un nouveau forfait intitulé forfait élaboration initiale du VSM* »²⁹⁸ a été créé. Il est prévu que ce forfait fasse l'objet d'un versement exclusif au cours du second semestre 2023 « *dans la mesure où l'objectif est de valoriser l'initiation de l'élaboration des VSM* »²⁹⁹. Ainsi, un forfait d'un montant de 1500 euros sera versé au médecin ayant élaboré des VSM alimentant le DMP d'au moins la moitié de sa patientèle en affection longue durée (ALD)³⁰⁰. Ce forfait sera porté à 3000 euros si le

²⁹⁴ ANS, Doctrine technique du numérique en santé, Concertation publique, janvier 2020, p. 2.

²⁹⁵ TALBOT (R.), *Quelle valeur pour le VSM ?*, 7 juillet 2019. Article disponible en ligne sur le site [www.fmfpro.org]. Consulté le 23 février 2020.

²⁹⁶ Article 4 de l'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, *JORF* n°224, 25 septembre 2021, texte n° 19.

²⁹⁷ *Ibid.*

²⁹⁸ *Ibid.*

²⁹⁹ *Ibid.*

³⁰⁰ *Ibid.*

médecin élabore des VSM pour 90 % de sa patientèle en ALD³⁰¹. Par surcroît, « *ce forfait est majoré de 20 % si plus d'un tiers des VSM alimentant le DMP sont générés de manière structurée dans le format conforme au Cadre d'interopérabilité des Systèmes d'information de Santé (CI-SIS)* »³⁰². Les médecins libéraux ont jusqu'au 30 juin 2023 pour satisfaire aux conditions de versement de ce forfait inédit. En supplément, de nouveaux indicateurs liés à l'usage et au remplissage du DMP permettent de générer des points ouvrant droit à une rémunération forfaitaire lorsque le médecin libéral atteint un nombre total de 400 points³⁰³. A compter de 2022, « *l'atteinte d'un taux de 20 % des consultations réalisées dans l'année donnant lieu à l'alimentation d'un document dans le DMP permet de valider l'indicateur. Pour 2022 et 2023, cet indicateur est valorisé à hauteur de 40 points* »³⁰⁴.

En outre, l'incitation financière à l'utilisation et à l'alimentation du DMP est marquée d'une manière punitive à l'article L.1111-14 du code de la santé publique. En effet, « *l'adhésion aux conventions nationales régissant les rapports entre les organismes d'assurance maladie et les professionnels de santé [...] et son maintien sont subordonnés à la consultation ou à la mise à jour du dossier médical partagé de la personne prise en charge par le médecin* »³⁰⁵. Le manquement à l'obligation de remplissage du DMP emporte donc des conséquences pécuniaires pour le professionnel de santé ; lesquelles peuvent se répercuter sur le patient. Certainement, si les acteurs de son parcours de santé n'étaient pas conventionnés avec l'Assurance maladie, le prix de la consultation ne lui serait pas remboursé par la sécurité sociale.

90. Malgré l'évolution sémantique du DMP initiée en 2016, cet outil de coordination des soins semble toujours perçu comme le carnet numérique personnel au patient et non comme un dispositif de la prise en charge sanitaire. L'esprit originnaire du DMP explique, en partie, les difficultés d'appropriation de cet outil par les professionnels de santé. De plus, jusqu'au 1^{er} juillet 2021, le DMP ne pouvait être créé qu'à l'initiative du patient ou de ses représentants légaux. En conséquence, les professionnels de santé ne pouvaient s'appuyer sur un

³⁰¹ *Ibid.*

³⁰² *Ibid.*

³⁰³ Article 5 de l'arrêté du 22 septembre 2021, *loc. cit.*

³⁰⁴ *Ibid.*

³⁰⁵ Article L.1111-14 alinéa 7 du code de la santé publique.

outil facultatif dont l'existence dépendait uniquement du bon vouloir du patient concerné. Contrairement aux dossiers de soins constitués à l'occasion de toute prise en charge médicale, le DMP n'était qu'un dossier supplémentaire constitué sous l'impulsion du patient. Si le patient n'avait pas créé son DMP, le professionnel de santé ne pouvait utiliser cet outil de coordination des soins. Dès lors, il pouvait être intéressant d'utiliser une solution indépendante, proposée par un acteur privé et indépendamment de la volonté du patient, sous-couvert du respect des règles applicables au secret professionnel médical et à la protection des données personnelles.

B) L'essentiel affermissement du rôle central du DMP

91. S'il apparaît que les professionnels de santé éprouvent des difficultés à tenir les dossiers de soins du patient, qu'en est-il de l'addition d'un dossier numérique supplémentaire ? Selon le législateur, il n'est pas concevable que le DMP vienne se substituer aux dossiers de soins tenus par les établissements de santé et les professionnels de santé³⁰⁶. Néanmoins, « *face à la démultiplication des dossiers se pose la question de savoir comment ceux-ci s'articulent entre eux. Est-ce qu'ils se complètent ? S'alimentent entre eux ? Ou alors sont-ils redondants, auquel cas certains d'entre eux seraient amenés à disparaître ? Finalement, la question principale qui se pose ici est de savoir si le DMP, de par ses particularités, est un concurrent ou un réel complément aux autres dossiers.* »³⁰⁷. Nous allons tenter de répondre à ces questionnements afin de déterminer si le DMP peut, ou non, constituer l'unique et exclusif dossier médical du patient.

92. D'abord, dans le cadre de la prise en charge sanitaire du patient, tant les dossiers de soins que le DMP ont pour finalité la conservation de ses informations médicales en vue de la continuité et de la coordination de ses soins. Selon la Haute Autorité de Santé (HAS), « *le défaut de communication constitue une des principales causes racines des événements*

³⁰⁶ Voir : GAGNEUX (M.), *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé*, Recommandations à la ministre de la santé, de la jeunesse, des sports et de la vie associative, avril 2008 ; R.1111-40 du code de la santé publique.

³⁰⁷ TILMAN (L.), *L'utilisation des technologies de l'information et de la communication à l'hôpital face au droit*, loc. cit., p.159.

indésirables en milieu de soins »³⁰⁸. L'accessibilité d'un dossier numérique unique participerait donc à la réduction des risques causés par le manque de communication des données médicales et, conséquemment, de coordination des soins. Le DMP apparaît alors comme un outil facilitateur du parcours de santé coordonné. Effectivement, si le DMP n'existait pas, les données médicales circuleraient par d'autres biais, certainement moins structurés et moins sécurisés. La centralisation des données médicales du patient au sein du DMP favoriserait donc la continuité et la coordination des soins tout au long de la vie du patient et, en particulier, dans le cadre de l'urgence, des maladies chroniques et des affections longue durée.

93. Ensuite, les périmètres des dossiers de soins et du DMP sont, *a minima*, identiques. Effectivement, les informations intégrées dans le dossier médical hospitalier et la fiche d'observation personnelle correspondent, tout au moins, au contenu minimal du DMP. L'alimentation du dossier de soins et du DMP représenterait donc un geste redondant et chronophage pour le professionnel de santé³⁰⁹. Pourtant, il serait envisageable de transposer le contenu réglementaire du dossier médical hospitalier au DMP, dont la structure et l'architecture sont homogènes et uniformes à toute structure de soins et tout professionnel de santé. Le dossier médical hospitalier et la fiche d'observation personnelle pourraient ainsi disparaître au profit d'un dossier unique et exclusif au patient. Bien entendu, les professionnels de santé pourraient prendre des notes personnelles au sujet des patients qu'ils prennent en charge à condition qu'elles ne puissent servir à l'élaboration et au suivi du diagnostic et de la thérapeutique³¹⁰. Toutefois, dans un contexte de coordination des soins entre professionnels de santé exerçant au sein de structures et secteurs différents, la surcharge d'informations paramédicales pourrait enliser la lisibilité du DMP. C'est pourquoi il conviendrait de définir une hiérarchie et une chronologie entre les différents onglets et documents du DMP, lesquelles seraient définies en considération de sa qualité de dossier médical exclusif.

³⁰⁸ HAS, *Un guide pour faciliter la communication entre professionnels de santé*, octobre 2014. Disponible en ligne sur le site [www.has-sante.fr]. Consulté le 02 décembre 2021.

³⁰⁹ Cf. Paragraphe 89.

³¹⁰ Cf. Paragraphe 71.

94. Finalement, depuis l'entrée en vigueur de l'article 50 de la loi Ma Santé 2022, le DMP est ouvert automatiquement pour tout assuré social, sauf opposition de la personne concernée ou de son représentant légal³¹¹. A moins que les résidents français n'exercent leur droit d'opposition à ce traitement de données personnelles, le DMP consiste désormais en un dossier rattaché à l'individu, de sa naissance à sa mort, retraçant l'historique de son histoire médicale. L'accélération du virage numérique en santé tend progressivement à affirmer le rôle central du DMP. En effet, les pouvoirs publics ont intégré le DMP au sein de l'ENS, au moyen duquel il devient accessible. Cet espace numérique personnel donne accès à un portail de services et d'applications en santé. L'ENS est notamment composé du DMP, d'une messagerie de santé sécurisée, d'un agenda de santé, et d'un catalogue d'applications référencées par l'État³¹². Cet espace personnel a pour objectif de permettre à toute personne, ou à ses représentants légaux, de gérer ses données médicales et de santé, dans un espace sécurisé, et ainsi, « *de participer à la construction de son parcours de santé en lien avec les acteurs des secteurs sanitaire, social et médico-social, favorisant ainsi la prévention, la coordination, la qualité et la continuité des soins* »³¹³. Plus concrètement, il s'agit d'un « *espace numérique individuel mis à la disposition par l'État et l'Assurance Maladie pour permettre à chaque citoyen de stocker ses informations médicales et les partager avec les professionnels de santé qui les soignent* »³¹⁴. En outre, l'ENS a pour objectif de fixer un cadre aux solutions en santé numérique afin de freiner les initiatives privées, disparates, non coordonnées et non interopérables³¹⁵. La portée de l'intégration du DMP au sein de l'ENS semble donc le référencer comme le dossier médical de référence.

95. La constitution d'un seul et unique dossier rattaché au patient lui offrirait une réelle transparence sur le traitement de ses données médicales à des fins de prise en charge sanitaire. D'une part, le patient bénéficierait de la parfaite connaissance de l'emplacement de ses données médicales et, conséquemment, profiterait davantage de contrôle sur celles-ci. Lucie

³¹¹ Cf. Paragraphes 117.

³¹² Article L.1111-13-1 II du code de la santé publique.

³¹³ Article L.1111-13 du code de la santé publique.

³¹⁴ Assurance maladie, *Réussir ensemble mon espace santé*, Point presse du 29 avril 2021. Disponible en ligne sur le site [www.esante.gouv.fr]. Consulté le 19 novembre 2021.

³¹⁵ Assemblée Nationale, Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à l'organisation et à la transformation du système de santé, Volume I : commentaires d'articles et annexes, 14 mars 2019.

Cluzel-Metayer et Armande François rapportent que les risques d'une perte de maîtrise des données résident dans « *la dispersion des données dans des espaces qui ne sont pas toujours parfaitement sécurisés. Or, les données de santé sont particulièrement exposées à des actes malveillants.* »³¹⁶. L'affermissement du rôle central du DMP faciliterait l'exercice des droits du patient sur ses données médicales alors cartographiées, et permettrait d'assurer leur sécurité et leur protection. D'ailleurs, la constitution du DMP, en tant que traitement de données sensibles mis en œuvre pour le compte de l'Etat, a reçu un avis favorable de la CNIL³¹⁷. D'autre part, le patient pourrait identifier chacune des connexions à son dossier. En effet, les accès au DMP requièrent une identification et une authentification des professionnels et sont, par ailleurs, tracés³¹⁸. Par conséquent, tout accès en dehors des règles établies par le code de la santé publique et le cadre juridique applicable en matière de protection des données personnelles serait illégitime et passible d'une sanction financière mais également de sanctions pénales et ordinaires³¹⁹.

96. Le législateur n'ayant pas anticipé que le DMP puisse éventuellement devenir l'unique et l'exclusif dossier médical du patient, cette conception exigerait de redéfinir les droits et les devoirs que le patient détient sur la création de son dossier numérique ainsi que sur les données personnelles contenues en son sein. D'une part, le patient ne devrait plus pouvoir s'opposer à la création de son DMP³²⁰. D'autre part, s'il ne fait nul doute que le patient est le titulaire de son DMP, il conviendrait de le responsabiliser quant à la gestion de ses données et à l'impact de ses actions sur sa prise en charge sanitaire³²¹. Le DMP pourrait ainsi devenir l'outil d'accomplissement de la démocratie sanitaire, et la prise en charge médicale deviendrait véritablement collaborative. De surcroît, le DMP étant un dossier collaboratif, son utilité et son succès dépendent indispensablement de son alimentation par l'ensemble des protagonistes autorisés à y contribuer. A cet effet, il conviendrait, en outre,

³¹⁶ CLUZEL-METAYER (L.), FRANCOIS (A.), *La protection des données personnelles à l'épreuve de la télémédecine*, RDSS, 2020, n°01, p. 51.

³¹⁷ CNIL, Délibération n° 2016-258 du 21 juillet 2016 portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'un traitement de données à caractère personnel dénommé « dossier médical partagé » (demande d'avis n° 16017107), *JORF* n°268, texte n° 37, 18 novembre 2016.

³¹⁸ Article R.1111-31 du code de la santé publique.

³¹⁹ CNIL, *Dossier médical partagé (DMP) : questions-réponses*, 07 novembre 2018. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 13 février 2020.

³²⁰ Cf. Paragraphe 117.

³²¹ Cf. Paragraphes 311 s.

d'instituer un devoir de renseignement du DMP à la charge de son titulaire³²², et de renforcer l'obligation d'alimentation à la charge des professionnels de santé³²³.

³²² *Ibid.*

³²³ *Cf.* Paragraphe 123.

Conclusion du chapitre

97. Toute donnée médicale, recueillie ou produite par les professionnels de santé à l'occasion de la prise en charge sanitaire du patient, doit être formalisée au sein d'un dossier médical. Le terme « dossier médical » est général, il couvre spécifiquement les dossiers de soins et les dossiers numériques partagés.

L'expression « dossiers de soins » renvoie, d'une part, aux dossiers médicaux hospitaliers constitués par les établissements de santé publics et privés et, d'autre part, aux fiches d'observation personnelles tenues par les médecins. Ces dossiers de soins ont pour finalité de tracer l'ensemble des actions médicales et paramédicales dispensées aux patients. Outre les données administratives du patient, indispensables à l'identitovigilance, ces dossiers contiennent l'ensemble des données médicales générées lors de la dispensation des actes de prévention, de diagnostic ou de soins. Toutefois, en vertu du principe de minimisation des données édicté à l'article 5 du RGPD, seules les données adéquates, pertinentes et limitées à ce qui est nécessaire à la prise en charge sanitaire du patient peuvent y être versées.

En supplément de ces deux catégories de dossiers, il existe le Dossier Médical Partagé créé automatiquement pour tout bénéficiaire de l'Assurance maladie et de l'aide médicale d'Etat qui ne s'y est pas opposé. Le DMP a pour finalité de faciliter l'accès aux données cliniques produites à l'occasion de la prise en charge médicale, afin de favoriser la coordination des soins du patient entre les différents professionnels y concourant, quels que soient leur secteur et leur modalités d'exercice. A l'occasion de l'alimentation du DMP, les professionnels doivent veiller à y reporter les seules informations médicales utiles à sa finalité : « *la prévention, la coordination, la qualité et la continuité des soins* »³²⁴.

En apparence, le contenu essentiel des données médicales formalisées au sein des différents dossiers médicaux est sensiblement identique. Toutefois, à l'inverse des dossiers médicaux hospitaliers et des fiches d'observation personnelles dont la forme et la substance peuvent être variables en fonction de leur producteur, le DMP est un dossier dont

³²⁴ Article L.1111-14 alinéa 1 du code de la santé publique.

l'organisation, l'architecture et le contenu sont homogènes et sécurisés³²⁵. En pratique, l'addition d'un nouveau dossier rattaché au patient pourrait complexifier la cartographie des supports pouvant contenir les éléments immatériels de son corps humain issus de la prise en charge sanitaire. En conséquence, il pourrait être opportun de faire du DMP l'unique dossier médical utilisé par tout professionnel dispensant des services de soins de santé.

³²⁵ CNIL, Délibération n° 2016-258 du 21 juillet 2016, *op. cit.*

Chapitre 2 :

La limitation des droits du patient sur les données personnelles colligées dans ses dossiers médicaux

98. La formalisation des informations relatives au patient dans ses dossiers médicaux constitue un traitement de données personnelles au sens de l'article 4 du RGPD. Cette opération de collecte, de structuration et de conservation des données est fondée sur l'obligation réglementaire des établissements et des professionnels de santé de constituer un dossier de soins pour les patients qu'ils prennent médicalement en charge³²⁶. Pareillement, l'alimentation du DMP correspond à un traitement obligatoire pour les professionnels de santé³²⁷. En conséquence, le patient, en tant que personne concernée par le traitement de ses données médicales et administratives, ne peut s'opposer à la constitution de ses dossiers médicaux et à la consignation de ses informations personnelles en leur sein (**Section 1**). Bien que le droit d'opposition au traitement conféré par le RGPD apparaît inefficace en l'espèce, la personne concernée dispose, en théorie, des droits à la rectification et à l'effacement de ses données personnelles. Seulement, appliqués aux informations contenues dans les dossiers médicaux, ces droits de modification des données sont, en pratique, fortement diminués (**Section 2**). L'autodétermination informationnelle du patient semble alors compromise.

³²⁶ Article R.1112-2 du code de la santé publique ; Article R.4127-45 du code de la santé publique.

³²⁷ Article L.1111-15 du code de la santé publique.

Section 1 : L'ineffectivité du droit d'opposition au traitement des données médicales aux fins de constitution et d'alimentation des dossiers médicaux

99. La mise en œuvre de tout traitement de données à caractère personnel doit être légalement justifiée par l'une des six conditions énumérées à l'article 6 du RGPD. En tant que traitement de données personnelles, la constitution d'un dossier médical doit alors être fondée sur l'une des six bases légales édictées à l'article susvisé. Parmi ces fondements juridiques, un traitement de données personnelles peut être licitement instauré lorsqu'il est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis³²⁸. Le cas échéant, le droit d'opposition consacré à l'article 21 du RGPD devient inopérant. C'est ainsi que le traitement des données personnelles du patient ayant pour finalité la constitution de son dossier de soins représente une obligation réglementaire pour les établissements et les professionnels de santé auquel le patient ne peut s'opposer (**Paragraphe 1**). Si le droit d'opposition à la constitution des dossiers de soins se révèle formellement inefficace, son application peut hypothétiquement être envisagée dans le cadre du traitement de données à caractère personnel dénommé Dossier Médical Partagé (**Paragraphe 2**).

Paragraphe 1 : L'obligation de constitution des dossiers de soins

100. Alors que le patient ne peut s'opposer ni à la constitution de son dossier médical hospitalier (**A**) ni à la création de sa fiche d'observation personnelle (**B**), ce dernier peut néanmoins refuser la tenue de notes personnelles le concernant par le professionnel de santé (**C**). En effet, si la constitution des dossiers de soins correspond à une obligation légale qui incombe au responsable de traitement, la prise de notes personnelles demeure facultative.

A) L'inopposition à l'obligation de constitution du dossier médical hospitalier

101. Préalablement à la mise en œuvre de tout traitement de données à caractère personnel, il convient de définir la base légale du traitement au regard de sa finalité. La définition de la base légale est primordiale, elle permet d'autoriser le traitement sur le plan juridique, et de déterminer les droits que la personne concernée détient sur ses données personnelles. En

³²⁸ Article 6.1 c) du RGPD.

effet, les droits de la personne concernée dépendent du fondement juridique sur lequel repose le traitement. En d'autres termes, le droit d'effectuer un traitement de données personnelles pour son responsable peut, à l'inverse, réduire les droits de la personne concernée à leur égard. Au sein de ce paragraphe, nous allons définir la base légale du traitement ayant pour finalité la constitution du dossier de soins, pour ensuite examiner les conséquences engendrées pour les droits des patients concernés.

102. Bien que tout traitement des données médicales est par principe interdit, il peut être autorisé lorsque la nécessité du traitement correspond à l'une des exceptions mentionnées à l'article 9.2 du RGPD³²⁹. Le législateur européen autorise ainsi le traitement des données médicales lorsqu'il est nécessaire à la prise en charge sanitaire des patients³³⁰. Si le traitement des données médicales à des fins de constitution des dossiers médicaux apparaît indispensable à la prise en charge sanitaire du patient, ce traitement doit, au surplus, être justifié par un fondement juridique autrement dénommé « base légale »³³¹. Parmi les six bases légales fixées à l'article 6 du RGPD, un traitement de données peut être mise en œuvre lorsqu'il est nécessaire au respect d'une obligation légale à laquelle le responsable de traitement est soumis³³².

103. Dans le cadre de la prise en charge sanitaire du patient, les établissements de santé ont l'obligation de constituer un dossier médical pour chaque personne admise ou hospitalisée. Cette obligation, à valeur réglementaire, est instituée à l'article R.1112-2 du code de la santé publique. Dès lors, le traitement des données médicales ayant pour finalité l'obligation de constitution du dossier médical hospitalier peut-il reposer sur la base légale susvisée ? Dans le cadre de sa mission d'accompagnement à la mise en conformité au RGPD³³³, la CNIL a élaboré une fiche pratique relative à « *l'obligation légale du responsable de traitement* »³³⁴, dans laquelle quatre conditions cumulatives requises à la détermination de cette base juridique sont détaillées.

³²⁹ Cf. Paragraphe 17.

³³⁰ Article 9.2 h) du RGPD.

³³¹ Cf. Paragraphe 19.

³³² Article 6.1 c) du RGPD.

³³³ Article 8 I. 2° b) de la loi Informatique et Libertés modifiée.

³³⁴ CNIL, *L'obligation légale : dans quels cas fonder un traitement sur cette base légale ?*, 02 décembre 2019. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 15 février 2020.

Premièrement, « *l'obligation doit être définie par le droit européen ou le droit national auquel le responsable de traitement est soumis* »³³⁵. En l'espèce, l'obligation de constitution du dossier médical hospitalier a d'abord été érigée par un décret du 30 mars 1992³³⁶, puis par un décret du 21 mai 2003³³⁷. Désormais, cette obligation est codifiée à l'article R.1112-2 du code de la santé publique. Il en advient que l'injonction de constituer un dossier médical hospitalier est effectivement définie par le droit national français. Deuxièmement, les « *dispositions légales doivent instituer une obligation impérative de traiter des données personnelles, suffisamment claire et précise* »³³⁸. Dans la rédaction de l'article susvisé, il est mentionné qu'« *un dossier médical est constitué pour chaque patient hospitalisé* »³³⁹. Cette formulation affirmative ne laisse pas de place au doute. La constitution du dossier médical hospitalier n'est ni une suggestion, ni une possibilité offerte aux établissements de santé. Le dossier médical doit être constitué par le simple fait de l'hospitalisation ou de l'admission du patient. Autrement dit, dès lors qu'un patient est pris en charge au sein d'un établissement de santé, un dossier médical hospitalier doit être créé. Le verbe *être* aurait pu être précédé du verbe *devoir* afin de marquer l'obligation pesant à la charge des établissements de santé. En tout état de cause, les dispositions de l'article R.1112-2 du code de la santé publique instituent une obligation impérative. Troisièmement, les dispositions de l'obligation légale « *doivent au moins définir les finalités du traitement concerné* »³⁴⁰. Lorsqu'un patient est admis au sein d'un établissement de santé, ses données médicales sont générées aux fins de sa prise en charge sanitaire. Si la constitution du dossier médical hospitalier constitue une finalité de traitement à part entière, elle contribue directement à l'objectif global de la prise en charge sanitaire du patient. En plus d'être légitime, la création obligatoire d'un dossier médical hospitalier constitue une finalité explicite et déterminée par les dispositions réglementaires susvisées. Quatrièmement, « *cette*

³³⁵ *Ibid.*

³³⁶ Décret n°92-329 du 30 mars 1992 relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santé publics et privés et modifiant le code de la santé publique, *JORF* n°78, 1^{er} avril 1992 p. 4607.

³³⁷ Décret n° 2003-462 du 21 mai 2003 relatif aux dispositions réglementaires des parties I, II et III du code de la santé publique, *JORF* n°122, 27 mai 2003, p. 37006.

³³⁸ CNIL, *L'obligation légale : dans quels cas fonder un traitement sur cette base légale ?*, *loc. cit.*

³³⁹ Article R.1112-2 du code de la santé publique.

³⁴⁰ *Ibid.*

obligation doit s'imposer au responsable du traitement, et non aux personnes concernées par le traitement »³⁴¹. La constitution du dossier médical hospitalier est une obligation qui incombe uniquement aux établissements de santé publics ou privés responsables de traitement. Il n'appartient en aucun cas aux patients de constituer leur propre dossier de soins.

L'ensemble de ces quatre conditions étant remplies, le traitement visant à la constitution du dossier médical hospitalier peut licitement reposer sur l'obligation légale qui incombe aux responsables de traitement. Néanmoins, la détermination de cette base légale n'est pas sans incidence sur les droits des patients concernés sur leurs données médicales et, en particulier, sur leur droit d'opposition à ce traitement de données sensibles.

104. Effectivement, les dispositions de l'article 56 de la loi Informatique et Libertés modifiée précisent que « *le droit d'opposition s'exerce dans les conditions prévues à l'article 21 du* » RGPD et qu'il « *ne s'applique pas lorsque le traitement répond à une obligation légale* ». En ce sens, les dispositions de l'article 21 du RGPD, auxquelles la loi Informatique et Libertés modifiée renvoie, énoncent que le droit d'opposition au traitement peut uniquement être exercé lorsque la base légale du traitement repose sur l'exécution d'une mission d'intérêt public dont le responsable de traitement est investi³⁴², ou sur les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers³⁴³. Les dispositions du RGPD affirment implicitement que l'opposition au traitement est inenvisageable lorsque la base légale du traitement est fondée sur l'obligation légale qui incombe au responsable de traitement. Autrement dit, le simple fait que la base légale du traitement aux fins de constitution du dossier médical hospitalier repose sur une obligation réglementaire suffit à faire obstacle à la possibilité, pour le patient concerné, de s'y opposer³⁴⁴. Il en résulte que les patients ne peuvent s'opposer à ce que leurs données médicales recueillies ou produites par les acteurs du système de santé y soient formalisées.

³⁴¹ CNIL, *L'obligation légale : dans quels cas fonder un traitement sur cette base légale ?*, loc. cit.

³⁴² Article 6.1 e) du RGPD.

³⁴³ Article 6.1 f) du RGPD.

³⁴⁴ CNIL, Délibération n°2020-081 du 18 juin 2020 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux, *JORF*, texte 94, 28 juillet 2020.

105. En l'espèce, l'exercice du droit d'opposition au traitement empêcherait l'exécution de l'obligation légale consistant en la création d'un dossier de soins qui pèse sur les établissements de santé. La limitation réglementaire du droit d'opposition apparaît donc justifiée, légitime et compréhensible. Assurément, si le patient s'opposait à la constitution de son dossier médical hospitalier, les établissements de santé ne pourraient satisfaire à leur obligation. Le cas échant, ce manquement serait constitutif d'une faute d'organisation et de fonctionnement du service hospitalier. En ce sens, le juge civil considère que la création et la bonne tenue d'un dossier de soins pour chaque patient est une obligation qui appartient à l'établissement de santé privé³⁴⁵. Le juge administratif observe également que le manquement d'un praticien hospitalier dans la tenue du dossier médical d'un patient est de nature à engager la responsabilité de l'établissement public de santé³⁴⁶. Force est donc de remarquer que l'exercice du droit d'opposition du patient s'opposerait à l'exécution de l'obligation légale à laquelle les établissements de santé sont soumis. A ce titre, le droit d'opposition à la constitution et à l'alimentation du dossier médical hospitalier ne peut être qu'ineffectif. L'autodétermination informationnelle du patient se trouve donc limitée au profit de sa prise en charge sanitaire. Certainement, l'obligation réglementaire pesant sur les établissements de santé est instituée dans l'intérêt de la coordination et de la continuité des soins du patient.

Alors que le patient ne peut s'opposer à la formalisation de ses données médicales au sein de son dossier médical hospitalier, qu'en est-il lorsqu'il est pris en charge en médecine de ville ?

B) L'inopposition à l'obligation de constitution des fiches d'observation personnelles

106. La médecine de ville regroupe les professionnels de santé libéraux ou salariés, qui exercent à titre individuel ou en cabinet, en groupe ou de manière coordonnée³⁴⁷.

³⁴⁵ Civ. 1^{ère}, 26 septembre 2018, n° 17-20.143, Bull. civ., ; D., 2018, n° 39 p. 2153, obs. M. Bacache, A. Guégan et S. Porchy-Simon ; RTD civ. 2019, n° 01, p. 119, obs. P. Jourdain ; Revue Responsabilité civile et assurances, 2018, n° 12, comm. 306, note L. Bloch ; Gaz. Pal., 2018, n° 35, p. 29, note C. Berlaud ; CA de Riom, ch. sociale, 6 mars 2018, n° 15/03035.

³⁴⁶ CAA de Marseille, 2^{ème} ch., 12 avril 2018, n° 15MA03742.

³⁴⁷ Définition de l'ARS disponible en ligne sur le site [www.ars.sante.fr]. Consulté le 17 février 2020.

107. Dès lors que le patient est pris en charge au sein d'une maison ou d'un centre de santé, une obligation réglementaire de constitution d'un dossier de soins incombe également à ces structures non-hospitalières. En effet, l'article D.6323-5 du code de la santé publique dispose qu'un dossier, comportant l'ensemble des informations de santé nécessaires aux décisions diagnostiques et thérapeutiques, doit être constitué pour chaque patient pris en charge dans un centre de santé. Bien que ces dossiers soient alimentés par les professionnels de santé exerçant au sein de cette structure, la conservation et la confidentialité de ce dossier relève de la responsabilité de la structure sanitaire en sa qualité de personne morale³⁴⁸. A l'instar des établissements de santé, les centres de santé sont des structures non-hospitalières assurant une prise en charge pluriprofessionnelle associant des professionnels et des auxiliaires médicaux³⁴⁹. Les actions réalisées par chacun de ces acteurs de santé doivent alors être détaillées et tracées dans un dossier propre à chaque patient. L'obligation de constitution du dossier médical semble donc être en lien avec la coordination des soins dispensés par plusieurs professionnels de santé autour d'un même patient. Assurément, la principale fonction du dossier médical est de garantir « *la traçabilité des actions effectuées dans le cadre de la prise en charge de chaque patient* »³⁵⁰. En application du syllogisme applicable à la détermination de la base légale d'un traitement de données personnelles, nous pouvons conclure que le fondement garantissant la licéité de la constitution du dossier des maisons et centres de santé repose sur l'obligation réglementaire du responsable de traitement. Par conséquent, les patients pris en charge au sein de telles structures ne peuvent s'opposer à la création et à la tenue de ce dossier de soins particulier.

108. Hormis l'hypothèse où la prise en charge médicale est réalisée de façon coordonnée au sein d'un centre de santé, il ne semble pas exister d'obligation légale ou réglementaire de création d'un dossier de soins à la charge du médecin de ville. Il pèse toutefois, sur tout médecin, l'obligation déontologique de tenir des fiches d'observation personnelles à chaque patient³⁵¹. Dès lors, le patient peut-il s'opposer à ce traitement ? L'établissement des fiches d'observation personnelles repose sur l'obligation déontologique qui incombe personnellement au médecin. Afin de déterminer si l'exercice du droit d'opposition est

³⁴⁸ Article D.6323-6 du code de la santé publique.

³⁴⁹ Article L.6323-1 du code de la santé publique.

³⁵⁰ Article D.6323-5 alinéa 3 du code de la santé publique.

³⁵¹ Cf. Paragraphe 109.

envisageable dans ce contexte, il convient de définir si une obligation déontologique peut être regardée comme une obligation légale au sens du RGPD.

109. Selon la CNIL, « *le RGPD n'impose pas de niveau de norme particulier : cette obligation légale peut donc découler de règlements européens, d'une loi, d'un décret, d'un arrêté, etc.* »³⁵². D'une part, les cinq premières versions du code de déontologie médicale ont été prises par décret³⁵³ avant que ces dispositions ne soient intégrées au sein de la partie réglementaire du code de la santé publique³⁵⁴, aux articles R.4127-1 à R.4127-112. D'autre part, l'appréciation des règles de déontologie médicale sont soumises au contrôle de légalité du Conseil d'Etat et doivent se conformer à la hiérarchie des normes. La valeur des obligations déontologiques est donc de nature réglementaire. Ainsi, la base légale de la constitution des fiches d'observation personnelles, en tant que traitement de données rendu obligatoire par des dispositions réglementaires, repose sur une obligation considérée, par le législateur européen, comme légale. Il en advient que les patients ne peuvent s'opposer à ce traitement impératif. A défaut, les médecins commettraient une infraction aux dispositions du code de déontologie médicale. En ce sens, la Chambre disciplinaire nationale de l'Ordre des médecins³⁵⁵ a prononcé une interdiction temporaire d'exercer d'une durée d'un an, dont six mois avec sursis, à l'encontre d'un médecin pour violation de l'article 45 du code de déontologie médicale. Il ressort de l'instruction de ce dossier que les fiches d'observation personnelles, tenues par le médecin contrevenant, ne contenaient que des renseignements sommaires et ne permettaient pas d'assurer le bon suivi médical des patients. Il ressort de cette décision que l'activité professionnelle du médecin peut être mise en cause dès lors qu'il ne satisfait pas à son obligation déontologique de constitution et de bonne tenue des fiches d'observation personnelles aux patients. La prise en charge médicale du patient implique

³⁵² CNIL, *L'obligation légale : dans quels cas fonder un traitement sur cette base légale ?*, loc. cit.

³⁵³ Décret n° 47-1169 du 27 juin 1947 portant code de déontologie médicale, *JORF* du 28 juin 1947, p. 5993 ; Décret n°55-1591 du 28 novembre 1955 abroge et remplace le d. 47-1169 du 27-06-1947, portant code de déontologie médicale, *JORF*, 6 décembre 1955, p. 11856 ; Décret n°79-506 du 28 juin 1979 portant code de déontologie médicale, *JORF*, 30 juin 1979, p.1565 ; Décret n°95-1000 du 6 septembre 1995 portant code de déontologie médicale, *JORF* n°209, 8 septembre 1995, p. 13305 .

³⁵⁴ Décret n° 2004-802 du 29 juillet 2004 relatif aux parties IV et V (dispositions réglementaires) du code de la santé publique et modifiant certaines dispositions de ce code Les dispositions réglementaires des parties IV et V du code de la santé publique font l'objet d'une publication spéciale annexée au Journal officiel de ce jour (voir à la fin du sommaire), *JORF* n°183, 8 août 2004, texte n° 5.

³⁵⁵ Chambre disciplinaire nationale de l'Ordre des médecins, 24 juin 2004, n°8856.

donc obligatoirement la constitution d'un dossier de soins et la formalisation de ses données médicales en son sein.

110. S'il n'est pas juridiquement possible de s'opposer aux traitements aux fins de constitution des fiches d'observation personnelles dans la mesure où ils reposent sur une obligation réglementaire incombant au médecin, le patient peut-il s'opposer au traitement de ses données personnelles ayant pour finalité l'établissement des notes personnelles du professionnel de santé ? Comme exposé précédemment, la frontière entre la fiche d'observation personnelle et les notes personnelles est particulièrement ténue³⁵⁶.

C) L'opposition à la prise de notes personnelles par le médecin

111. Tout professionnel de santé peut, dans le cadre de son activité, prendre des notes personnelles relatives aux patients qui le consultent. Pour qu'elles soient qualifiées de notes personnelles, ces informations ne doivent pas contribuer à l'élaboration et au suivi du diagnostic et de la thérapeutique du patient³⁵⁷. Autrement dit, les notes du professionnel de santé ne lui sont « personnelles » que lorsqu'elles n'apportent pas de plus-value médicale dans le cadre de la prise en charge du patient. Définies au regard de leur fonction, les notes personnelles prises par le médecin peuvent, entre autres, relater des comportements ou des propos du patient ou faire état de sa vie privée ou professionnelle à condition qu'elles ne présentent aucune utilité pour sa prise en charge médicale. Selon la chambre disciplinaire du Conseil national de l'Ordre des médecins, les notes personnelles qui contiennent, pour l'essentiel, des informations sur la vie familiale et les relations d'un patient avec son entourage témoignent de la relation de confiance qui s'est établie entre le patient et le médecin³⁵⁸. Quand bien même les notes personnelles du médecin ne contiendraient pas de données médicales nécessaires à la prise en charge sanitaire du patient, le fait est qu'elles comportent des données personnelles concernant le patient. Dès lors, le patient peut-il exercer son droit d'opposition au traitement ? Pour répondre à cette question, nous devons, à

³⁵⁶ Cf. Paragraphe 62.

³⁵⁷ Cf. Paragraphe 71.

³⁵⁸ Chambre disciplinaire nationale de l'Ordre des médecins, 17 mars 2016, n°12639.

nouveau, déterminer la base légale justifiant la nécessité, pour le professionnel de santé, de prendre des notes concernant les patients.

112. En considération des bases légales définies à l'article 6 du RGPD, la prise de notes personnelles ne peut être fondée sur la sauvegarde des intérêts vitaux de la personne concernée³⁵⁹. En effet, les notes personnelles étant définies au regard de leur fonction, elles ne peuvent être nécessaires à la prise en charge médicale du patient. Dans le cas contraire, ces notes devraient être versées dans son dossier de soins. En outre, même si la prise en charge médicale repose sur un contrat de soins, la prise de notes personnelles n'est pas strictement nécessaire³⁶⁰ à l'exécution d'un contrat auquel le patient serait partie³⁶¹. En effet, la prise en charge médicale implique uniquement le traitement de données médicales et de santé intégrées au sein des dossiers de soins. Par ailleurs, les notes personnelles n'apparaissent pas nécessaires au respect d'une obligation légale à laquelle le professionnel de santé est soumis³⁶² puisqu'aucune disposition juridique n'impose une telle injonction aux professionnels de santé. Pour le reste, la prise de notes personnelles n'est pas nécessaire à l'exécution d'une mission d'intérêt public dont est investi le responsable du traitement dans l'exécution de ses missions³⁶³. En effet, la prise de notes personnelles ne correspond pas à une prérogative publique définie par un texte. Quatre bases légales sur les six fixées par le RGPD étant écartées, il convient de rechercher si les notes personnelles peuvent être nécessaires aux fins des intérêts légitimes poursuivis par le responsable du traitement³⁶⁴. A défaut, seul le consentement du patient pourrait fonder ce traitement³⁶⁵.

113. La CNIL indique que « *le recours à l'intérêt légitime pour fonder légalement un traitement est soumis à trois conditions* »³⁶⁶. En premier lieu, l'intérêt poursuivi doit évidemment être *légitime*. La CNIL présume la légitimité de l'intérêt poursuivi lorsqu'il est

³⁵⁹ Article 6.1 d) du RGPD.

³⁶⁰ Article 5.1 c) du RGPD.

³⁶¹ Article 6.1 b) du RGPD.

³⁶² Article 6.1 c) du RGPD.

³⁶³ Article 6.1 e) du RGPD.

³⁶⁴ Article 6.1 f) du RGPD.

³⁶⁵ Article 6.1 a) du RGPD.

³⁶⁶ CNIL, *L'intérêt légitime : comment fonder un traitement sur cette base légale ?*, 02 décembre 2019. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 15 février 2020.

manifestement licite au regard du droit, déterminé de façon claire et précise et qu'il n'est pas fictif³⁶⁷. L'intérêt de prendre des notes personnelles peut résulter de la nécessité d'établir une relation de confiance entre le professionnel de santé et le patient. La relation médicale est avant tout une relation humaine entre deux individus au cours de laquelle le patient livre ses confidences au professionnel de santé. A l'instar d'un memento, la prise de notes personnelles peut permettre de contextualiser la prise en charge médicale et de se remémorer les particularités personnelles du patient. Une telle prise de note n'est ni illicite, ni fictive, ni obscure. L'intérêt poursuivi par le professionnel de santé apparaît donc légitime. En effet, tout professionnel, quel que soit le domaine d'activité, est amené à prendre des notes dans le cadre de l'exercice de sa profession. L'ensemble des notes prises à cette occasion ne sert pas nécessairement à l'accomplissement de la mission dont est investi le professionnel, mais peut néanmoins s'avérer utiles dans un contexte général. A titre d'illustration, au cours d'un premier rendez-vous, l'avocat qui reçoit un client va colliger un certain nombre d'éléments, dont des données à caractère personnel, qui n'auront pas forcément vocation à être réutilisées dans le traitement de l'affaire qui lui est soumise. De la même manière, dans le cadre de l'activité médicale, le professionnel de santé peut également prendre des notes étrangères à l'établissement du diagnostic ou de la thérapeutique mais qui, pour autant, seront utiles dans le cadre de la contextualisation de cette activité humaine et intime.

En deuxième lieu, « *l'intérêt légitime ne peut être retenu que si le traitement satisfait à la condition de "nécessité"* »³⁶⁸. Dans le cadre de la relation médicale, le professionnel de santé ne peut pas retenir l'ensemble des histoires personnelles et des particularités propres à chacun des patients. Si l'ensemble des informations médicales ou personnelles ayant un lien avec la prise en charge médicale sont incluses dans le dossier de soins du patient, il est important que le professionnel de santé puisse également se souvenir des éléments contextuels et personnels de la personne qui le consulte. La prise de notes se révèle alors nécessaire. En effet, si le professionnel de santé venait à mélanger ou oublier les confidences de ses patients, le lien de confiance qui les unit pourrait être fragilisé. En complément, la CNIL précise qu'en vertu de cette condition de nécessité, le traitement de données doit permettre d'atteindre l'unique objectif poursuivi. Il en résulte que la prise de notes personnelles ne doit pas conduire à une immixtion dans les affaires de famille ni dans la vie

³⁶⁷ *Ibid.*

³⁶⁸ *Ibid.*

privée des patients³⁶⁹, et encore moins à un abus de faiblesse d'une personne vulnérable³⁷⁰. Dans le cadre de la relation médicale entre le patient et le professionnel de santé, la prise de notes personnelles doit être indispensable pour encrer un contexte ou une situation personnelle dont le professionnel de santé a besoin de se souvenir.

En troisième et dernier lieu, « *le traitement ne doit pas heurter les droits et intérêts des personnes dont les données sont traitées, compte tenu de leurs attentes raisonnables* »³⁷¹. Autrement dit, les intérêts poursuivis par le professionnel de santé ne doivent pas créer de « *déséquilibre au détriment des droits et intérêts des personnes dont les données sont traitées* »³⁷². Selon le principe du secret professionnel, « *le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris* »³⁷³. Plus généralement, « *ce secret couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel* »³⁷⁴ intervenant dans le système de santé. Le secret professionnel n'est pas limité aux informations médicales mais bien à toute information relative au patient. En conséquence, les confidences et les éléments relatifs à la vie privée du patient ne peuvent, en aucun cas, sortir du cadre de la relation médicale. De surcroît, la violation du secret professionnel médical est sanctionnée pénalement³⁷⁵ et disciplinairement³⁷⁶. Les données personnelles relatives au patient, contenues au sein des notes personnelles prises par le professionnel de santé, font donc l'objet d'une protection légale. Les droits et les intérêts en cause en sont ainsi pondérés.

114. Compte tenu de la démonstration qui précède, nous pouvons considérer que le traitement visant à la prise de notes personnelles peut être légalement fondé sur les intérêts légitimes poursuivi par le professionnel de santé. Dès lors, il résulte du RGPD que le patient,

³⁶⁹ Article R.4127-51 du code de la santé publique.

³⁷⁰ Article 223-15-2 du code pénal.

³⁷¹ CNIL, *L'intérêt légitime : comment fonder un traitement sur cette base légale ?*, loc. cit.

³⁷² *Ibid.*

³⁷³ Article R.4127-4 du code de la santé publique.

³⁷⁴ Article L.1110-4 du code de la santé publique.

³⁷⁵ Article 226-13 du code de la santé publique.

³⁷⁶ Article 4127-1 du code de la santé publique.

en tant que personne concernée, peut exercer son droit d'opposition au traitement de ses données personnelles³⁷⁷. En d'autres termes, le patient peut refuser que le professionnel de santé prenne des notes personnelles le concernant. Dans ce cas, le professionnel de santé ne pourra prendre des notes relatives à son patient, « *à moins qu'il ne 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* »³⁷⁸. Par définition, est impérieux ce « *qui s'impose avec le caractère d'une obligation qu'il faut absolument satisfaire* »³⁷⁹ Dans le cadre de la relation médicale, la prise de notes personnelles ne présente pas de caractère impérieux dans la mesure où ces informations ne peuvent directement contribuer à la prise en charge sanitaire. Le patient doit donc pouvoir effectivement exercer son droit d'opposition au traitement conféré par le RGPD. Toutefois, pour faire valoir ce droit, encore faut-il que le patient soit informé de la prise de notes à son égard, des droits qu'il détient sur celles-ci et particulièrement de son droit d'opposition « *présenté clairement et séparément de toute autre information* »³⁸⁰.

Paragraphe 2 : La constitution du Dossier Médical Partagé

115. Au moment de la création automatique du DMP lors de l'ouverture automatique de l'ENS, son titulaire bénéficie du droit de s'y opposer (**A**). Cependant, une fois que le DMP a été effectivement créé, son titulaire ne peut faire obstacle à son alimentation (**B**). Assurément, le traitement de données médicales consistant au remplissage du DMP constitue une obligation légale incombant aux professionnels de santé participant à la prise en charge médicale de son titulaire. Par conséquent, le patient ne peut contrarier l'exercice de cette exigence.

³⁷⁷ Article 21.1 du RGPD.

³⁷⁸ *Ibid.*

³⁷⁹ Définition du dictionnaire Larousse. Disponible en ligne sur le site [www.larousse.fr]. Consulté le 19 février 2020.

³⁸⁰ Article 21.4 du RGPD.

A) *L'opposition à la création du Dossier Médical Partagé*

116. Antérieurement à l'entrée en vigueur de l'article 50 de la loi Ma Santé 2022³⁸¹, la création du DMP nécessitait le consentement exprès et éclairé de son titulaire ou, le cas échéant, de son représentant légal. La création du DMP était donc soumise à la manifestation de volonté de la personne concernée. Lorsque le bénéficiaire de l'Assurance maladie souhaitait ouvrir son DMP, il pouvait directement le créer en ligne sur un portail internet dédié, en s'adressant à un professionnel de santé muni d'un logiciel compatible avec le DMP, ou aux agents de sa Caisse primaire d'assurance maladie (CPAM). Dans le cas où le titulaire du DMP était mineur au moment de sa création, ce dernier devait consentir à la conservation de son DMP à sa majorité. La création de ce dossier médical numérique était donc perçue comme une prérogative facultative offerte aux bénéficiaires de l'Assurance maladie. Autrement dit, le DMP ne pouvait être créé que sous l'impulsion de la personne concernée. Alors que ce dossier était déjà reconsidéré comme l'outil de coordination du professionnel de santé³⁸², son existence dépendait de l'assentiment de son titulaire. Seulement, pour que le bénéficiaire de l'Assurance maladie ait pu en solliciter la création, encore fallait-il qu'il ait connaissance de l'existence de ce dispositif et, le cas échéant, ait compris les enjeux liés à sa finalité³⁸³. Les informations relatives aux finalités du DMP et aux modalités de sa création, de son accès, de sa clôture et de sa destruction étaient mises à disposition sur le site internet de l'Assurance maladie³⁸⁴, ainsi que sur celui dédié au DMP³⁸⁵. Pour être informé, le patient devait donc rechercher, par lui-même, les éléments d'information pouvant éclairer sa décision de créer un carnet de santé numérique.

117. Dorénavant, le Dossier Médical Partagé est ouvert automatiquement, sauf opposition de la personne concernée ou de son représentant légal³⁸⁶. Le DMP étant devenu l'une des composantes principales de l'ENS, le succès de cet espace numérique dépend inextricablement de l'existence de ce dossier numérique. C'est ainsi que « *l'ouverture*

³⁸¹ Article 50 de la loi n°2019-774 du 24 juillet 2019, *loc. cit.*

³⁸² Cf. Paragraphe 76.

³⁸³ Selon l'article L.1111-14 du code de la santé publique, le DMP a pour finalité de « *favoriser la prévention, la coordination, la qualité et la continuité des soins* ».

³⁸⁴ Site internet disponible à l'adresse : [www.ameli.fr].

³⁸⁵ Site internet disponible à l'adresse [www.dmp.fr].

³⁸⁶ Article L.1111-14 du code de la santé publique dans sa version en vigueur au 1^{er} juillet 2021.

automatique de l'espace numérique de santé [...] emporte la création automatique du dossier médical partagé »³⁸⁷. Si les pouvoirs publics ont imposé l'instauration de ces dispositifs de partage dématérialisé des données médicales du patient sur l'ensemble du territoire et par-delà ses frontières³⁸⁸, c'est dans l'unique espoir d'accélérer et de faciliter le virage numérique en santé³⁸⁹. Il en résulte que la création du DMP n'est plus soumise à l'accord préalable de la personne concernée. C'est ainsi qu'au premier trimestre de l'année 2022, soixante-neuf millions d'assurés sociaux ont été préalablement et individuellement informés de l'ouverture de leur ENS et de la création de leur DMP par courrier électronique³⁹⁰. Ils disposaient alors d'un délai de six semaines à compter de cet envoi pour s'opposer à leur déploiement respectif³⁹¹. Bien que le DMP soit désormais intégré dans l'ENS par l'intermédiaire duquel il est accessible, l'opposition à la création de l'un n'emporte pas la fermeture de l'autre. En l'absence d'opposition à leur déploiement dans le délai susvisé, ces dispositifs numériques ont été instaurés par défaut. Néanmoins, la création effective du DMP n'emporte pas son existence perpétuelle. En effet, son titulaire peut procéder à sa clôture à tout moment³⁹² « *soit directement, soit en en formulant la demande auprès de l'opérateur de l'espace numérique de santé* »³⁹³. Dans l'hypothèse où l'assuré social revenait sur sa décision, il pourrait, à tout moment, en demander une nouvelle création³⁹⁴. Le cas échéant, les données intégrées dans son DMP initial, et archivées pendant un délai de dix ans, seraient versées dans son nouveau dossier numérique³⁹⁵. Il en est exactement de même pour son espace numérique personnel³⁹⁶. Il en ressort que la création automatique de ce dossier médical numérique ne présente pas un caractère obligatoire.

³⁸⁷ Article L.1111-14 alinéa 2 du code de la santé publique.

³⁸⁸ Article L.1111-22 du code de la santé publique.

³⁸⁹ Voir : MILON (A.), *Rapport n°524 fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé*, Sénat, 22 mai 2019, p. 188 à p. 211.

³⁹⁰ Article R.1111-28 alinéa 1 du code de la santé publique.

³⁹¹ Article R.1111-28 alinéa 6 du code de la santé publique.

³⁹² Article R.1111-52 du code de la santé publique.

³⁹³ Article R.1111-36 alinéa 1 du code de la santé publique.

³⁹⁴ Article R.1111-36 alinéa 4 du code de la santé publique.

³⁹⁵ *Ibid.*

³⁹⁶ *Ibid.*

118. En revanche, bien qu'elle soit favorable à la sécurité des soins des individus, l'instauration automatique de ces dispositifs numériques semble comporter un caractère contraignant pour les personnes déconnectées. Effectivement, les dispositions réglementaires relatives au fonctionnement du DMP prévoient que « *le titulaire est informé de la création de son dossier médical et de son articulation avec son espace numérique de santé, à l'occasion de l'information individuelle* »³⁹⁷ délivrée « *au moyen d'un courrier électronique adressé à l'adresse déclarée auprès de celui-ci* »³⁹⁸. Seulement, parmi l'ensemble des personnes concernées, plus de 15 % ne disposait pas d'une connexion internet à domicile³⁹⁹ et n'était pas équipé d'un ordiphone⁴⁰⁰. Le cas échéant, comment pouvaient-elles être informées de ces traitements de données sensibles et, subséquemment, exercer leur autodétermination informationnelle ? De surcroît, cette information délivrée au patient *via* les technologies de l'information et de la communication portait également sur « *les modalités de création, de clôture et de destruction du dossier médical partagé, ainsi que les modalités d'accès par lui-même et par les professionnels, établissements de santé, établissements ou services sociaux ou médico-sociaux appelés à le prendre en charge, de ses droits sur les données contenues et des droits particuliers dont bénéficie son médecin traitant* »⁴⁰¹. Cette information essentielle sur le fonctionnement de l'outil principal du partage de leurs données médicales avec les professionnels participant à leur parcours de santé pourrait alors ne jamais leur parvenir. Force est d'observer que ces deux traitements, mis en œuvre pour le compte de l'Etat, ne respectent pas le principe de transparence consacré à l'article 12 du RGPD. En effet, ce principe « *exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples* »⁴⁰². Il en résulte que la fracture numérique emporte des inégalités dans l'accès aux droits des personnes concernées à l'égard de leurs données à caractère personnel. « *De manière évidente, l'environnement*

³⁹⁷ Article R.1111-40 du code de la santé publique.

³⁹⁸ Article R.1111-28 du code de la santé publique.

³⁹⁹ Autorité de régulation des communications électroniques, des postes et de la distribution de la presse , *Enquête sur la diffusion des technologies de l'information et de la communication dans la société française*, Baromètre du numérique, 2021, p. 56.

⁴⁰⁰ Autorité de régulation des communications électroniques, des postes et de la distribution de la presse , *op. cit.* p. 27.

⁴⁰¹ Article R.1111-40 alinéa 2 du code de la santé publique.

⁴⁰² Considérant 39 du RGPD.

numérique renforce certaines vulnérabilités. »⁴⁰³. Pourtant, quels que soient les milliards d'euros versés pour le développement du numérique en santé, le succès de ces dispositifs repose principalement sur leur appréhension et leur adhésion par les sujets principaux : les patients. Si les données médicales permettent d'optimiser les prises en charge sanitaires, la personne vulnérable devrait également être en mesure « *de stocker et partager ses documents et ses données de santé en toute sécurité pour être mieux soigné[e]* »⁴⁰⁴. Si le DMP est considéré comme un vecteur de démocratie sanitaire, une proportion de la population française semble en être écartée.

119. Tandis que les assurés sociaux disposent théoriquement du droit de s'opposer à la création de leur DMP, ces derniers ne peuvent s'opposer à son alimentation dès lors qu'il leur a été effectivement ouvert.

B) L'inopposition à l'obligation d'alimentation du Dossier Médical Partagé

120. Lorsque l'assuré social ne s'est pas opposé à la création de son DMP, les professionnels de santé qui le prennent en charge ont le devoir de l'alimenter⁴⁰⁵. Si le titulaire du DMP dispose de la maîtrise des données qu'il y consigne à titre personnel, ce dernier peut-il s'opposer à son remplissage par les professionnels de santé ? Afin de pouvoir statuer sur l'existence de ce droit, il convient d'identifier le responsable du traitement consistant en l'alimentation du DMP d'une part, et de déterminer la base juridique sur laquelle repose ce traitement d'autre part. La qualification des parties au traitement est essentielle dans la mesure où le responsable de traitement et le sous-traitant supportent des fonctions, des obligations et des responsabilités qui leurs sont propres⁴⁰⁶. Par conséquent, « *l'identification de l'ensemble des opérations d'un traitement composant un traitement de données à caractère personnel revêt une importance particulière en cas de pluralité d'acteurs intervenant pour mettre en œuvre le traitement* »⁴⁰⁷. Néanmoins, cette caractérisation s'avère

⁴⁰³ DOUVILLE (T.), HERVOCHON (C.), NOËL (E.), PAQUIER (Y.), *Les vulnérabilités numériques*, Cahiers de la recherche sur les droits fondamentaux, 2020, n°18, p. 111.

⁴⁰⁴ Assurance maladie, *Réussir ensemble mon espace santé*, Point presse du 29 avril 2021. Disponible en ligne sur le site [www.esante.gouv.fr]. Consulté le 19 novembre 2021.

⁴⁰⁵ Article L.1111-15 du code de la santé publique.

⁴⁰⁶ Voir : Chapitre IV du RGPD « *Responsable du traitement et sous-traitant* ».

⁴⁰⁷ DOUVILLE (T.), *Droit des données à caractère personnel*, op. cit., p. 57.

délicate au regard de la complexité de l'ensemble des traitements que regroupe le Dossier Médical Partagé.

121. Le remplissage du DMP consiste, pour le professionnel, à y verser les données médicales du patient qu'il prend en charge. Cet acte d'alimentation, par extraction ou enregistrement des informations, correspond à un traitement de données à caractère personnel au sens du RGPD⁴⁰⁸. Le traitement consistant au remplissage du DMP semble alors constituer un traitement distinctif de celui ayant pour finalité sa création. En effet, la CNIL a précisé que la conception et la création du DMP constituaient un traitement de données à caractère personnel⁴⁰⁹. Toutefois, les différentes actions pouvant être réalisées au sein du DMP se déclinent en autant d'opérations de traitement connexes et répondant à une finalité globale : la coordination et la continuité des soins du patient. Il est important de rappeler que le principe de limitation des finalités exige que chaque traitement remplisse un objectif qui soit précisément déterminé et légitime⁴¹⁰. Chacune des opérations de traitement intervenant dans la mise en œuvre du DMP correspond donc à une sous-finalité distincte effectuée par de multiples acteurs. Il en résulte que l'action d'alimentation du DMP constitue un traitement de données connexe au traitement à des fins de sa création. Alors, indépendamment de la conception du DMP, son alimentation semble constituer un traitement de données médicales autonome.

Alors que « *la conception, la mise en œuvre et l'administration du dossier médical partagé* »⁴¹¹ ont légalement été confiées à la CNAM, le traitement aux fins d'alimentation de ce dossier est exécuté par les professionnels de santé participant à la prise en charge médicale de son titulaire. Nous pouvons alors nous interroger sur la qualification des professionnels de santé intervenant dans le cadre de ce traitement spécifique. Afin de déterminer le rôle et les obligations des professionnels de santé quant au traitement consistant en l'alimentation du DMP, il convient de déterminer s'ils agissent en qualité de *responsables de traitement*⁴¹²

⁴⁰⁸ Article 4.2 du RGPD.

⁴⁰⁹ CNIL, Délibération n° 2016-258 du 21 juillet 2016, *loc. cit.*

⁴¹⁰ Article 5.1 b) du RGPD.

⁴¹¹ Article L.1111-14 alinéa 5 du code de la santé publique.

⁴¹² Article 24 du RGPD.

ou de *sous-traitants*⁴¹³. L'enjeu de cette qualification consiste à identifier l'entité qui supporte la responsabilité du traitement et auprès de laquelle la personne concernée peut exercer les droits qui lui sont reconnus sur ses données. Bien qu'il soit capital, cet exercice s'avère délicat lorsque plusieurs acteurs interviennent dans un traitement de données⁴¹⁴.

122. Le responsable de traitement est défini comme la personne ou l'entité qui détermine la finalité et les moyens d'un traitement de données à caractère personnel⁴¹⁵. Dans le cas spécifique du DMP, la finalité (pourquoi) et les moyens (comment) de ce traitement ont été décidés par les pouvoirs publics. Ils ont alors déterminé que les données médicales du patient seraient collectées au moyen d'un dossier médical numérique accessible *via* l'Internet afin de favoriser la prévention, la coordination, la qualité et la continuité de ses soins. Partant, l'ensemble des traitements intervenant dans le cadre général du DMP doivent satisfaire à cette finalité globale. Il en advient que ni la CNAM, ni les professionnels de santé n'ont participé à la détermination de la finalité et des moyens du DMP. Néanmoins, le RGPD rapporte que « *lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné* »⁴¹⁶ par le législateur. La désignation légale du responsable de traitement peut être explicitement nominative. C'est ainsi que le législateur a confié la responsabilité de l'opération de traitement ayant pour objet la conception et le déploiement du DMP à la CNAM⁴¹⁷. Seulement, cette opération particulière de traitement ne correspond pas à celle consistant en l'alimentation du DMP. La CNAM ne semble donc pas être investie de la responsabilité du traitement des données médicales des patients à des fins de remplissage de leur dossier numérique. Par suite, les professionnels de santé peuvent-ils endosser la qualité de responsable du traitement ayant pour finalité l'alimentation du DMP ?

Le Comité européen sur la protection des données (CEPD) considère qu'il est également possible, pour le droit de l'Union ou le droit d'un État membre, de désigner plus

⁴¹³ Article 28 du RGPD.

⁴¹⁴ DELFORGE (A.), *Les obligations générales du responsable du traitement et la place du sous-traitant*, In DE TERWANGNE (C.), ROSIER (K.), *Le règlement général sur la protection des données (RGPD/GDPR)*, *op. cit.*, p. 381.

⁴¹⁵ Article 4.7 du RGPD.

⁴¹⁶ *Ibid.*

⁴¹⁷ Article L.1111-14 alinéa 5 du code de la santé publique.

d'un responsable du traitement⁴¹⁸, notamment lorsque chacun des acteurs intervenant dans une chaîne de traitements effectuent un objectif distinct qui leur est propre⁴¹⁹. Or, seule la CNAM a été expressément désignée par les pouvoirs publics comme l'organisme responsable du traitement dénommé Dossier Médical Partagé. Toutefois, le législateur européen a prévu que la désignation légale d'un responsable de traitement pouvait être déduite de « *critères spécifiques [...] prévus par le droit de l'Union ou par le droit d'un État membre* »⁴²⁰. Concrètement, le CEPD explique que plutôt que de nommer directement le responsable de traitement, « *la loi établira une tâche ou imposera une obligation impliquant, pour une entité, de collecter et de traiter certaines données* »⁴²¹. Dans cette hypothèse, « *le responsable du traitement sera normalement celui désigné par la loi pour la réalisation de l'objectif* »⁴²² déterminé par les pouvoirs publics. A titre d'exemple, l'autorité européenne de contrôle indique que tel est le cas lorsque la loi impose aux entités publiques ou privées des missions qui nécessitent la collecte, la conservation ou la transmission de données personnelles⁴²³. Le cas échéant, « *ces entités seraient alors normalement considérées comme des responsables du traitement en ce qui concerne le traitement nécessaire à l'exécution de ces obligations* »⁴²⁴. Il en résulte qu'un responsable de traitement peut être implicitement et indirectement désigné par l'exécution d'une obligation légale de traiter des données à caractère personnel.

123. Dès lors qu'un patient est effectivement titulaire d'un DMP (en l'absence d'opposition ou de clôture⁴²⁵), son alimentation constitue une obligation légale à la charge des professionnels de santé. En effet, l'article L.1111-15 du code de la santé publique dispose que « *chaque professionnel de santé, quels que soient son mode et son lieu d'exercice, doit reporter dans le dossier médical partagé, à l'occasion de chaque acte ou consultation, les*

⁴¹⁸ CEPD, *Lignes directrices 07/2020 sur les concepts de responsable du traitement et de sous-traitant dans le RGPD*, V. 2.0, 7 juillet 2021, § 22.

⁴¹⁹ CEPD, *Lignes directrices 07/2020 sur les concepts de responsable du traitement et de sous-traitant dans le RGPD*, *op. cit.*, § 72.

⁴²⁰ Article 4.7 du RGPD.

⁴²¹ CEPD, *Lignes directrices 07/2020 sur les concepts de responsable du traitement et de sous-traitant dans le RGPD*, *loc. cit.*

⁴²² *Ibid.*

⁴²³ *Ibid.*

⁴²⁴ *Ibid.*

⁴²⁵ Cf. Paragraphe 117.

éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge ». L'utilisation du verbe *devoir* marque le caractère obligatoire de ce que le sujet est tenu d'acquiescer⁴²⁶. Outre cette obligation générale d'alimentation, les professionnels de santé hospitaliers doivent, en prime, y reporter un résumé des principaux éléments relatifs à l'hospitalisation du patient titulaire du DMP⁴²⁷. De surcroît, le médecin traitant du titulaire du DMP doit, en plus de son obligation générale d'alimentation du DMP consécutivement à tout acte ou consultation, y verser périodiquement, et au moins une fois par an, une synthèse médicale⁴²⁸. A l'aune des lignes directrices formulées par le CEPD, les professionnels de santé légalement obligés d'alimenter le DMP de la personne concernée en sont les responsables de traitement. Il en ressort que le fondement juridique de l'alimentation du DMP repose sur l'obligation légale qui incombe aux professionnels de santé en leur qualité de responsable de traitement.

124. En conséquence, les personnes titulaires d'un DMP ne peuvent théoriquement s'opposer à ce que les professionnels de santé qui les prennent en charge l'alimentent. En effet, l'exercice du droit d'opposition au traitement ne peut s'appliquer lorsque le traitement est nécessaire *« au respect d'une obligation légale à laquelle le responsable du traitement est soumis »*⁴²⁹. L'ineffectivité du droit d'opposition à l'alimentation du DMP est affirmée à l'article R.1111-47 du code de la santé publique. Selon ces dispositions, une fois que l'assuré social ne s'est pas opposé à la création de son DMP, *« il ne peut s'opposer, sauf motif légitime, à ce que ceux-ci [les professionnels de santé] versent dans son dossier médical partagé les données utiles à la prévention, la coordination, la qualité et la continuité des soins »*. Alors que le droit à la protection des données⁴³⁰ exclut toute possibilité d'opposition au traitement lorsque son fondement juridique repose sur l'obligation légale qui incombe au responsable de traitement, le législateur national admet que le titulaire du DMP puisse s'opposer à son alimentation à condition de justifier de motifs légitimes. Selon l'article 21 du RGPD, l'exposé de motifs légitimes tenant à la situation particulière de la personne concernée constitue la

⁴²⁶ Voir : Définition du verbe « devoir » proposé par le CNRTL. Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 21 novembre 2021.

⁴²⁷ Article L.1111-15 alinéa 1 du code de la santé publique.

⁴²⁸ *Ibid.*

⁴²⁹ Article 6.1 c) du RGPD.

⁴³⁰ Article 56 de la loi Informatique et Libertés modifiée ; Article 21 du RGPD.

condition d'exercice du droit d'opposition lorsque celui-ci lui est effectivement reconnu. Par conséquent, la possibilité d'exposer des motifs légitimes à l'opposition de l'alimentation du DMP revient, finalement, à concéder l'existence de ce droit aux titulaires d'un DMP. Les dispositions de l'article R.1111-47 du code de la santé publique apparaissent donc contraires aux principes encadrant le droit d'opposition au traitement tels que prévus par le cadre juridique applicable à la protection des données personnelles. De surcroît, cette prérogative concédée par le droit national attente à la portée de l'obligation d'alimentation incombant aux professionnels de santé, pourtant renforcée par la loi ASAP⁴³¹. Compte tenu de la primauté du droit communautaire sur le droit national⁴³², le titulaire du DMP ne devrait pouvoir s'opposer à son remplissage, nonobstant la justification de motifs légitimes résultant de sa situation particulière. Si la personne concernée ne souhaite pas voir ses données médicales apparaître dans son carnet numérique de santé, elle dispose néanmoins de la faculté de les masquer⁴³³.

125. Par ailleurs, les non-professionnels de santé ainsi que le médecin du travail ne sont pas concernés par cette obligation générale d'alimentation du DMP. En effet, ces derniers ne peuvent le renseigner qu'avec le consentement de son titulaire⁴³⁴. Toutefois, lorsque la personne concernée leur a expressément donné accès à ce dossier numérique aux fins de l'alimenter, ce remplissage ne constituerait-il pas une obligation pour ces derniers ? Qu'il s'agisse d'un devoir ou d'une possibilité, il n'en demeure pas moins que l'alimentation du DMP consenti par son titulaire constitue une mission légale impliquant un traitement de données sensibles. Ils en seraient donc les responsables au même titre que les professionnels de santé obligés de le remplir⁴³⁵. En revanche, ce traitement de données sensibles effectué par les non-professionnels de santé et le médecin du travail n'est pas fondé sur une obligation légale mais sur le consentement de la personne concernée. Il en résulte que le patient bénéficiaire d'un DMP conserve la maîtrise du remplissage non obligatoire de ses données médico-sociales, sociales et des éléments de son dossier médical en santé au travail.

⁴³¹ Article 98 de la loi n°2020-1525 du 7 décembre 2020, *op. cit.*

⁴³² CJCE, 15 juillet 1964, aff. 6/64, *Flaminio Costa contre E.N.E.L*, Rec. Lebon, p. 1141.

⁴³³ Cf. Paragraphe 293.

⁴³⁴ Article L.1111-17 III et IV du code de la santé publique.

⁴³⁵ CEPD, *Lignes directrices 07/2020 sur les concepts de responsable du traitement et de sous-traitant dans le RGPD*, *loc. cit.*

L'autodétermination informationnelle du titulaire du DMP n'est donc limitée qu'en ce qui concerne le traitement de ses données médicales générées dans le cadre exclusif de sa prise en charge médicale. Il en advient que la coordination et la continuité de ses soins semblent prévaloir sur la maîtrise de ses informations intimes. Néanmoins, il bénéficie tout de même de certains droits sur les données médicales versées dans son carnet de santé numérique.

Section 2 : La réduction des droits du patient à la modification de ses dossiers médicaux

126. Conformément au RGPD, le patient jouit de droits sur ses données personnelles formalisées au sein de ses dossiers médicaux. A cet égard, le patient dispose du droit de faire modifier ses données consignées dans son dossier médical hospitalier ou dans sa fiche d'observation personnelle (**Paragraphe 1**). De la même manière, le patient, en sa qualité de personne concernée, peut obtenir la modification de ses données personnelles reportées dans son DMP (**Paragraphe 2**).

Paragraphe 1 : La modification des dossiers de soins

127. En vertu des droits conférés par le RGPD, la modification du dossier de soins peut intervenir de deux manières : par la rectification des données qui le composent (**A**), ou par leur effacement (**B**).

A) La rectification des données colligées dans les dossiers de soins

128. Le droit à la rectification des données personnelles contenues dans les dossiers de soins s'applique tant aux données administratives (**2**) qu'aux données médicales du patient (**3**). Si l'exercice de ce droit s'exerce en considération des conditions prescrites par le RGPD (**1**), l'effectivité du droit de rectification dépend de la nature de la donnée concernée. En effet, la rectification des données administratives ne doit porter atteinte à l'identitovigilance. Identiquement, la rectification des données médicales ne doit attenter à leur intégrité, ni contrarier la réalité qu'elles retranscrivent.

1. Les conditions d'exercice du droit de rectification

129. Toute personne concernée par un traitement de données à caractère personnel jouit du droit de les faire rectifier auprès du responsable de traitement. L'article 50 de la loi Informatique et Libertés modifiée dispose très simplement que « *le droit de rectification s'exerce dans les conditions prévues à l'article 16* » du RGPD. Seulement, le législateur européen s'attache davantage à définir le droit de rectification qu'à encadrer ses conditions d'exercice. En vertu de cet article, la personne concernée a le droit d'obtenir du responsable de traitement la rectification de ses données inexactes ou incomplètes. En d'autres termes, le droit de rectification des données peut s'entendre comme un droit de correction des erreurs et des lacunes dont les données sont affectées. Par le biais du droit d'accès à ses informations personnelles⁴³⁶, la personne concernée peut s'assurer que ses données sont exactes et, à défaut, les corriger. Egalement, elle peut vérifier que ses données sont tenues à jour et, au besoin, les actualiser. La personne concernée dispose donc de la possibilité de contrôler et de maîtriser les informations qui la concernent. Par conséquent, le droit de rectification participe à l'autodétermination informationnelle des individus. Toutefois, cette prérogative de contrôle offerte à la personne concernée ne devrait-elle pas s'inscrire comme un devoir ?

130. Au regard du principe réglementaire d'exactitude des données traitées, « *les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour* »⁴³⁷. Ce principe est traduit par l'obligation, à la charge du responsable de traitement, de prendre sans tarder toutes les mesures raisonnables pour que les données inexactes ou incomplètes soient rectifiées⁴³⁸. Seulement, les données personnelles collectées à un moment déterminé peuvent évoluer au regard de la situation de la personne concernée. S'il appartient au responsable de traitement de s'assurer de l'exactitude des données au moment de leur collecte, ce dernier ne peut présumer tout changement de situation relatif à une personne concernée. En conséquence, la notion d'exactitude se révèle temporelle et variable. Ainsi, des données personnelles exactes peuvent, dans le temps, devenir inexactes. En outre, les données collectées peuvent s'avérer incomplètes. Cette insuffisance peut évidemment provenir du responsable de traitement, mais également de la personne concernée qui aurait omis,

⁴³⁶ Cf. Paragraphe 189.

⁴³⁷ Article 5.1 d) du RGPD.

⁴³⁸ *Ibid.*

activement ou passivement, de renseigner certaines informations. Dès lors, comment le responsable de traitement pourrait veiller à la collecte d'une donnée dont il ignore l'existence ou qui lui serait cachée ?

Il peut sembler difficile, pour le responsable de traitement, de procéder à des modifications ou à des actualisations ultérieures à la collecte des données personnelles sans l'intervention préalable de la personne concernée. L'obligation d'exactitude du responsable de traitement constitue donc le corollaire du droit de rectification de la personne concernée. Ainsi, l'obligation d'exactitude pesant sur le responsable de traitement devrait être considérée comme une obligation de moyens jusqu'à ce que la personne concernée ait, par le biais du droit de rectification, porté à sa connaissance les données à corriger. Le cas échéant, cette injonction évoluerait vers une obligation de résultat. Par suite, le responsable de traitement devrait relayer la modification intervenue à l'ensemble des destinataires auxquels les données personnelles de la personne concernée ont été communiquées⁴³⁹, ceci afin de lui éviter toute conséquence dommageable. Compte tenu de ce qui précède, le droit de rectification reconnu à la personne concernée devrait être considéré comme un devoir de déclarer toute modification de données personnelles en vue de leur rectification. Pour envisager le droit de rectification comme un devoir, la personne concernée devrait être expressément informée de la portée et des enjeux liés à la rectification et à l'actualisation de ses données personnelles, ainsi que des modalités d'exercice de ce droit. A l'instar de l'information relative au droit d'opposition, l'information relative au droit de rectification devrait être présentée clairement et séparément de toute autre information relative au traitement des données personnelles. Compte tenu de ce qui précède, le responsable de traitement ne pourrait être tenu pour responsable d'un préjudice consécutif à l'absence de correction d'une donnée qui ne pouvait intervenir que sous l'impulsion de la personne concernée.

131. Lorsque la personne concernée exerce son droit de rectification, le responsable de traitement doit, dans les meilleurs délais, informer la personne concernée des mesures prises consécutivement à sa demande. Selon le principe d'exactitude, les données inexacts doivent être rectifiées sans tarder. C'est pourquoi toutes mesures raisonnables doivent être prises dans

⁴³⁹ Article 19 du RGPD.

un délai d'un mois à compter de la réception de la demande de la personne concernée⁴⁴⁰. Néanmoins, ce délai peut être prorogé de deux mois compte tenu de la complexité de la demande ou du nombre de demandes adressées au responsable de traitement⁴⁴¹. Le cas échéant, le responsable du traitement doit informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande⁴⁴². En tout état de cause, toute erreur doit être indispensablement rectifiée dans un délai maximal de trois mois à compter de la demande de rectification. Compte tenu de ce qui précède, le principe d'exactitude semble constituer une obligation à la charge du responsable de traitement qu'à partir du moment où cette inexactitude est soulevée et corrigée par la personne concernée. Toutefois, cette inexactitude ne doit pas être imputable au responsable de traitement. Evidemment, celui-ci doit s'assurer de l'exactitude des données à l'instant où il procède à leur collecte.

132. Si le responsable de traitement a l'obligation de rectifier les données inexactes ou incomplètes portées à sa connaissance ultérieurement à leur collecte, encore faut-il que l'inexactitude soit certaine et avérée ou que la déclaration complétant les données soit justifiée au regard de la finalité du traitement. C'est ainsi que le Conseil d'Etat a jugé qu'une demande visant à la modification du fichier à partir duquel sont édités les bulletins de paye, pour y ajouter une mention relative à l'exercice de la profession de la personne concernée, n'est pas fondée dans la mesure où cette déclaration complémentaire n'a aucune incidence sur le montant du salaire⁴⁴³. Le responsable de traitement n'est pas forcé de donner suite aux demandes infondées ou excessives. En effet, le responsable de traitement doit analyser le bienfondé de la demande de rectification eu égard aux données concernées et à la finalité du traitement. En cas de refus, le responsable de traitement doit, sans tarder, informer la personne concernée de ces motifs⁴⁴⁴. La personne concernée est également avertie de la possibilité d'introduire une réclamation auprès de la CNIL et de former un recours juridictionnel⁴⁴⁵.

⁴⁴⁰ Article 12.3 du RGPD.

⁴⁴¹ *Ibid.*

⁴⁴² *Ibid.*

⁴⁴³ CE, 17 avril 1992, n°115688 et n°116291.

⁴⁴⁴ Article 12.4 du RGPD.

⁴⁴⁵ Article 12.4 du RGPD.

2. La rectification des données administratives contenues dans les dossiers de soins

133. L'étude des dispositions de droit commun encadrant l'exercice du droit de rectification relève d'une importance particulière. Contrairement au droit d'opposition étudié précédemment⁴⁴⁶, le droit de rectification ne connaît pas de spécificité en considération de la base légale justifiant le traitement des données personnelles. Aussi, l'exercice du droit de rectification ne tient pas compte de la nature des données traitées. Les dispositions relatives à la rectification des données personnelles s'appliquent donc aux données administratives et médicales du patient lorsqu'elles sont traitées dans le cadre de sa prise en charge sanitaire et colligées dans ses dossiers de soins. Alors qu'aucune norme juridique ne précise les modalités d'exercice du droit de rectification du dossier de soins, il est indispensable d'adapter les règles de droit commun édictées par le RGPD aux particularités des données y étant formalisées. Cette adaptation ne peut s'effectuer qu'au cas par cas. En conséquence, il revient aux responsables de traitement d'étudier chaque demande de rectification des données intégrées dans le dossier de soins du patient en considération des informations qu'elles renferment.

134. Si le dossier de soins du patient contient principalement des données médicales, il comporte également des données administratives nécessaires à la sécurité des soins⁴⁴⁷. Comme il l'a été démontré, « *l'identification du patient est un élément clé de la prise en charge* »⁴⁴⁸. Cependant, « *les systèmes d'identifications au sein des établissements de santé reposent sur des collectes hétérogènes de traits d'identification, en particulier en ce qui concerne le nom du patient, qui peut être son nom de naissance, son nom marital ou son nom d'usage. [...] Or si le nom de naissance, et la date de naissance sont réellement invariants, le nom usuel du patient, peut changer (mariage, divorce, etc.) favorisant la création de doublons d'identité (un même patient est identifié plusieurs fois, sous son nom de naissance,*

⁴⁴⁶ Cf. Paragraphes 116 s.

⁴⁴⁷ Cf. Paragraphe 60.

⁴⁴⁸ DGOS, Instruction n°2013-281 du 7 juin 2013 relative à l'utilisation du nom de famille (ou nom de naissance) pour l'identification des patients dans les systèmes d'information des structures de soins, Visa CNP 2013-131.

puis d'usage, ou marital), ce qui entraîne des risques d'erreurs accrues. »⁴⁴⁹. De surcroît, les informations relatives à l'identité ne sont pas la seule catégorie de données administratives pouvant faire l'objet d'une modification. Certainement, les informations relatives aux coordonnées du patient peuvent régulièrement changer ; c'est pourquoi elles devraient corrélativement être tenues à jour.

135. En conséquence, la rectification des données administratives devrait davantage consister en un devoir pour le patient plus que d'un droit. Par suite, le patient devrait veiller à signaler toute erreur et tout changement intervenant sur ses données (nom, prénom, adresse, numéro de téléphone, etc.) à l'établissement ou au professionnel de santé qui le prend en charge. En ce sens, l'ARS Nouvelle-Aquitaine affirme qu' « *en cas de désaccord avec les traits d'identité enregistrés par une structure de santé, il appartient à l'utilisateur d'exercer son droit d'accès et de rectification auprès de la structure, sous réserve de respecter les règles applicables en matière d'identitovigilance* »⁴⁵⁰. Cette exactitude est absolument indispensable en ce qu'elle participe à la sécurité des prises en charge médicales. En effet, l'identitovigilance est un enjeu majeur pour la continuité et la sécurité des soins « *compte tenu du risque d'erreurs potentiellement graves liées à une mauvaise identification (erreur de site opératoire, erreur de traitement, erreur transfusionnelle, erreurs de résultats de laboratoire, etc.). Un système de surveillance, de correction et de prévention des erreurs permet de maîtriser ce risque.* »⁴⁵¹. Outre les actions d'identitovigilance à déployer par les établissements et les professionnels de santé, l'exactitude des informations identifiantes relatives au patient reposerait également sur le patient lui-même. A travers son devoir de rectification des données administratives contenues dans son dossier de soins, le patient deviendrait un acteur de l'identitovigilance et de la sécurité des soins. A l'appui de sa demande, le patient devrait fournir un document certifiant de ses données administratives : son passeport, sa carte nationale d'identité, son titre de séjour ou encore un justificatif de domicile. De cette façon, le responsable de traitement serait le garant de la certification de l'exactitude des données administratives du patient.

⁴⁴⁹ *Ibid.*

⁴⁵⁰ ARS Nouvelle Aquitaine, *L'identitovigilance au cœur de la sécurité des soins*, article diffusé en ligne le 27 juin 2019. Disponible en ligne sur le site [www.nouvelle-aquitaine.ars.sante.fr]. Consulté le 04 mars 2020.

⁴⁵¹ HAS, *Identification du patient à toutes les étapes de sa prise en charge*, 26 juin 2017. Disponible en ligne sur le site [www.has-sante.fr]. Consulté le 04 mars 2020.

136. Cependant, l’accomplissement d’un tel devoir de rectification pourrait rapidement devenir une tâche administrative complexe à mettre en œuvre. Pour un patient, il existe autant de dossiers de soins que d’établissements et de professionnels de santé qu’il a consultés. En d’autres termes, il existe une pluralité de dossiers de soins pouvant être rattachés à un même patient. L’accomplissement d’un devoir de rectification supposerait, pour le patient, d’en examiner les modalités d’exercice déterminées par chaque établissement ou professionnel de santé ayant participé à sa prise en charge sanitaire. Il en advient que l’affermissement du rôle central du DMP⁴⁵² faciliterait l’exercice de ce devoir et favoriserait la sécurité de la dispensation des services de soins de santé.

3. La rectification des données médicales contenues dans les dossiers de soins

137. Alors que la rectification des données identifiantes contenues dans le dossier de soins pourrait être conçue comme un devoir pour le patient, la rectification des données médicales ne constitue pas un droit acquis. Certes, aucune disposition légale ou réglementaire n’interdit la rectification des données médicales colligées dans le dossier de soins du patient. Seulement, leur rectification pourrait attenter à leur intégrité ou mettre en péril la traçabilité des actes médicaux et paramédicaux, et ainsi impacter la continuité des soins. Malgré ces inconvénients, il apparaît toutefois essentiel que le patient puisse faire corriger toute erreur ou omission liée à l’alimentation de son dossier de soins et pouvant affecter la sécurité et la qualité de sa prise en charge sanitaire.

Le dossier de soins a pour principale fonction la traçabilité de toute action effectuée au cours de la prise en charge du patient et de toute information médicale et paramédicale recueillie et produite à cette occasion. Ces données, formalisées et intégrées dans le dossier de soins, doivent être datées et comporter l’identité du professionnel de santé qui en est à l’origine⁴⁵³. Le dossier de soins permet donc de retracer et de comprendre la chronologie et le déroulement du parcours de soins du patient. A ce titre, l’absence de rectification du dossier de soins est essentielle pour deux raisons. D’une part, le dossier de soins permet de retracer, jour par jour et heure par heure, toute intervention et toute décision médicale ou paramédicale

⁴⁵² Cf. Paragraphes 91 à 96.

⁴⁵³ Article R.1112-3 du code de la santé publique.

concernant le patient. Le dossier de soins constitue donc un élément de preuve capital dans la mise en jeu de la responsabilité médicale⁴⁵⁴. D'autre part, une erreur ou une omission dans l'alimentation du dossier de soins pourrait expliquer des décisions préjudiciables prises sur la base d'une donnée inexacte ou incomplète. La conservation de ces éléments erronés semble alors fondamentale en matière de responsabilité médicale. Seulement, la rectification d'une donnée incomplète ou inexacte permettrait d'éviter toute décision ultérieure préjudiciable. Il convient alors de balancer les bénéfices et les risques de la modification du dossier de soins. Chaque demande de rectification des données médicales requiert donc d'être vigoureusement examinée.

138. Eu égard à la complexité de l'étude des demandes de rectification des données médicales, il serait opportun de définir des critères sur lesquels les responsables de traitement pourraient évaluer ces demandes. En effet, le RGPD ne précisant pas les éléments sur lesquels le responsable de traitement pourrait motiver son inaction, il convient de guider les établissements et les professionnels de santé dans la réponse à apporter aux demandes de modification des dossiers de soins.

139. Le premier critère que nous retiendrons a trait à la factualité de la donnée. La demande de rectification doit concerner une erreur ou une omission factuelle avérée et dont la preuve apportée par le patient est indiscutable. Par exemple, le patient pourrait faire rectifier une erreur liée au fait que l'action médicale n'a pas porté sur le bras mais sur la main, ou que le membre soigné n'était pas la jambe gauche mais la jambe droite. Egalement, le patient pourrait demander la rectification des données recueillies lors de l'interrogatoire médical⁴⁵⁵ telles que des antécédents médicaux erronés ou des allergies non renseignées. S'il est indiqué que le patient a enduré une amygdalectomie alors qu'il n'a subi qu'une ablation des végétations, il est indispensable que cette erreur soit rectifiée.

140. Le deuxième critère que nous retiendrons concerne l'intégrité des informations médicales. La demande de rectification des données médicales ne doit pas avoir pour effet de porter atteinte à leur intégrité, *a fortiori* lorsqu'elles ont été produites ou validées par les professionnels de santé. En effet, les professionnels de santé doivent rester libres et

⁴⁵⁴ Cf. Paragraphes 68 et 69.

⁴⁵⁵ Cf. Paragraphe 50.

indépendants dans l'exercice de leur art. Alors, « *quand peut-il être considéré, dans l'exercice de l'art de guérir, qu'une donnée relative à la santé est inexacte ?* »⁴⁵⁶. La médecine n'étant pas une science exacte, l'interprétation des données cliniques peut différer selon le professionnel de santé et les moyens techniques utilisés. Par conséquent, que le patient soit profane ou professionnel de santé, il ne peut rectifier les données cliniques dont il réfuterait l'interprétation. Il est primordial que les données médicales demeurent intègres et intactes pour le suivi et la coordination de la prise en charge sanitaire du patient.

141. Le troisième et dernier critère que nous retiendrons porte sur la prise d'une décision résultant d'une donnée de santé erronée. Dans l'hypothèse où une décision sanitaire préjudiciable pour le patient a été fondée sur une donnée médicale incomplète ou erronée, il paraît important que cette causalité ne soit pas totalement rectifiée. En effet, en cas de recours amiable ou contentieux à l'encontre d'un établissement ou d'un professionnel de santé, le médecin expert et le juge devront analyser l'ensemble des liens de causalité intervenus dans la réalisation du dommage. Dans ce cas, la rectification du dossier de soins pourrait être considérée comme une falsification de preuve par le patient allant, de surcroît, à l'encontre de ses intérêts. Cependant, afin d'éviter qu'une donnée médicale incomplète ou erronée puisse à nouveau conduire à des décisions médicales ou paramédicales préjudiciables pour le patient, il semble inévitable de la rectifier pour l'avenir. A l'instar des erreurs matérielles des actes de l'état civil⁴⁵⁷, la rectification de la donnée médicale pourrait intervenir par une mention rectificative horodatée et apposée en marge du dossier de soins après avoir pris le soin de barrer l'information inexacte.

142. Compte tenu de ces trois critères, la demande de rectification exercée par le patient ne pourrait être accordée qu'à la condition qu'elle porte sur une erreur purement factuelle ne pouvant faire l'objet d'une interprétation. Dès lors, l'établissement ou le professionnel de santé, en tant que responsable de traitement, aurait l'obligation de procéder à la modification du dossier de soins du patient. En pratique, la rectification devrait être effectuée par le professionnel de santé identifié comme ayant recueilli ou produit la donnée médicale, ou à défaut, par le médecin chef du service dans lequel exerce le professionnel de santé à l'origine de l'erreur ou de l'omission.

⁴⁵⁶ HERVEG (J.), VERHAEGEN (M.-N.), POULLET (Y.), *op. cit.*, p. 78.

⁴⁵⁷ Article 99-1 du code civil.

Par ailleurs, la modification du dossier médical hospitalier et de la fiche d'observation personnelle peut intervenir par l'effacement des données qu'ils contiennent. Alors que l'exercice du droit de rectification du dossier de soins semble périlleux en raison de son absence d'encadrement, le législateur européen a pris le soin de préciser les conditions d'exercice du droit à l'effacement des données traitées.

B) L'effacement des données colligées dans les dossiers de soins

143. En vertu de l'article 51 de la loi Informatique et Libertés modifiée, les personnes concernées par le traitement de leurs données personnelles peuvent en demander l'effacement dans les conditions de l'article 17 du RGPD. Le législateur européen a intitulé le droit à l'effacement comme le « *droit à l'oubli* »⁴⁵⁸. Le droit à l'effacement des données semble alors conçu comme le droit, pour la personne concernée, de se faire oublier. L'analogie entre les notions d'effacement et d'oubli est issue d'une jurisprudence de la Cour de justice de l'Union européenne (CJUE) relative au déréférencement. En effet, la CJUE a consacré le droit, pour une personne physique, d'obtenir la suppression des résultats la concernant suite à une recherche effectuée sur la base de ses noms et prénoms sur un moteur de recherche internet⁴⁵⁹. Toutefois, au regard du champ d'application territorial du RGPD, ce déréférencement ne peut intervenir qu'à l'échelle européenne et ainsi ne concerner que les versions européennes du moteur de recherche⁴⁶⁰. De surcroît, le droit au déréférencement des données personnelles, mêmes sensibles, doit être mis en balance avec les droits fondamentaux dus à toute personne physique. Partant, il est admis que les données personnelles d'une personne physique soient traitées par l'exploitant d'un moteur de recherche internet dès lors qu'elles apparaissent « *strictement nécessaires pour protéger la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page internet au moyen d'une telle*

⁴⁵⁸ Intitulé de l'article 17 du RGPD.

⁴⁵⁹ CJUE, Gr. Ch., 13 mai 2014, aff. C-131/12, *Google Spain* : AJDA, 2014, n° 20, p. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D., 2014, n° 25, p. 1476, note V.-L. Benabou et J. Rochfeld et p. 1481, note N. Martial-Braz et J. Rochfeld ; D., 2014, n° 40, p. 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; AJCT, 2014, n° 10, p. 502, obs. O. Tambou ; JCP E, 2014, 1326, note M. Griguer et 1327, note G. Busseuil ; CCE, 2014, étude 13, A. Debet ; RLDI, 2014, n° 106, 3535 note C. Castets-Renard, 3536, note D. Forest et 3537, note A. Casanova.

⁴⁶⁰ CJUE, 24 septembre 2019, aff. C-507-17 : Gaz. Pal., 2020, n° 06, p. 31, P. Piot ; D., 2019, n° 36, p. 2022, note J.-L. Sauron ; D., 2020, n° 09, p. 515, note T. Douville ; Légipresse, 2019, n° 377, p. 687, note N. Mallet-Poujol.

recherche »⁴⁶¹. La personne concernée peut ainsi demander à se faire oublier d'un moteur de recherche internet sans pour autant obtenir la suppression de ses informations personnelles contenues au sein de pages web. Le droit à l'effacement ne constitue donc pas un droit absolu et ne permet pas systématiquement de se faire oublier du responsable de traitement. Les limites du droit à l'effacement des données personnelles ont été affirmées par le RGPD.

144. Sous l'empire de la directive 95/46 du 24 octobre 1995⁴⁶², l'exercice du droit à l'effacement était conditionné par l'allégation de motifs légitimes par la personne concernée. C'est ainsi que la CNIL a autorisé l'effacement de données médicales contenues dans le dossier de soins d'un patient hospitalisé « *au motif qu'un membre de sa famille travaillait dans cet établissement et qu'il ne souhaitait pas que sa famille soit informée des traitements qu'il suivait* »⁴⁶³. Le droit à l'effacement pouvait s'exercer à condition de justifier d'un *motif légitime* en appui de la demande. Depuis l'entrée en vigueur du RGPD, cette notion abstraite et subjective a laissé place à une liste exhaustive de motifs objectifs donnant droit, pour la personne concernée, à l'effacement de ses données personnelles. En vertu du deuxième paragraphe de l'article 17 du RGPD, le droit à l'effacement des données personnelles est devenue une obligation à la charge du responsable de traitement, notamment lorsqu'elles n'apparaissent « *plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées* »⁴⁶⁴, ou qu'elles « *ont fait l'objet d'un traitement illicite* »⁴⁶⁵. Alors que le droit à l'effacement est dû à la personne placée dans une telle situation, le législateur européen a également pris le soin d'arrêter des contextes dans lesquels il ne trouvait à s'appliquer. En effet, le droit à l'effacement est notamment inopérant lorsque le traitement des données personnelles est nécessaire « *pour respecter une obligation légale qui requiert le traitement [...], à des fins archivistiques dans l'intérêt public, à des fins de recherche*

⁴⁶¹ CJUE, 24 septembre 2019, aff. C-136/17 : Gaz. Pal., 2020, n° 06, p. 28, P. Piot ; JCP E, 2019, n° 40, act. 633 ; CCE, 2020, n° 02, étude 3, G. Desgens-Pasanau ; CE, 6 décembre 2019, n°405464, Rec. Lebon T. ; Revue Communication Commerce électronique, 2020, n° 02, comm. 17, N. Metallinos.

⁴⁶² 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, JOUE L 281, 23 novembre 1995, p. 31-50.

⁴⁶³ CNIL, *Dossier médical : puis-je demander à effacer des données après une hospitalisation ?*, Question – Réponse. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 05 mars 2020.

⁴⁶⁴ Article 17.1 a) du RGPD.

⁴⁶⁵ Article 17.1 d) du RGPD.

scientifique ou historique ou à des fins statistiques [...], ou à la constatation, à l'exercice ou à la défense de droits en justice »⁴⁶⁶.

La question se pose alors de savoir si les patients disposent du droit d'effacer leurs données personnelles – obligatoirement – formalisées au sein de leurs dossiers de soins⁴⁶⁷. Bien que l'obligation de constitution et d'alimentation des dossiers de soins s'oppose *a priori* au droit à l'effacement des données qu'ils contiennent, le patient devrait pouvoir demander la suppression de ses données personnelles lorsqu'elles sont plus nécessaires à sa prise en charge sanitaire (2) et, en particulier, lorsqu'elles ont été collectées en violation du principe de minimisation des données (1).

1. L'obligation d'effacement des données non minimisées

145. Bien qu'en principe le droit à l'effacement des données personnelles ne peut s'appliquer aux traitements fondés sur le respect d'une obligation légale, le RGPD admet que la personne concernée puisse obtenir l'effacement de ses données personnelles dès lors qu'elles ont fait l'objet d'un traitement illicite. Assurément, le respect d'une obligation légale ne peut être exécuté illégalement. A défaut, cette obligation serait réputée inexécutée par son débiteur qui, de surcroît, commettrait une infraction aux dispositions juridiques violées. Par conséquent, cette limitation au droit à l'effacement posée par le RGPD ne peut être applicable lorsque le motif de la demande de suppression repose sur l'illicéité du traitement. Autrement dit, dans la mesure où les données personnelles contenues dans le dossier de soins du patient ont fait l'objet d'un traitement illicite, le patient est en droit d'en demander l'effacement, et le responsable de traitement est dans l'obligation de les effacer dans les meilleurs délais.

146. Les conditions de licéité d'un traitement de données personnelles sont édictées au deuxième chapitre du RGPD. Plus précisément, l'article 5 du RGPD énonce les six conditions de licéité auxquelles tout traitement de données personnelles doit répondre pour être légalement entrepris⁴⁶⁸. Par conséquent, tout traitement réalisé en méconnaissance des dispositions de l'article 5 du RGPD est *de facto* illicite. Parmi les conditions de licéité listées

⁴⁶⁶ Article 17.3 du RGPD.

⁴⁶⁷ Cf. Paragraphes 105 et 109.

⁴⁶⁸ Cf. Paragraphe 20.

à l'article susvisé, il est impératif que les données soient « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* »⁴⁶⁹. En vertu de ce principe essentiel de la protection des données personnelles, les données personnelles du patient consignées dans son dossier de soins doivent être minimisées à ce qui est nécessaire au regard de la prise en charge sanitaire du patient⁴⁷⁰. Si les professionnels et les établissements de santé ont l'obligation de constituer un dossier de soins pour tout patient pris en charge, seules les données personnelles adéquates et pertinentes à cette fin peuvent y être insérées. En vertu du principe de minimisation des données traitées, le patient est alors dûment fondé à demander l'effacement, de son dossier de soins, des données n'ayant aucune pertinence pour l'accomplissement de cette exigence réglementaire.

147. Toutefois, il peut exister une divergence entre ce que le professionnel de santé et le patient considèrent comme pertinent dans le cadre d'une prise en charge sanitaire. Alors que le patient pourrait estimer qu'une information personnelle est superflue, sous un prisme médical, cette même information pourrait revêtir d'une importance primordiale. A titre d'exemple, la collecte de données de nature sensibles liées à l'origine raciale peut s'avérer essentielle en matière de prévention, de suivi ou de soins médicaux. Effectivement, il est scientifiquement fondé que certaines ethnies sont considérées comme plus susceptibles de contracter certaines pathologies. En ce sens, l'Institut de cardiologie de l'Université d'Ottawa explique que « *la race ou le groupe ethnique auquel vous appartenez peut avoir une constitution génétique et environnementale qui prédispose ses membres aux maladies cardiovasculaires. Les personnes de même ethnie ont plusieurs gènes en commun, ce qui explique pourquoi les antécédents familiaux et l'origine ethnique sont si étroitement liés.* »⁴⁷¹. La connaissance d'une telle information est fondamentale pour l'anticipation et la prévention des prédispositions génétiques. La demande d'effacement d'une information relative aux origines raciales, pouvant paraître incongrue au sein du dossier de soins, pourrait *in fine* constituer une perte de chance dans la prise en charge médicale du patient. L'analyse de l'adéquation des données personnelles intégrées dans le dossier de soins du patient à des fins de prise en charge sanitaire requiert donc une interprétation médicale.

⁴⁶⁹ Article 5.1 c) du RGPD.

⁴⁷⁰ Cf. Paragraphe 43.

⁴⁷¹ Institut de cardiologie de l'Université d'Ottawa, *Prévention et mieux-être*. Disponible en ligne sur le site [<https://pwc.ottawaheart.ca/fr>]. Consulté le 18 mars 2020.

148. La demande d’effacement d’une donnée personnelle consignée dans le dossier de soins doit donc être adressée au responsable de traitement et étudiée par le professionnel de santé ayant renseigné la donnée litigieuse. Autrement dit, l’appréciation du bienfondé de la demande d’effacement doit être examinée et justifiée par le professionnel de santé l’ayant documentée. Toutefois, n’existerait-il pas un conflit d’intérêt pour le professionnel de santé ? En effet, celui qui a renseigné une donnée personnelle impertinente dans le dossier de soins du patient sera tenté de soutenir l’adéquation de l’information consignée avec la prise en charge sanitaire. Dans ce cas, le responsable de traitement pourrait, en toute légalité, refuser de faire droit à la demande d’effacement formulée par le patient à condition de l’informer des motifs de son inaction et des possibilités d’introduire une réclamation auprès de la CNIL et de former un recours juridictionnel⁴⁷². Dans cette hypothèse, il paraît opportun qu’un tiers puisse examiner la licéité des données intégrées dans le dossier de soins en toute impartialité. L’appréciation de la licéité étant soumise à interprétation, l’allégation du motif selon lequel les données à caractère personnel ont fait l’objet d’un traitement illicite ne suffit donc pas à faire droit à la demande du patient. Cependant, dès lors que l’illicéité des données est avérée, le responsable de traitement est obligé de les effacer du dossier de soins.

149. Par ailleurs, parmi les six conditions de licéité prévues à l’article 5 du RGPD, le législateur européen annonce que la conservation des données doit être limitée. En conséquence, le patient est en droit de demander l’effacement de ses données personnelles périmées. Corrélativement, le responsable de traitement est tenu d’effacer les données qui ne se trouvent plus nécessaires à la finalité du traitement⁴⁷³.

2. L’obligation d’effacement des données périmées

150. La personne concernée a le droit d’obtenir l’effacement de ses données personnelles traitées en contradiction des principes de licéité édictés à l’article 5 du RGPD. Au nombre de ces principes, les données personnelles doivent être « *conservées [...] pendant une durée n’excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* »⁴⁷⁴.

⁴⁷² Considérant 124 du RGPD.

⁴⁷³ Article 17.1 a) du RGPD.

⁴⁷⁴ Article 5.1 e) du RGPD.

Si les établissements et les professionnels de santé ont l'obligation de formaliser les données personnelles des patients dans un dossier de soins, ils sont également tenus à leur conservation en leur sein, ou auprès d'un hébergeur de données de santé⁴⁷⁵. Néanmoins, la conservation des dossiers de soins doit être assortie d'une durée à l'issue de laquelle ils pourront être supprimés. Dès lors, il convient de déterminer les délais de conservation du dossier médical hospitalier et de la fiche d'observation personnelle.

151. Les délais de conservation des dossiers médicaux hospitaliers, constitués par les établissements de santé, sont encadrés par les dispositions réglementaires de l'article R.1112-7 du code de la santé publique. Le dossier médical hospitalier doit être conservé pendant une durée de vingt ans à compter de la date de la dernière hospitalisation ou consultation externe du patient au sein de l'établissement de santé. Il existe toutefois deux tempéraments. D'abord, si « *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* »⁴⁷⁶. Ensuite, « *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* »⁴⁷⁷. En outre, il s'agit de préciser que « *ces délais sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité médicale de l'établissement de santé ou de professionnels de santé à raison de leurs interventions au sein de l'établissement* »⁴⁷⁸.

152. Alors que les durées de conservation des dossiers médicaux hospitaliers sont précisément déterminées par les pouvoirs publics, aucun texte juridique ne limite le délai de conservation des fiches d'observation personnelles élaborées par les médecins exerçant en médecine de ville. En l'absence de précisions juridiques et déontologiques, le CNOM a émis des recommandations relatives au délai de conservation à appliquer. Dans un premier temps, la durée de conservation préconisée était calquée sur le délai de prescription de l'action en responsabilité civile professionnelle. Seulement, depuis l'entrée en vigueur de l'article L.1142-28 du code de la santé publique, le délai de prescription de l'action en responsabilité

⁴⁷⁵ Article L.1111-8 du code de la santé publique.

⁴⁷⁶ Article R.1112-7 du code de la santé publique.

⁴⁷⁷ *Ibid.*

⁴⁷⁸ *Ibid.*

médicale applicable à la médecine privée a été réduit de trente ans à dix ans à compter de la consolidation d'un dommage subi à l'occasion d'actes de prévention, de diagnostic ou de soins. Dans l'hypothèse où la consolidation du dommage interviendrait plus de dix ans après les derniers soins prodigués, la responsabilité des professionnels de santé pourrait être engagée postérieurement à la limite de conservation des fiches d'observation personnelles. Seulement, le dossier de soins constitue un élément de preuve crucial en matière de recours gracieux ou contentieux⁴⁷⁹. Il apparaît donc inapproprié de transposer le délai de prescription de l'action en responsabilité médicale à la durée de conservation des fiches d'observation personnelles étant donné que les points de départ de ces deux délais peuvent être espacés de plus de dix années. Dorénavant, le CNOM conseille « *aux médecins de s'aligner sur le délai minimal de vingt ans appliqué par les établissements de santé de façon à préserver la justification essentiellement médicale de cette durée, à conserver les preuves nécessaires à toute défense utile du médecin comme du patient, enfin, à garantir le droit d'accès des patients aux informations de santé les concernant très largement ouvert par la loi précitée du 4 mars 2002* »⁴⁸⁰.

153. Afin qu'il n'y ait plus de rupture d'égalité entre les patients pris en charge en médecine hospitalière ou de ville, et en secteur public ou privé, il est fondamental que les durées de conservation des dossiers de soins soit unifiées. L'harmonisation des durées de conservation des dossiers de soins est notamment essentielle en matière du droit, pour le patient, d'accéder à ses informations médicales. En effet, tout patient devrait bénéficier de ce droit pendant une durée équivalente quelles que soient les modalités de sa prise en charge médicale. Compte tenu de ce qui précède, nous affirmons que les fiches d'observation personnelles doivent être conservées pendant une durée de vingt ans à compter de la dernière consultation du patient auprès du médecin de ville. Dans l'hypothèse où la durée de conservation s'achève avant le vingt-huitième anniversaire du patient, la conservation de la fiche d'observation personnelle doit être reportée jusqu'à cette date. De même, lorsque le patient décède moins de dix ans après sa dernière consultation, sa fiche d'observation personnelle doit être conservée pendant dix années à compter de la date de son décès. Il convient de préciser que ces durées de conservation des dossiers de soins constituent des

⁴⁷⁹ Cf. Paragraphes 68 et 69.

⁴⁸⁰ Commentaire sous l'article 45 du code de déontologie médicale disponible sur le site internet du CNOM à l'adresse [www.conseil-national.medecin.fr]. Consulté le 20 novembre 2021.

délais minimum en-deçà desquels il n'est pas possible de procéder à leur effacement. Autrement dit, les dossiers de soins peuvent être conservés pour des durées supérieures à celles énumérées. Une instruction ministérielle du 14 août 2007 de la Direction de l'hospitalisation et de l'organisation des soins a donc indiqué qu'il revenait « à chaque établissement d'apprécier au cas par cas si, en raison de l'intérêt qu'elles présentent encore à l'issue de ce délai, tout ou partie des informations médicales relatives à un même patient doivent être conservées plus longtemps ou si elles peuvent être éliminées »⁴⁸¹.

154. Cependant, le RGPD impose au responsable de traitement de communiquer, à la personne concernée, la durée de conservation de ses données à caractère personnel⁴⁸². Lorsqu'une telle communication n'est pas possible, le responsable de traitement doit néanmoins lui indiquer les critères utilisés pour déterminer cette durée⁴⁸³. La durée de conservation des données personnelles formalisées au sein des dossiers de soins n'est pas déterminable mais effectivement déterminée par les dispositions réglementaires susvisées⁴⁸⁴. Il en advient que le patient concerné devrait pouvoir demander l'effacement de son dossier de soin au terme de la durée minimale de conservation sur le fondement de l'article 17 du RGPD. Si le dossier de soins doit être supprimé de l'établissement de santé, de la structure non-hospitalière ou des serveurs de l'hébergeur de données de santé au sein duquel il était conservé, les données médicales qu'il comporte peuvent être sauvegardées par-delà ce fichier en raison de leur intérêt pour la collectivité⁴⁸⁵. Autrement dit, les données médicales du patient peuvent être conservées au-delà du terme de conservation du dossier de soins et, subséquentement, de sa suppression.

155. Nonobstant l'absence de précision des modalités d'élimination des fiches d'observation personnelles des patients pris en charge en médecine de ville, le principe voudrait qu'à l'issue du délai de conservation communiqué à la personne concernée, ses données personnelles soient effacées. En effet, l'article 226-20 du code pénal sanctionne « le

⁴⁸¹ DHOS, Instruction ministérielle n°DHOS/E1/DAF/DPACI/2007/322 du 14 août 2007 relative à la conservation du dossier médical.

⁴⁸² Article 13.2 a) du RGPD.

⁴⁸³ *Ibid.*

⁴⁸⁴ *Cf. supra.*

⁴⁸⁵ *Cf. Paragraphe 156.*

fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement ». Néanmoins, les dispositions de cet article poursuivent que l'infraction de conservation des données au-delà de la durée prévue réglementairement ne s'applique pas lorsque « *cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi* »⁴⁸⁶.

156. Dans un premier temps, les pouvoirs publics ont organisé la possibilité de conserver les données médicales du patient incluses dans son dossier médical hospitalier en dépit de la suppression de leur support original. En effet, l'article R.1112-7 du code de la santé publique dispose que les directeurs des établissements participant aux missions du service public hospitalier doivent soumettre la décision d'élimination du dossier médical hospitalier « *au visa de l'administration des archives qui détermine ceux de ces dossiers dont elle entend assurer la conservation indéfinie pour des raisons d'intérêt scientifique, statistique ou historique* »⁴⁸⁷. Si la conservation des données médicales présentant de tels intérêts constitue une exception au droit à l'effacement des données personnelles, à quel titre l'administration des archives peut-elle s'opposer à la suppression des données médicales produites par le service public hospitalier ?

Selon l'article L.211-4 du code du patrimoine, « *les documents qui procèdent de la gestion d'un service public ou de l'exercice d'une mission de service public par des personnes de droit privé* » sont des archives publiques. Ainsi, les dossiers médicaux hospitaliers constitués par les établissements de santé participant au service public disposent de cette qualité. Toutefois, lorsque les archives publiques comportent des données à caractère personnel, l'article L.212-3 du code du patrimoine rappelle que leur traitement demeure soumis à la législation applicable en matière de protection des données personnelles. Par suite, bien que les dossiers médicaux hospitaliers soient des archives publiques, ces données doivent faire l'objet, à l'expiration de leur durée de conservation, « *d'une sélection pour déterminer les données destinées à être conservées et celles, dépourvues d'utilité administrative ou d'intérêt scientifique, statistique ou historique, destinées à être éliminées* »⁴⁸⁸. En ce sens, la loi Informatique et Libertés modifiée conforte que « *les données*

⁴⁸⁶ Article 226-20 du code pénal.

⁴⁸⁷ Article R.1112-7 alinéa 4 du code de la santé publique.

⁴⁸⁸ Article L.212-3 du code du patrimoine.

*à caractère personnel peuvent être conservées au-delà [de leur durée de conservation déterminée] dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine »*⁴⁸⁹. Concrètement, après avoir été sélectionnées par la personne chargée du contrôle scientifique et technique de l'Etat sur les archives, les données médicales à caractère personnel présentant un intérêt public scientifique ou statistique issues des dossiers médicaux hospitaliers sont versées dans un service public d'archives de façon définitive. A l'inverse, les données médicales personnelles considérées comme inutiles à ces fins peuvent effectivement être éliminées⁴⁹⁰.

157. Si, à l'échelle nationale, cette exception à l'effacement des données médicales ne concernait que les informations publiques, le législateur européen a généralement étendu cette possibilité à toute information à caractère personnel. En effet, l'article 17 du RGPD précise que le droit à l'effacement des données personnelles ne s'applique pas dans la mesure où leur traitement est nécessaire « *pour des motifs d'intérêt public dans le domaine de la santé publique* » ou « *à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* »⁴⁹¹. Au regard de ces dispositions, il faut comprendre que toute donnée médicale nécessaire à des fins de recherche répondant à un motif d'intérêt public peut être conservée au-delà de la durée de conservation du dossier de soins du patient⁴⁹². C'est ainsi que le Système national des données de santé (SNDS), qui était initialement un entrepôt de données médico-administratives et publiques couvrant l'intégralité de la population française⁴⁹³, a été légalement élargi à l'ensemble des données médicales recueillies à l'occasion des actes financés par la solidarité nationale⁴⁹⁴. Il s'ensuit que les données médicales produites par le secteur privé ont vocation à alimenter le SNDS afin d'être mises à disposition pour la recherche et l'innovation dans les domaines de la santé

⁴⁸⁹ Article 4, 5° de la loi Informatique et Libertés modifiée.

⁴⁹⁰ Article R.212-14 du code du patrimoine.

⁴⁹¹ Article 17.3 d) du RGPD.

⁴⁹² Cf. Paragraphe 506.

⁴⁹³ Cf. Paragraphe 483.

⁴⁹⁴ Article L.1641-1 I 6° du code de la santé publique tel que modifié par l'article 41 de la loi n°2019-774 du 24 juillet 2019, *loc. cit.*

et de la prise en charge médico-sociale⁴⁹⁵ à condition que leur réutilisation présente un motif d'intérêt public⁴⁹⁶. Alors que l'ensemble des données médicales intégrées au sein du SNDS ne peuvent y être conservées que pendant une durée déterminée de vingt ans⁴⁹⁷, l'expiration de ce délai emporte leur intégration dans le service public des archives pourvu qu'elles présentent une utilité d'intérêt scientifique⁴⁹⁸. Il en ressort que les données médicales produites par tout établissement et professionnel de santé, quel que soit leur secteur, peuvent devenir des archives publiques en raison de leur intérêt scientifique⁴⁹⁹. Les archives publiques étant imprescriptibles⁵⁰⁰, les patients concernés par un traitement de leurs données médicales à des fins archivistiques dans l'intérêt public de la science ne peuvent exercer leur droit à l'effacement. Compte tenu de ce qui précède, toute donnée médicale aurait vocation à devenir une donnée de recherche au profit de la collectivité⁵⁰¹.

158. La réutilisation des données médicales à des fins de recherche dans l'intérêt public compromet le droit à l'effacement dont jouit, par principe, toute personne concernée⁵⁰². Dans ces conditions, le droit à l'oubli devient opposable au patient au bénéfice de l'intérêt général⁵⁰³. Assurément, le droit à l'effacement des données médicales empêcherait irrémédiablement leur réutilisation à des fins de recherche scientifique. Or, la réutilisation des données à des fins de recherche et d'innovation dans le domaine de la santé est indispensable au progrès des connaissances biologiques et médicales, à l'amélioration de la santé individuelle et collective, et à l'optimisation du système de santé. L'abaissement des droits du patient concerné sur ses données médicales colligées dans ses dossiers médicaux, dont notamment son droit à l'oubli, paraît donc nécessaire au bénéfice de l'intérêt de la collectivité. En ce sens, le quatrième considérant du RGPD souligne 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*

⁴⁹⁵ Article L.1641-1 III 6° du code de la santé publique

⁴⁹⁶ Article L1461-3 I 1° du code de la santé publique.

⁴⁹⁷ Article L.1461-4 IV du code de la santé publique.

⁴⁹⁸ Article R.1461-4 II du code de la santé publique.

⁴⁹⁹ Cf. Paragraphe 506.

⁵⁰⁰ Article L.212-1 du code du patrimoine.

⁵⁰¹ Cf. Paragraphes 441 et 506.

⁵⁰² Cf. Paragraphe 506.

⁵⁰³ *Ibid.*

fondamentaux, conformément au principe de proportionnalité ». Si le DMP avait vocation à devenir l'unique dossier médical du patient, le versement de ses données médicales dans un format structuré et interopérable avec le SNDS faciliterait leur mise à disposition au profit de l'intérêt général tout en préservant leur qualité et leur intégrité.

Paragraphe 2 : La modification du Dossier Médical Partagé

159. Conformément aux droits octroyés par le RGPD, le titulaire du Dossier Médical Partagé peut obtenir la modification des données médicales qu'il comporte auprès du professionnel de santé qui les y a reportées (**A**). En outre, le titulaire du Dossier Médical Partagé dispose du droit de modifier lui-même les informations qu'il y a consignées (**B**).

A) La modification des données consignées par les professionnels de santé

160. Le législateur national a pris le soin d'encadrer les droits que le titulaire du Dossier Médical Partagé détient sur les données qu'il contient. C'est ainsi que le code de la santé publique précise les modalités d'exercice des droits de modification des données personnelles – conférés par le RGPD – en tenant compte des particularités propres au droit de la santé. A la différence des dossiers de soins, le droit national envisage clairement la faculté, pour le titulaire du DMP, de rectifier les données qui y sont colligées (**1**) et de les effacer (**2**).

1. Le droit de rectification des données médicales colligées par les professionnels de santé

161. Le droit de rectification du DMP, octroyé par les dispositions de l'article R.1111-51 du code de la santé publique, correspond à celui consacré à l'article 16 du RGPD. La rectification des données du DMP doit alors être entendue comme la correction et la mise à jour des données inexactes, incomplètes et équivoques qu'il comporte. Tandis que les dispositions du code de la santé publique ne précisent pas les catégories de données pouvant faire l'objet d'une demande de rectification par la personne concernée, il faut comprendre que l'exercice de ce droit peut s'appliquer à toute donnée alimentée par les professionnels de

santé. Ainsi, le titulaire du DMP est fondé à demander la rectification de ses données administratives, mais également de ses données médicales.

162. Les demandes de rectification des données de nature administrative ne présentent pas de difficulté. Lorsque le titulaire du DMP décèle une erreur liée à son identité ou ses coordonnées, il est nécessaire qu'il fasse procéder à sa correction. A l'inverse de la rectification des données médicales, la correction des données administratives n'appelle pas à la discussion. En revanche, la rectification des données médicales recueillies et produites à l'occasion de la prise en charge sanitaire, lorsqu'elle est sollicitée par le patient, s'avère particulièrement délicate. Compte tenu de la complexité de l'évaluation d'une telle demande, il est nécessaire d'établir des éléments objectifs conditionnant l'exécution de ce droit. A cet effet, nous retiendrons les mêmes conditions cumulatives d'exercice du droit de rectification que celles dégagées pour les demandes de modification des données médicales contenues dans les dossiers de soins⁵⁰⁴. La rectification des données médicales contenues dans le DMP pourrait alors être admise à condition que les trois critères dégagés soient réunis : la remise en cause de la transposition d'une donnée médicale factuelle⁵⁰⁵, l'absence d'atteinte à l'intégrité de cette donnée⁵⁰⁶, et l'absence de décision médicale résultant d'une donnée médicale initialement erronée⁵⁰⁷. Autrement dit, la demande de rectification exercée par le patient ne pourrait être accordée qu'à la condition qu'elle porte sur une erreur purement factuelle ne pouvant faire l'objet d'une interprétation subjective.

163. Outre les données alimentées par les professionnels de santé, le DMP contient les données de remboursement des actes et des produits de santé pris en charge par l'organisme d'assurance maladie auquel l'assuré social est rattaché. Ces données sont automatiquement générées dans le DMP à partir du système d'information de l'Assurance maladie à l'instant où la procédure de remboursement est traitée. Lorsque le titulaire se connecte à son DMP, il est indiqué que les données de remboursement « *sont fournies à titre purement informatif et leur exhaustivité ne peut être garantie* »⁵⁰⁸. Faut-il comprendre que ces données peuvent

⁵⁰⁴ Cf. Paragraphe 138.

⁵⁰⁵ Cf. Paragraphe 139.

⁵⁰⁶ Cf. Paragraphe 140.

⁵⁰⁷ Cf. Paragraphe 141.

⁵⁰⁸ Voir : Plateforme web du DMP.

potentiellement se révéler inexactes ? Les données de remboursement contiennent le libellé du produit de santé délivré ainsi que le libellé et le code de l'acte prodigué par le professionnel de santé. Si les données de remboursement ne constituent pas véritablement des données médicales, elles correspondent tout au moins à des données personnelles concernant la santé. Le titulaire du DMP peut alors vérifier l'exactitude entre les actes et produits de santé qui lui ont été effectivement dispensés et ceux facturés à l'Assurance maladie. En cas d'erreur avérée, le titulaire du DMP devrait alors pouvoir demander la rectification de la donnée inexacte. Seulement, une telle rectification n'impliquerait pas uniquement la correction d'une donnée erronée. En effet, la rectification du libellé de l'acte dispensé par le professionnel de santé entraînerait la rectification du codage de cet acte selon la classification commune des actes médicaux sur laquelle repose ses règles de facturation. Une telle demande de rectification pourrait ainsi conduire l'Assurance maladie à réaliser un contrôle de l'adéquation entre la facturation de l'acte sur lequel porte la demande de rectification et l'acte réellement dispensé. Dans l'hypothèse d'une inexactitude avérée, l'établissement ou le professionnel de santé pourrait devoir répéter l'indu injustement facturé.

164. En théorie, le législateur n'a pas indiqué que les données de remboursement pouvaient effectivement faire l'objet d'une rectification par le titulaire du DMP. Faute de précision des données effectivement rectifiables, nous déduisons cette possibilité des dispositions de l'article R.1111-51 du code de la santé publique. Il y est précisé que « *le droit d'accès et de rectification des données personnelles contenues dans son dossier médical partagé, reconnu à son titulaire, s'exerce [...] [notamment] auprès de la Caisse nationale de l'assurance maladie dans les conditions définies par celle-ci, dans le respect des règles de confidentialité précisées au premier alinéa de l'article L. 1110-4* »⁵⁰⁹ dudit code. Assurément, l'accès aux données médicales contenues dans le DMP est, en vertu de l'article L.1110-4 du code de la santé publique, limité aux seuls professionnels participant à la prise en charge sanitaire de son titulaire. Par conséquent, la CNAM ne peut accéder aux données personnelles alimentées par les professionnels de santé et encore moins procéder à leur modification. En revanche, cet organisme peut certainement prendre connaissance des données de remboursement de tout assuré social. Il en résulte que la demande du droit de rectification exercée auprès de la

⁵⁰⁹ Article R.1111-51 3° du code de la santé publique.

Caisse nationale de l'assurance maladie ne devrait concerner que les données de remboursement générées au sein du DMP.

165. Si les modalités de rectification des données de remboursement paraissent obscures, les modalités de rectification des données médicales alimentées par les professionnels de santé sont formellement spécifiées par le législateur. En effet, le droit de rectification des données colligées au sein du DMP s'exerce « *auprès du professionnel autorisé à accéder au dossier médical partagé et identifié dans le dossier médical partagé comme l'auteur de la donnée à rectifier* »⁵¹⁰. En d'autres termes, lorsque le titulaire du DMP souhaite exercer son droit de rectification, il doit adresser sa demande auprès du professionnel de santé ayant recueilli ou produit ses données médicales à l'occasion de sa prise en charge sanitaire. Dans l'hypothèse où le professionnel de santé rectifie une donnée médicale erronée au sein du DMP, ne devrait-il pas subséquemment modifier le dossier de soins du patient ?

166. Les informations contenues au sein du DMP doivent être identiques à celles formalisées dans le dossier de soins du patient. Assurément, les données reportées dans le DMP sont générées, par tout professionnel de santé, à l'occasion de chaque acte, consultation ou séjour hospitalier de son titulaire⁵¹¹. Egalement, le DMP peut être alimenté des documents élaborés à l'occasion de la prise en charge sanitaire du patient, initialement intégrés au sein de son dossier de soins. Dans la mesure où les données médicales colligées dans le DMP et dans le dossier de soins du patient sont recueillies et produites par un même professionnel de santé à l'occasion d'une même prise en charge sanitaire, les données renseignées dans le DMP ne peuvent différer de celles contenues dans le dossier de soins. La rectification des données contenues dans le DMP – ou dans le dossier de soins – engendrerait donc une incohérence réciproque entre ces deux dossiers médicaux. Dans l'hypothèse où le professionnel de santé accueillerait favorablement la demande de rectification des données médicales factuelles du patient⁵¹², il serait indispensable de corriger les données analogues consignées dans le dossier corollaire. Autrement dit, la modification de l'un de ces dossiers devrait emporter la modification de l'autre avec, à l'appui, la traçabilité de leur rectification

⁵¹⁰ Article R.1111-51 1° du code de la santé publique.

⁵¹¹ Cf. Paragraphe 123.

⁵¹² Cf. Paragraphe 142.

identique. En effet, toute action et rectification devant être horodatées⁵¹³, les professionnels de santé effectuant la correction d'une donnée médicale devraient s'assurer de la similitude de chacun des dossiers médicaux qu'ils alimentent respectivement. Certainement, l'incohérence entre les dossiers médicaux du patient pourrait occasionner des risques dommageables pour la continuité et la coordination de ses soins.

167. Par ailleurs, le DMP du patient peut être alimenté par ses données médicales générées par les dispositifs médicaux connectés et référencés au catalogue de son Espace numérique de santé⁵¹⁴. Si les constantes du titulaire du DMP produites par des applications ou des objets connectés se révélaient inexactes, incomplètes ou équivoques, il devrait pouvoir en demander la rectification. A ce titre, le droit national affirme que le titulaire du DMP peut exercer son droit de rectification « *auprès du responsable de l'outil ou du service numérique en santé [...] qui se trouve à l'origine de l'enregistrement de la donnée dans le dossier médical partagé* »⁵¹⁵. Dans cette hypothèse, les critères objectifs de modification de la donnée médicale, dégagés à l'occasion de ces travaux de recherche⁵¹⁶, pourraient être évalués par le responsable du dispositif médical connecté avant que le DMP ne soit effectivement modifié.

Si la modification du DMP peut intervenir par la rectification des données qu'il comporte, sa modification peut également résulter de l'effacement des données qui y sont renseignées par les professionnels de santé.

2. Le droit à l'effacement des données médicales colligées par les professionnels de santé

168. Toute personne concernée par le traitement de ses données personnelles bénéficie du droit d'en demander l'effacement dans les conditions de l'article 17 du RGPD auprès du responsable de leur traitement. Tandis que la CNAM a été légalement désignée comme responsable de la conception du DMP, les professionnels qui procèdent à son alimentation

⁵¹³ Article R.1111-43 du code de la santé publique ; Cf. Paragraphe 141.

⁵¹⁴ Article L.1111-13-1 II 3° du code de la santé publique.

⁵¹⁵ Article R.1111-51 2° du code de la santé publique.

⁵¹⁶ Cf. Paragraphes 138 à 142.

assument la responsabilité de cette opération de traitement⁵¹⁷. Par conséquent, le titulaire du DMP ne peut pas, par lui-même, « *supprimer les données qui ont été enregistrées par un professionnel, un établissement de santé, un établissement ou un service social ou médico-social ou l'hôpital des armées* »⁵¹⁸. Certainement, le patient qui souhaite exercer son droit à l'effacement des données médicales qui y sont reportées doit adresser sa demande « *auprès de l'auteur de ces données* »⁵¹⁹ à la condition de justifier d'un « *motif légitime* »⁵²⁰.

169. Effectivement, les pouvoirs publics conditionnent l'exercice du droit à l'effacement des données reportées par les professionnels de santé dans le DMP à l'existence d'un motif légitime pour son titulaire. A l'aune de la directive 95/46 du 24 octobre 1995⁵²¹, le droit à l'effacement pouvait s'exercer à condition de justifier d'un motif légitime évalué par le responsable de traitement⁵²². Toutefois, le législateur européen a abandonné cette notion au profit de six motifs objectifs conditionnant l'exercice du droit à l'effacement des données personnelles⁵²³. Compte tenu de la primauté du droit européen sur le droit national, la justification de l'existence d'un motif légitime pour le titulaire du DMP ne devrait donc suffire à accorder l'effacement de ses données personnelles qui y sont consignées. Certainement, la loi Informatique et Libertés modifiée affirme que « *le droit à l'effacement s'exerce dans les conditions prévues à l'article 17 du règlement (UE) 2016/679 du 27 avril 2016* »⁵²⁴. Il en résulte que les professionnels auteurs des données reportées dans le DMP doivent examiner la demande d'effacement à la lumière des conditions édictées à l'article 17 du RGPD. Il convient alors d'examiner chacune des hypothèses dans lesquelles le titulaire du DMP pourrait être fondé à demander la suppression de ses données personnelles. Cette étude suppose d'étudier les différentes opérations de traitement inscrites dans le DMP.

⁵¹⁷ Cf. Paragraphe 122.

⁵¹⁸ Article R.1111-51 du code de la santé publique.

⁵¹⁹ *Ibid.*

⁵²⁰ *Ibid.*

⁵²¹ 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, JOUE n° L 281, 23 novembre 1995, p. 31-50.

⁵²² Cf. Paragraphe 144.

⁵²³ *Ibid.*

⁵²⁴ Article 51 I de la loi Informatique et Libertés modifiée.

170. D'abord, l'alimentation du DMP peut consister en une obligation pour les professionnels de santé à compter de sa création automatique⁵²⁵. Compte tenu de la base juridique sur laquelle repose cette opération de traitement⁵²⁶, le droit à l'effacement des données médicales qui y sont colligées devrait être inopérant nonobstant la justification de motifs légitimes pour son titulaire. Néanmoins, par analogie avec le dossier de soins, le titulaire du DMP devrait pouvoir en demander la suppression lorsqu'elles n'apparaissent pas pertinentes, adéquates et limitées à ce qui est nécessaire à la coordination de ses soins⁵²⁷. Lorsque les données médicales incluses dans le DMP ne sont pas minimisées à la coordination des soins de son titulaire, il lui appartient de contacter le professionnel de santé qui en est l'auteur afin qu'il apprécie l'adéquation entre l'information personnelle et la finalité de leur traitement. En cas de divergence, la personne concernée devrait pouvoir solliciter l'interprétation médicale d'un tiers professionnel de santé alors chargé d'examiner la licéité des données intégrées dans son DMP en toute impartialité⁵²⁸. Dès lors que l'illicéité de la collecte de la données médicale est avérée, son auteur est obligé de l'effacer de ce dossier médical numérique. Par ailleurs, le titulaire du DMP devrait pouvoir exiger l'effacement de ses données médicales à l'issue du terme de leur durée de conservation⁵²⁹. Or, le DMP correspond à un carnet de santé numérique ayant vocation à perdurer tout au long de la vie de son titulaire et, ainsi, à retracer l'intégralité de son histoire médicale⁵³⁰. A moins que la personne concernée ne sollicite la clôture de son dossier médical numérique, seul son décès entraîne sa fermeture et, consécutivement⁵³¹, l'effacement de ses données médicales à l'issue d'un délai de dix années⁵³². Il en résulte que le décès du titulaire du DMP permet de déterminer la durée de ce traitement de données à caractère personnel et la période de leur conservation.

⁵²⁵ Cf. Paragraphe 123.

⁵²⁶ Article 6.1 c) du RGPD.

⁵²⁷ Article 17.1 d) du RGPD.

⁵²⁸ Cf. Paragraphe 126.

⁵²⁹ Article 17.1 a) du RGPD.

⁵³⁰ Cf. Paragraphe 94.

⁵³¹ Article L.1111-13-1 IV 3° du code de la santé publique.

⁵³² Article R.1111-36 alinéa 2 du code de la santé publique.

171. Ensuite, l'opération de traitement consistant en l'alimentation du DMP par les non-professionnels de santé et le médecin du travail repose sur le consentement de son titulaire⁵³³. Dans cette hypothèse, le législateur européen annonce que « *la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant [...] lorsque [...] la personne concernée retire le consentement sur lequel est fondé le traitement* »⁵³⁴. A priori, le titulaire du DMP pourrait alors solliciter, auprès de ces professionnels, la suppression de ses données médico-sociales et des éléments de son dossier de santé au travail au moment du retrait de son consentement. Néanmoins, le législateur européen limite le droit à l'effacement des données médicales lorsqu'elles apparaissent nécessaires à la prise en charge sanitaire de la personne concernée⁵³⁵. De la même façon, le pouvoir exécutif aurait-il limité l'exercice du droit à l'effacement en le soumettant à l'allégation de motifs légitimes ? Eu égard au fondement juridique du remplissage du DMP par les non-professionnels de santé et le médecin du travail, le droit à l'effacement des informations qu'ils y ont versées pourrait éventuellement être appliqué sous réserve de justifications appropriées.

172. Finalement, le traitement aux fins de création du DMP, dont la responsabilité incombe à la CNAM, est fondé sur les motifs d'intérêt public dont cet organisme a été légalement investi⁵³⁶. En vertu de ce fondement juridique, la personne concernée peut s'opposer, à tout moment, au traitement de ses données personnelles⁵³⁷. C'est ainsi que le titulaire du DMP peut, n'importe quand, procéder à sa fermeture⁵³⁸ soit directement, soit en formulant sa demande auprès du responsable de traitement. La clôture du DMP emporte l'archivage des données personnelles qu'il contient pendant une période de dix ans à l'issue de laquelle elles sont supprimées automatiquement⁵³⁹. Toutefois, l'exercice du droit d'opposition au traitement par la personne concernée lui ouvre le droit de demander l'effacement de ses

⁵³³ Cf. Paragraphe 125.

⁵³⁴ Article 17.1 a) du RGPD.

⁵³⁵ Article 17.3 c) du RGPD.

⁵³⁶ Article 6.1 e) du RGPD.

⁵³⁷ Article 21.1 du RGPD.

⁵³⁸ Article R.1111-52 du code de la santé publique.

⁵³⁹ Article R.1111-36 alinéa 2 du code de la santé publique.

données personnelles⁵⁴⁰. Par conséquent, le titulaire du DMP peut expressément demander la suppression des informations qui le concernent avant le terme du délai d'archivage susmentionné. Dans cette hypothèse, « *il est fait droit à sa demande dans un délai maximum de trois mois* »⁵⁴¹. Néanmoins, la durée de l'archivage du DMP correspond au délai de prescription de l'action en responsabilité médicale. Si la personne concernée demandait la suppression définitive de son contenu avant le terme de son archivage, elle risquerait de perdre des éléments de preuve indispensables à la caractérisation d'une faute médicale ou d'un aléa thérapeutique. Seulement, le délai de prescription ne courant qu'à compter de la date de consolidation du dommage, le DMP peut être définitivement supprimé avant même que la prescription de l'action en responsabilité civile ne soit éteinte.

173. Hormis la situation où les données sont traitées de façon illicite, l'effacement des informations médicales reportées dans le DMP ne peut intervenir qu'au moyen de sa clôture. En d'autres termes, seule la clôture du DMP donne droit, pour son titulaire, à l'effacement des données personnelles alimentées par les professionnels de santé. Manifestement, les données contenues dans le DMP ont vocation à subsister en son sein aussi longtemps que le titulaire vivra.

B) La modification des données documentées par le titulaire du Dossier Médical Partagé

174. Le Dossier Médical Partagé est un carnet de santé numérique par lequel tout assuré social devient l'acteur de son parcours de santé par la gestion de ses données médicales. Le titulaire du DMP peut, entre autres, consulter les informations qui y sont reportées, autoriser les professionnels concourant à sa prise en charge sanitaire à y accéder, ajouter des informations et documents utiles à la coordination des soins et maîtriser les données qui y figurent. Parmi les prérogatives qui lui sont octroyées, « *le titulaire peut rectifier lui-même les informations qu'il a consignées dans son dossier médical partagé* »⁵⁴². Si les données personnelles renseignées au sein du DMP peuvent être modifiées par leur auteur, le titulaire du DMP peut directement modifier les informations qu'il y a reportées. En effet, il peut, à

⁵⁴⁰ Article 17.1 c) du RGPD.

⁵⁴¹ Article R.1111-36 alinéa 3 du code de la santé publique.

⁵⁴² Article R.1111-51 du code de la santé publique.

tout moment, modifier ses coordonnées, les informations relatives à l'organisation de sa fin de vie et les informations relatives à sa santé (antécédents, allergies, documents produits antérieurement à l'ouverture du dossier, etc.) en s'y connectant directement grâce à l'Internet. La modification des données consignées par le titulaire du DMP comprend tant leur rectification que leur effacement. Seulement, alors que certaines données administratives ne peuvent être modifiées, certaines données connexes à la santé devraient y être conservées.

175. A la création du DMP, les données d'identification telles que le nom, le prénom, le sexe, la date de naissance et l'identifiant national de santé sont générées automatiquement. Ces informations n'étant pas renseignées par le titulaire du DMP, celui-ci ne peut procéder à leur modification. En effet, le législateur a affirmé que le titulaire du DMP ne pouvait modifier que les informations dont il était l'auteur. A l'instar des dossiers de soins, ces informations participant à l'identitovigilance sont essentielles. Dès lors, leur renseignement est obligatoire et leur effacement impossible. Néanmoins, si ces informations s'avéraient inexacts, le titulaire du DMP aurait la possibilité de les faire rectifier auprès de la CNAM en sa qualité de responsable du traitement à des fins de conception du DMP. En complément de ces informations administratives, le titulaire du DMP doit renseigner ses coordonnées. L'ensemble des coordonnées postales, téléphoniques et numériques reportées dans cet outil peuvent être rectifiées par leur auteur. Toutefois, certaines de ces données doivent être impérativement renseignées dans la mesure où le DMP comporte des « champs obligatoires ». En conséquence, le titulaire du DMP ne peut effacer mais seulement corriger son numéro de téléphone mobile et son adresse électronique. Les droits que le titulaire du DMP détient sur ses données administratives apparaissent donc limités.

176. Outre ces données administratives, le titulaire du DMP peut modifier les informations qu'il a inscrites dans la rubrique relatives à « ses droits et volontés ». En effet, ce dernier peut librement rectifier les informations relatives aux personnes à prévenir en cas d'urgence, à la personne de confiance désignée, aux directives anticipées déposées et au don d'organes et de tissus. Pareillement, le titulaire du DMP peut supprimer chacune de ces informations. À tout moment, il peut décider de révoquer les personnes à prévenir en cas d'urgence et la personne de confiance renseignées. Il peut également effacer le document consignait ses directives anticipées. De même, il peut supprimer la déclaration selon laquelle il a été effectivement informé des dispositions portant sur le prélèvement d'organes et de tissus effectué sur une personne décédée. Cependant, la portée de la réception d'une telle information est limitée.

En effet, faute de refus clairement exprimé, toute personne est présumée consentir au don de ses organes et de ses tissus⁵⁴³. Si le DMP permet à son titulaire d'attester de la réception d'une information relative au don, ce dossier numérique ne permet pas de s'y opposer. Pour l'heure, l'opposition au don d'organes et de tissus ne peut être inscrite que sur le registre national des refus tenu par l'Agence de la biomédecine⁵⁴⁴. L'expression de ce refus peut également être consignée au sein d'un écrit confié à un proche ou affirmée à l'oral auprès des proches de la personne concernée. Il est regrettable que le DMP ne permette pas d'ajouter un document faisant valoir ce refus écrit, daté et signé. Malgré que le DMP se borne à renseigner la prise en compte, par son titulaire, d'une information portant sur les dispositions relatives à ces dons, son titulaire peut renseigner toute donnée, au moyen d'une saisie de texte libre ou de documents versés. Dès lors, le titulaire du DMP peut prendre l'initiative d'indiquer, de façon générale ou partielle, son opposition au don de ses organes et de ses tissus.

177. Finalement, le titulaire du DMP a la possibilité de renseigner ses données médicales et de santé en rédigeant un document composé d'une expression libre, ou en joignant un fichier. Ces documents, consignés par le titulaire du DMP, peuvent être modifiés à tout moment. En effet, le titulaire du DMP peut rectifier le titre et la nature du document. De même, lorsque le document est constitué d'une expression libre, le titulaire du DMP peut directement en corriger le contenu. En prime, il peut exercer son droit à l'effacement des données en supprimant l'ensemble des documents qu'il a ajoutés. Toutefois, même si le document supprimé n'est plus accessible ni pour le titulaire, ni pour les professionnels de santé, une mention inscrite sur la plateforme du DMP indique qu'il sera conservé dans une zone spécifique de sauvegarde. Aucune disposition législative ou réglementaire n'indique les modalités de sauvegarde des documents supprimés par le titulaire du DMP. Pourtant, la sauvegarde d'une donnée étant une opération de traitement⁵⁴⁵, il aurait été légitime que cette mention explicite la durée et le lieu de conservation de l'information supprimée. A défaut de précision, nous pouvons déduire que la donnée supprimée demeure conservée auprès de l'hébergeur de données de santé auprès duquel le DMP a été créé⁵⁴⁶. En effet, cet hébergeur

⁵⁴³ Article L.1232-1 alinéa 3 du code de la santé publique.

⁵⁴⁴ *Ibid.*

⁵⁴⁵ Article 4.2 du RGPD.

⁵⁴⁶ Article L.1111-14 alinéa 6 du code de la santé publique.

garantit, entre autres, la sauvegarde des données collectées dans ce cadre⁵⁴⁷. En outre, nous pouvons déduire que ces données sauvegardées demeureront jusqu'à la suppression définitive du DMP, à savoir dix années après sa clôture⁵⁴⁸.

178. Compte tenu de ce qui précède, le titulaire du DMP semble jouir de la pleine effectivité des droits qu'il détient sur les données connexes à sa santé qu'il y a consignées. Assurément, celui-ci peut les modifier sans justification, ni condition. Nous pouvons donc affirmer que le titulaire du DMP dispose de l'entière maîtrise des données sanitaires dont il est l'auteur. A cet égard, ces prérogatives pourraient être assorties de devoirs. En ce sens, les conditions générales d'utilisation du DMP signalent que « *les utilisateurs du service sont seuls responsables [...] des informations et documents qu'ils seraient susceptibles d'y ajouter les concernant* »⁵⁴⁹. Ainsi, le titulaire du DMP devrait veiller à la bonne gestion des informations dont il est l'informateur, notamment en veillant à l'actualisation de ses informations médicales. En effet, tout document ajouté par le titulaire du DMP peut être porté à la connaissance des professionnels de santé. En conséquence, ces informations médicales peuvent orienter ou fonder les analyses médicales élaborées par les professionnels de santé y ayant accès. Au moyen du DMP, le patient devient donc véritablement un acteur des décisions médicales le concernant. A ce titre, le titulaire du DMP devrait concourir à la coordination de ses propres soins en s'abstenant de supprimer tout document nécessaire à cette finalité. D'une autre manière, le titulaire du DMP devrait tenir à jour l'expression de ses droits et volontés. En définitive, l'autodétermination informationnelle du titulaire du DMP devrait pouvoir s'exercer de façon responsable eu égard au fait que ce dernier est à compter parmi les acteurs du monde de la santé⁵⁵⁰.

⁵⁴⁷ Article L.1111-8 du code de la santé publique.

⁵⁴⁸ Article L.1111-18 alinéa 5 du code de la santé publique.

⁵⁴⁹ Article 6.2 des conditions générales d'utilisation du service DMP pour les bénéficiaires de l'assurance maladie.

⁵⁵⁰ Il existe, en France, cinq acteurs du système de santé qu'il est possible de distinguer : les offreurs de soins, les producteurs de biens et services en santé, les institutions publiques, les financeurs du système de santé et les bénéficiaires, à savoir, les usagers du système de santé. VIE PUBLIQUE, *Qu'est-ce qu'un système de santé*, 29 février 2016. Disponible en ligne sur le site : [<http://www.vie-publique.fr>], consulté le 05 avril 2020.

Conclusion du chapitre

179. Le caractère impérieux de la constitution et de l'alimentation des dossiers médicaux tend à restreindre les droits que le patient détient sur ses données personnelles, *a fortiori* lorsqu'elles ont été recueillies ou produites par les professionnels de santé lors de sa prise en charge médicale.

En principe, toute personne concernée par un traitement de données personnelles bénéficie, en vertu des droits qui lui sont reconnus par le RGPD, de la maîtrise des informations qui la concernent. Seulement, dans le cadre d'une prise en charge sanitaire, seuls les professionnels de santé doivent pouvoir contrôler les données médicales indispensables à la dispensation des actes de prévention, de diagnostic et de soins ainsi qu'à la coordination et à la continuité du parcours de santé. Assurément, la délivrance des services de soins de santé repose exclusivement sur les données médicales générées à l'occasion de la prise en charge sanitaire et formalisées au sein des dossiers médicaux attachés au patient.

Dès lors, l'interférence du patient dans la gestion de ses informations médicales pourrait contrarier et importuner la délivrance de soins consciencieux, attentifs et dévoués⁵⁵¹. En conséquence, la limitation des droits du patient sur les données contenues dans ses dossiers médicaux apparaît donc impérieuse et légitime.

⁵⁵¹ Article R.4127-32 du code de la santé publique.

Conclusion du titre

180. La prise en charge médicale du patient suppose le traitement de ses données administratives et de santé. Plus spécifiquement, tout acte de prévention, de diagnostic ou de soins repose sur l'analyse des informations médicales de la personne concernée. Pour ce faire, le professionnel de santé procède à leur collecte et les formalise au sein des dossiers médicaux du patient. Plus qu'un processus indispensable à la prise en charge sanitaire, ces traitements de données personnelles sont exigés par les dispositions réglementaires du code de la santé publique. En effet, les établissements et les professionnels de santé doivent obligatoirement constituer et alimenter un dossier de soins pour tout patient pris en charge. Au surplus, lorsqu'il a été ouvert, les professionnels de santé doivent obligatoirement alimenter le DMP du bénéficiaire de l'Assurance maladie ou de l'aide médicale d'Etat par les informations médicales nécessaires à la coordination et à la continuité de ses soins.

Ces traitements de données sensibles sont exceptionnellement autorisés dans la mesure où ils sont indiscutablement nécessaires à la prise en charge sanitaire des personnes concernées⁵⁵². De surcroît, ces traitements sont juridiquement fondés sur les obligations réglementaires qui pèsent sur les responsables de traitement⁵⁵³. En conséquence, le patient ne peut s'opposer ni à la constitution de son dossier de soins, ni à l'alimentation de son DMP. De la même manière, les droits que le patient devrait théoriquement détenir sur les données contenues dans ses dossiers médicaux se trouvent limités.

Il est important de noter que les dispositions du RGPD façonnent le droit commun de la protection des données personnelles sans tenir compte des spécificités inhérentes à la finalité du traitement ou à la nature des informations traitées. C'est pourquoi « *le droit à la protection des données à caractère personnel [...] doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux* »⁵⁵⁴. En raison de la nécessité du traitement des données médicales pour la prise en charge sanitaire

⁵⁵² En vertu de l'article 9.2 h) du RGPD.

⁵⁵³ En vertu de l'article 6.1 c) du RGPD.

⁵⁵⁴ Considérant 4 du RGPD.

du patient, la protection et la préservation de sa santé⁵⁵⁵ semblent primer, au regard de leur impériosité, sur les droits qui lui sont reconnus à l'égard des informations qui le concernent.

181. Compte tenu de ce qui précède, il apparaît donc légitime de limiter la portée des actions du patient sur ses données médicales dès lors qu'il a consenti à sa prise en charge sanitaire. Par conséquent, la seule façon de conserver son autodétermination informationnelle sur ses informations sensibles résiderait dans le renoncement aux soins.

⁵⁵⁵ La protection et la préservation de la santé des individus étant un principe général du droit garanti par le onzième alinéa du préambule de la Constitution du 27 octobre 1946.

TITRE 2 :

LA COMMUNICATION DES DONNEES MEDICALES FORMALISEES DANS LES DOSSIERS MEDICAUX DU PATIENT

182. L'ensemble des informations médicales collectées et produites à l'occasion de la prise en charge sanitaire du patient doivent être formalisées dans un dossier médical. A cet effet, elles sont systématiquement répertoriées et conservées dans un document identifié. Ce travail de formalisation permet de transposer et de réifier un état biologique en une donnée médicale tangible et accessible. Il en advient que la matérialisation des données médicales du patient au sein d'un fichier constitue le préalable essentiel à leur communicabilité.

La formalisation des informations médicales présente un intérêt, en particulier pour la coordination et la continuité du parcours de santé du patient. De cette façon, le professionnel qui intervient à sa prise en charge sanitaire peut prendre connaissance de son historique médical et, ainsi, établir un diagnostic ou déterminer une thérapeutique en considération de ses antécédents médicaux. En conséquence, la formalisation des informations médicales du patient et leur communication entre les professionnels participant à son parcours de santé garantissent la qualité, la sécurité et la continuité de ses soins (**Chapitre 2**). C'est pourquoi la circulation de la donnée médicale du patient entre les professionnels concourant à sa prise en charge manifesterait un caractère impérieux.

183. Toutefois, si la communication des informations médicales formalisées entre ces professionnels est permise, c'est à condition que le patient accepte de leur confier les informations intimes qui le concernent. En effet, les informations médicales correspondent à des données personnelles touchant à l'intimité de la vie privée de la personne concernée. Le patient est alors observé comme l'unique détenteur de ses données médicales et le seul titulaire du secret médical, au demeurant partagé avec les professionnels concourant à sa prise en charge sanitaire. Dès lors, le patient est en droit d'obtenir l'accès aux données collectées lors de son parcours de santé (**Chapitre 1**).

Chapitre 1 :

L'accès du patient aux données médicales générées lors de sa prise en charge sanitaire

184. Le droit d'accès est considéré comme le premier des droits octroyés à la personne concernée par le traitement de ses données personnelles. En effet, l'exercice de ce droit lui permet « *d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données* »⁵⁵⁶. Par suite, la personne concernée est en mesure de vérifier les données la concernant et, le cas échéant, d'en demander la rectification ou la suppression. Autrement dit, le droit d'accès semble promouvoir l'exercice de droits subséquents. Egalement, le droit d'accès aux données personnelles est observé comme le corollaire du droit à l'information qui incombe au responsable de traitement. Appliqué au secteur de la santé, le droit d'accès aux données médicales, *a fortiori* lorsqu'elles sont consignées dans un dossier éponyme, renforce le droit à l'information médicale du patient et accroît la transparence dans la relation de soins. Au-delà d'un mécanisme de maîtrise de ses données personnelles, le droit d'accès direct aux données médicales permet donc au patient de prendre le contrôle de sa santé (**Section 1**). Si le droit d'accès aux données personnelles constitue un droit fondamental⁵⁵⁷, il n'en demeure pas moins que l'accès aux données formalisées dans les dossiers médicaux du patient connaît certaines restrictions, non absolues, justifiées par la protection de la personne en état de vulnérabilité ainsi que par la confidentialité des informations relatives aux tiers à la prise en charge sanitaire (**Section 2**).

⁵⁵⁶ Article 15 du RGPD.

⁵⁵⁷ Article 8 de la Charte des droits fondamentaux de l'Union Européenne, *JOUE* du 26 octobre 2012.

Section 1 : Le principe de l'accès direct aux données médicales consignées dans les dossiers médicaux

185. Le droit d'accès aux données médicales constitue un droit personnel attaché à la personne concernée. En conséquence, l'exercice du droit d'accès aux données médicales ne peut, en principe, être exercé que par le principal intéressé (**Paragraphe 1**). Seulement, lorsque la personne concernée est frappée d'une incapacité juridique en raison de son âge ou de l'altération de ses facultés mentales, l'exercice de ce droit subjectif peut également être dévolu à l'organe en charge de sa protection (**Paragraphe 2**). Sauf exception, l'ensemble des destinataires de l'information médicale concernant la santé du patient bénéficie également d'un droit d'accès à ses données médicales.

Paragraphe 1 : L'exercice du droit d'accès direct par la personne concernée

186. Les données médicales consignées dans les dossiers médicaux du patient touchent à l'intimité de sa vie privée. Dès lors, ces informations personnelles et confidentielles ne peuvent lui être dissimulées. Assurément, le secret médical est inopposable au patient. Ainsi, le droit d'accès aux données médicales consacre un « *droit de savoir* »⁵⁵⁸ exercé *a posteriori* de tout acte de prévention, de diagnostic ou de soins (**A**). Ce droit particulier déroge au droit commun de l'accès aux données personnelles tel que prescrit par le RGPD. En effet, les règles de l'accès aux données consignées dans les dossiers médicaux du patient sont spécifiées par le code de la santé publique (**B**).

A) La reconnaissance du droit d'accès direct à l'information médicale

187. À l'époque du paternalisme médical⁵⁵⁹, le patient ignorant était opposé au médecin sachant auquel il abandonnait la gestion de sa santé. La confiance absolue que le patient accordait au soignant reposait sur l'occultation de l'information médicale. En effet, le médecin estimait qu'il était inenvisageable d'instruire le patient et moins encore de le faire consentir aux décisions médicales. Le patient ne pouvait qu'acquiescer le diagnostic posé et

⁵⁵⁸ Expression analogue au « droit à l'information » utilisée lors des travaux préparatoires de la loi n° 2002-303 du 4 mars 2002, *op. cit.*

⁵⁵⁹ Antérieurement à la loi n°2002-303 du 4 mars 2002, *loc. cit.*

le traitement associé sans en comprendre les vertus. Seulement, l'ignorance du patient engendrait une asymétrie et un déséquilibre dans la relation qu'il entretenait avec le médecin. Le savoir unilatéral du médecin le plaçait dans une position de domination et de suprématie⁵⁶⁰. De cette façon, le médecin appréciait souverainement l'opportunité de tenir le patient dans la méconnaissance de sa maladie. Comme l'écrivait Henri de Mondeville, chirurgien français du XIII^{ème} siècle, « *le moyen pour le chirurgien de se faire obéir de ses malades, c'est de leur exposer les dangers qui résultent pour eux de leur désobéissance. Il les exagérera si le patient a l'âme brave et dure ; il les atténuera, les adoucira ou les taira si le malade est pusillanime ou bénin, de crainte qu'il ne désespère* »⁵⁶¹. Le médecin se trouvait donc libre de délivrer les éléments qu'il jugeait favorable à l'obtention de l'adhésion du malade. Le patient pouvait ainsi être trompé par un médecin qui le tenait à distance de son destin. Fort heureusement, depuis le célèbre arrêt Teyssier⁵⁶² rendu le 28 janvier 1942, et aux travaux engagés par le législateur, cette réticence dolosive⁵⁶³ a laissé place à la transparence dans la relation médicale.

188. En effet, plus qu'une obligation prétorienne⁵⁶⁴ et déontologique⁵⁶⁵ incombant aux professionnels de santé, le droit à l'information médicale a été consacré comme un droit fondamental du patient par la loi relative aux droits des malades du 4 mars 2002⁵⁶⁶. A cet égard, les dispositions de l'article L.1111-2 du code de la santé publique explicitent que « *toute personne a le droit d'être informée sur son état de santé* ». Ce droit à l'information est assimilé à un droit à la transparence quant aux « *différentes investigations, traitements ou actions de prévention qui sont proposés, leur utilité, leur urgence éventuelle, leurs*

⁵⁶⁰ Voir : LAUDE (A.), *Le consommateur de soins*, Recueil Dalloz, 2000, n°26, p. 415.

⁵⁶¹ DE MONDEVILLE (H.), *La chirurgie*, Tome 1, ed. 1897-1898, Société des anciens textes français, Bibliothèque nationale de France. Disponible en ligne sur le site [<https://gallica.bnf.fr>]. Consulté le 30 décembre 2020.

⁵⁶² Cass. req., 28 janvier 1942, Teyssier, Gaz. Pal., 62, 1942, 1, p. 177 ; D. Recueil critique de jur., 1942, p. 63.

⁵⁶³ Voir : PY (B.), SEGURA (J.), *L'obligation d'information est le devoir incombant à la partie qui détient une information utile à l'autre partie de la lui délivrer, si cette information peut avoir une influence sur son consentement*, RDS, 2005, n° 08, p. 505 ; DEBOST (V.-C.), GIRAUDEAU (N.), VERON (P.), VIALLA (F.), *La réforme du Code de déontologie médicale*, RGDM, 2012, n° 44, p. 231.

⁵⁶⁴ Arrêt Teyssier, *loc. cit.*

⁵⁶⁵ Article R.4127-35 du code de la santé publique (médecin) ; Article R.4127-236 du code de la santé publique (chirurgien-dentiste) ; Article R4312-13 du code de la santé publique (Infirmier) ; Article R.4321-83 du code de la santé publique (Masseur-kinésithérapeute) ; Article R.4322-55 du code de la santé publique (Pédicure-podologue).

⁵⁶⁶ Loi n°2002-303 du 4 mars 2002, *loc. cit.*

conséquences, les risques fréquents ou graves normalement prévisibles qu'ils comportent ainsi que sur les autres solutions possibles et sur les conséquences prévisibles en cas de refus »⁵⁶⁷. Ainsi, les connaissances médicales relatives à la santé du malade ne relèvent plus du monopole du soignant. Ce dernier a l'obligation légale de délivrer l'intégralité des composantes de l'information médicale au principal intéressé : le patient. Hormis l'hypothèse où le patient a manifesté la volonté d'être tenu dans l'ignorance d'un diagnostic ou d'un pronostic⁵⁶⁸, il est interdit au professionnel de santé de taire toute information médicale concernant le malade. Par conséquent, le soignant – placé dans la phase passive de l'obligation – devient débiteur de l'information médicale et le patient devient créancier d'un droit exigible. Subséquemment, l'inexécution de cette obligation cause au patient un préjudice moral, autonome de tout préjudice corporel, lui ouvrant droit à réparation⁵⁶⁹. L'information médicale du patient constitue donc un droit général et absolu.

189. L'esprit du droit à l'information est corroboré par le droit du patient à l'accès direct aux informations médicales le concernant, également institué par la loi relative aux droits des malades⁵⁷⁰. En effet, « *la possibilité pour une personne d'accéder directement aux informations formalisées ne fait que compléter son droit à l'information* »⁵⁷¹. Guillaume Rousset considère que « *l'accès direct au dossier médical est souvent présenté comme une mutation emblématique permise par la loi du 4 mars 2002, symbolisant le droit de regard des patients sur les informations relatives à leur santé* »⁵⁷². Jusqu'à l'entrée en vigueur de cette loi emblématique, l'accès aux données médicales contenues au sein des dossiers médicaux du patient ne pouvait intervenir qu'indirectement par l'intermédiaire d'un médecin désigné par le malade. Désormais, les dispositions de l'article L.1111-7 du code de la santé

⁵⁶⁷ Article L.1111-2 I alinéa 1 du code de la santé publique.

⁵⁶⁸ *Ibid.*

⁵⁶⁹ Civ. 1^{ère}, 3 juin 2010, n° 09-13.591, Bull. civ. I n° 128 ; RGDM, 2010, n° 36, p. 233, note S. Prieur ; Recueil Dalloz, 2010, p. 1522, note P. Sargos, p. 2092, chron. N. Auroy et C. Creton ; RDSS, 2010, n° 05 p. 898, note F. Arhab-Girardin ; RTD civ. 2010, n° 03, p. 571, obs. P. Jourdain ; JCP 2010, p. 788, note S. Porchy-Simon, et Chron. resp. civ. 1015, spéc. n° 3 et 6 ; C. Corgas-Bernard, RLDC, oct. 2010, p. 21 ; LPA 17-18 août 2010, note R. Milawsk.

⁵⁷⁰ Loi n°2002-303 du 4 mars 2002, *loc. cit.*

⁵⁷¹ Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, *JORF* n°65 du 17 mars 2004, *op. cit.*

⁵⁷² ROUSSET (G.), *Le droit à l'information de l'utilisateur et du patient depuis les lois des 2 janvier et 4 mars 2002*, RDSS, 2012, n°3, p. 431.

publique énoncent que « *toute personne a accès à l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit* » par tout professionnel de santé et toute structure sanitaire. Bien que le patient puisse toujours solliciter un accès indirect par l'intermédiaire du médecin de son choix, celui-ci jouit d'un accès direct aux données médicales le concernant « *sans que l'entremise d'un professionnel de santé ne soit imposée* »⁵⁷³. Le droit, pour le patient, d'accéder directement aux données médicales générées lors de sa prise en charge sanitaire s'avère donc lié au droit d'être informé sur son état de santé.

190. Si les dispositions du code de la santé publique encadrent les conditions d'exercice du droit d'accès direct aux informations médicales du patient, « *le droit d'accès aux informations médicales codifié à l'article L.1111-7 est fondé sur des droits fondamentaux* »⁵⁷⁴. En effet, cette prérogative repose sur le droit commun de l'accès aux documents administratifs, ainsi que sur le droit commun de l'accès aux données à caractère personnel. Concrètement, le patient qui souhaite accéder aux informations concernant sa santé peut fonder sa demande au moyen de ces deux principes fondamentaux.

191. En premier lieu, lorsque les données médicales du patient sont détenues par un établissement de santé chargé d'une mission de service public, le patient peut fonder sa demande sur le droit d'accès aux documents administratifs. En effet, les dossiers médicaux constitués par les établissements de santé participant au service public hospitalier disposent de la qualité de documents administratifs⁵⁷⁵. A ce titre, et compte tenu du principe de la communicabilité de ces documents⁵⁷⁶, ces établissements sont tenus de transmettre, au patient intéressé, les informations médicales formalisées au sein de son dossier médical hospitalier. Bien que le droit d'accès à ce dossier repose sur le droit à la communication des documents administratifs, cette communication doit néanmoins être exécutée dans le respect des dispositions de l'article L.1111-7 du code de la santé publique⁵⁷⁷. Lorsque l'établissement de santé rejette la demande formée par le patient, ce dernier dispose d'un délai de deux mois

⁵⁷³ VIALLA (F.), *L'accès du dossier médical*, In VIALLA (F.), *Les grandes décisions du droit médical*, op. cit., p. 217.

⁵⁷⁴ LALLET (A.), NGUYEN DUY (P.), *Communication des documents administratifs*, Répertoire de contentieux administratif, juin 2019.

⁵⁷⁵ Article L.300-2 du code des relations entre le public et l'administration.

⁵⁷⁶ Article L.311-1 du code des relations entre le public et l'administration.

⁵⁷⁷ Article L.311-6 du code des relations entre le public et l'administration.

pour saisir la Commission d'accès aux documents administratifs (CADA)⁵⁷⁸. Cette commission est chargée de garantir l'effectivité de la liberté d'accès aux documents administratifs⁵⁷⁹. Toutefois, la CADA est habilitée à rendre des avis non contraignants. Cela signifie que l'autorité administrative détentrice du document litigieux est libre « *de déterminer la position qu'elle entend finalement retenir et d'en informer la commission* »⁵⁸⁰. En conséquence, l'établissement de santé peut outrepasser l'avis de la CADA et maintenir son refus de communication du dossier médical hospitalier. Le cas échéant, le patient peut élever le contentieux devant le juge administratif dans le cadre d'un recours pour excès de pouvoir. La saisine du juge administratif suppose, au préalable, une décision de refus de l'administration suivie d'un recours pour avis auprès de la CADA. En revanche, lorsque la demande de communication du dossier médical hospitalier porte sur des informations recueillies dans le cadre d'une admission en soins psychiatriques sans consentement, la saisine de la Commission départementale des hospitalisations psychiatriques (CDHP) se substitue à celle de la CADA⁵⁸¹. Contrairement à l'avis de la CADA, l'avis de la CDHP s'impose au détenteur des informations comme au demandeur.

192. En deuxième lieu, le patient qui désire accéder aux informations concernant sa santé peut fonder sa demande sur l'article 64 de la loi Informatique et Libertés modifiée. Ce dispositif légal permet à toute personne d'accéder directement à ses données médicales, dans les conditions de l'article L.1111-7 du code de la santé publique, quels que soient le secteur et les modalités de sa prise en charge sanitaire. L'application des dispositions de la loi Informatique et Libertés écarte donc les règles applicables à la communication des documents administratifs, quand bien même le patient serait hospitalisé dans un établissement public de santé⁵⁸². En effet, les établissements publics ou privés de santé et les professionnels de santé libéraux disposent, chacun, de la qualité de responsable de traitement des données médicales des personnes prises en charge. En cas de refus d'accès aux données médicales formalisées au sein de son dossier de soins, le patient dispose de voies de recours amiables et

⁵⁷⁸ Article R.343-1 du code des relations entre le public et l'administration.

⁵⁷⁹ Article L.340-1 du code des relations entre le public et l'administration.

⁵⁸⁰ LALLET (A.), NGUYEN DUY (P.), *Communication des documents administratifs*, *op. cit.* p. 88.

⁵⁸¹ CE, 10 avril 2009, n°289794, Rivoallan, Rec. Lebon, 2009, p. 752 ; RDSS, 2009, n° 04, p. 688, note F. Dieu ; RDS, 2009, n°30, p. 343, obs. F. Violla..

⁵⁸² CE, Ass., 19 mai 1983, n° 40680, *Bertin*, Rec. Lebon, 1983, p. 208 ; AJDA, 1983, p. 402, chron. Lasserre et Delarue.

juridictionnels⁵⁸³. D'abord, indépendamment de tout recours administratif ou juridictionnel, le patient dont les droits conférés par le RGPD et la loi Informatique et Libertés n'ont pas été respectés peut adresser une réclamation auprès de la CNIL⁵⁸⁴. Dans ce contexte, le président de la CNIL peut mettre le responsable de traitement en demeure de satisfaire à la demande de la personne concernée d'accéder aux données qui la concernent⁵⁸⁵. Toutefois, la CNIL demeure libre de clôturer ou de refuser de donner suite à la plainte formulée par le patient. Le cas échéant, le patient bénéficie du droit d'introduire un recours juridictionnel à l'encontre de la décision prise par la CNIL⁵⁸⁶ devant le Conseil d'Etat pendant un délai de 2 mois à compter de la notification de la décision⁵⁸⁷. Ensuite, le patient dont le droit d'accès aux données personnelles a été illicitement refusé peut former un recours juridictionnel à l'encontre de l'établissement ou du professionnel de santé responsable de traitement⁵⁸⁸. Autrement dit, le patient peut obtenir, devant les juridictions civiles et administratives, l'exécution de son droit d'accès aux données contenues dans ses dossiers médicaux, ainsi que l'indemnisation du préjudice subi consécutivement au refus opposé par le responsable de traitement. Le droit à un recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant a été introduit par le RGPD⁵⁸⁹. Céline Bloud-Rey semble néanmoins douter du succès de ce mécanisme. En effet, l'auteur présage qu'« *en pratique, la grande majorité des personnes concernées préféreront porter une réclamation auprès de la CNIL en raison de la gratuité du service et de la facilité à s'adresser à cette autorité plutôt que saisir la justice* »⁵⁹⁰.

193. Eu égard aux principes fondamentaux garantissant le droit d'accès direct aux données médicales du patient, aucune information relative à sa santé ne peut lui être dissimulée. Nous pouvons donc affirmer que le droit d'accès aux dossiers médicaux cristallise le *droit de savoir* octroyé au patient. En vertu de ce droit à la transparence, il n'est pas permis, pour le

⁵⁸³ Article 12 du RGPD.

⁵⁸⁴ Article 77 du RGPD.

⁵⁸⁵ Articles 20 II 1° et 21 de la loi Informatique et Libertés modifiée.

⁵⁸⁶ Article 78 du RGPD.

⁵⁸⁷ Conseil d'Etat, 28 mars 1997, n°18291.

⁵⁸⁸ Article 79 du RGPD.

⁵⁸⁹ *Ibid.*

⁵⁹⁰ BLOUD-REY (C.), *Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ?*, Recueil Dalloz, 2013, n°42, p.2798.

professionnel de santé, de cacher au patient des informations relatives à sa santé. Assurément, il n'existe aucun secret entre le professionnel de santé et le destinataire de l'information médicale. En ce sens, Fanny Vasseur-Lambry certifie que « *si le professionnel de santé est le débiteur de l'obligation de « garder le secret », le bénéficiaire de ce droit n'est autre que le malade à qui profite directement ce secret* »⁵⁹¹. En effet, le secret professionnel médical est institué, dans l'intérêt du patient, afin de garantir le droit au respect de sa vie privée contre toute atteinte⁵⁹². D'une certaine façon, la loi relative aux droits des malades a érigé le « secret médical » en un droit appartenant au patient et, corrélativement, en une obligation qui « *s'impose à tous les professionnels intervenant dans le système de santé* »⁵⁹³. Autrement dit, le patient partage ses informations médicales confidentielles avec les professionnels de santé qui n'en sont que les gardiens. Certainement, « *le professionnel de santé est dépositaire du secret. Les informations dont il est en possession ne lui appartiennent pas* »⁵⁹⁴. Dès lors, le professionnel de santé ne peut régulièrement faire obstacle au droit à l'information médicale en refusant la demande d'accès aux données médicales formulée par le patient.

194. C'est ainsi que la CNIL a prononcé une sanction pécuniaire d'un montant de 10 000 euros à l'encontre d'un cabinet dentaire qui refusa de répondre à la demande d'un patient d'accéder aux données à caractère personnel contenues dans son dossier médical. En défense, le cabinet dentaire a fait valoir « *qu'avant d'envoyer son dossier médical au plaignant, il s'était préalablement renseigné sur ses obligations déontologiques, notamment afin de s'assurer que les données contenues dans son dossier n'étaient pas couvertes par le secret médical* »⁵⁹⁵. La CNIL a alors considéré que « *le secret médical ne saurait s'opposer, en l'espèce, à la communication au patient des données le concernant et contenues dans son dossier médical* »⁵⁹⁶. Indéniablement, les données médicales formalisées au sein des dossiers médicaux constituent des données personnelles et confidentielles relatives au patient. A ce

⁵⁹¹ VASSEUR-LAMBRY (F.), *Le secret professionnel/médical : une protection forte dans l'intérêt du patient*, RGDM, 2018, n° 69, p. 102.

⁵⁹² KAYSER (P.), *La protection de la vie privée*, 3^e ed., PUAM, 1995, § 212.

⁵⁹³ Article L.1110-4 du code de la santé publique.

⁵⁹⁴ VASSEUR-LAMBRY (F.), *Le secret professionnel/médical : une protection forte dans l'intérêt du patient*, *op.cit.*, p. 100.

⁵⁹⁵ CNIL, Délibération de la formation restreinte SAN-2017-008 du 18 mai 2017 prononçant une sanction pécuniaire à l'encontre de la société d'exercice libéral à responsabilité limitée X.

⁵⁹⁶ *Ibid.*

titre, en tant que titulaire du secret médical, le patient bénéficie du droit d'y accéder sans que le caractère secret de ses informations intimes ne puisse lui être opposé. Ce dernier « *bénéficie même d'un véritable droit d'information sur toutes les informations médicales le concernant* »⁵⁹⁷. En tant que bénéficiaire de l'information médicale, seul le patient est, en principe, autorisé à exercer ce droit d'accès particulier.

195. Les dispositions de la loi Informatique et Libertés et du RGPD, les normes applicables aux relations entre le public et l'administration, ainsi que les dispositions de la loi relative aux droits des malades tendent à s'entremêler et se confondre. En effet, il convient de préciser que la personne prise médicalement en charge peut cumuler les statuts de patient, de personne concernée par le traitement de ses données médicales et, le cas échéant, d'usager du service public hospitalier. Afin de prévenir toute confusion, le droit d'accès aux données médicales du patient sera examiné conformément aux dispositions de l'article L.1111-7 du code de la santé publique. Autrement dit, le droit d'accès aux données médicales détenues par les établissements et les professionnels de santé sera davantage appréhendé sous le prisme universel des « droits du patient ». Néanmoins, il convient d'admettre que si le droit d'accès du patient à ses données médicales préexistait à l'entrée en vigueur du RGPD, ce règlement européen a considérablement renforcé cette accessibilité⁵⁹⁸. Désormais, le patient est systématiquement informé de l'existence de ce droit et de ses modalités d'exercice préalablement à la mise en œuvre du traitement de ses données à caractère personnel⁵⁹⁹. De surcroît, le droit d'accès aux données personnelles permet l'exercice des autres droits consacrés par le législateur européen. Le droit d'accès constitue donc la pierre angulaire de l'ensemble des droits octroyés à la personne concernée à l'égard de ses données personnelles. Après avoir obtenu la communication de ses informations médicales, le patient peut, le cas échéant, en demander la rectification⁶⁰⁰ ou l'effacement⁶⁰¹. Plus qu'un simple droit d'accès

⁵⁹⁷ SAINT MARTIN (A.), *Le secret médical et le patient (I) le patient (a priori) maître du secret professionnel médical*, RDS, 2010, n° 34, p. 109.

⁵⁹⁸ Alors que le droit à l'information des personnes concernées était déjà consacré par l'ancienne loi Informatique et Libertés, les responsables de traitement se sont effectivement assurés de l'information du patient quant à ses droits depuis l'entrée en vigueur du RGPD, lequel a initié le principe d'*accountability* défini comme « *l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données* » (définition proposée par la CNIL, disponible en ligne sur le site [<https://www.cnil.fr>], consulté le 17 mars 2021).

⁵⁹⁹ Article 13 du RGPD.

⁶⁰⁰ Cf. Paragraphes 137 à 142.

⁶⁰¹ Cf. Paragraphe 143 à 158.

à ses données médicales, le patient bénéficie effectivement d'un véritable droit de contrôle de ses informations intimes. Assurément, par définition, le contrôle consiste en une opération de vérification⁶⁰².

B) Les modalités d'accès aux données médicales consignées dans les dossiers médicaux

196. « *L'accès aux informations médicales est un droit personnel et direct que seul le patient est en droit d'exercer.* »⁶⁰³. En ces quelques mots, Virginie Rivière a exposé le principe selon lequel les données à caractère personnel ne sont accessibles et communicables qu'à l'intéressé. La demande d'accès aux informations médicales nominatives doit donc être adressée par la personne concernée au responsable de traitement : « *au professionnel de santé et, dans le cas d'un établissement de santé, au responsable de cet établissement* »⁶⁰⁴. Afin d'éviter toute violation de données personnelles, le destinataire de la demande d'accès au dossier médical hospitalier, ou à la fiche d'observation personnelle, doit s'assurer de l'identité de la personne concernée⁶⁰⁵. Dès lors, aucune demande d'accès ne peut être honorée sans certitude de l'identité du demandeur. Par suite, « *lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande* »⁶⁰⁶ d'accès aux informations médicales, le législateur européen invite le responsable de traitement à « *demande que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée* »⁶⁰⁷. Le responsable de traitement doit ainsi obtenir la confirmation que le patient est effectivement la personne concernée par les informations médicales relatives à sa santé. Dans l'hypothèse où le patient souhaite exercer son droit d'accès indirectement par l'intermédiaire d'un

⁶⁰² Définition du substantif masculin « contrôle » proposée par le CNRTL. Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 07 décembre 2021.

⁶⁰³ RIVIERE (V.), *Refus par un mineur de la communication de son dossier médical*, RDS, 2007, n°16, p. 245.

⁶⁰⁴ Article R.1111-1 du code de la santé publique.

⁶⁰⁵ *Ibid.*

⁶⁰⁶ Article 12.6 du RGPD.

⁶⁰⁷ *Ibid.*

médecin, le responsable de traitement doit également veiller à la qualité de médecin de la personne désignée comme intermédiaire⁶⁰⁸.

197. L'arrêté du 5 mars 2004⁶⁰⁹, portant sur les recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, autorise la communication des données médicales du patient à une personne qu'il a mandatée. Dès lors, le médecin désigné par le patient comme l'intermédiaire par lequel il souhaite obtenir la communication des informations le concernant a-t-il la qualité de mandataire ? En vertu de l'article 1984 du code civil, « *le mandat ou procuration est un acte par lequel une personne donne à une autre le pouvoir de faire quelque chose pour le mandant et en son nom* ». Le droit d'accès au dossier médical constitue un droit subjectif octroyé aux personnes concernées auxquelles son exercice appartient. Le législateur a offert la possibilité, aux personnes concernées, d'exercer ce droit indirectement par l'intermédiaire d'une tierce personne : le médecin. De cette façon, la personne concernée donne au médecin le pouvoir d'exercer son droit personnel d'accéder aux informations concernant sa santé. A cet égard, nous considérons que, dans le cadre d'un exercice indirect du droit d'accès, le médecin intervient en la qualité de mandataire. A cet instant, l'accès aux informations médicales du mandant ne peut lui être autorisé qu'à la condition qu'il « *dispose d'un mandat exprès et peut justifier de son identité* »⁶¹⁰. A défaut, toute personne justifiant uniquement de la qualité de médecin pourrait obtenir la communication de données médicales alors même qu'elle n'aurait été ni désignée, ni mandatée par la personne concernée. En outre, il convient de préciser que la personne concernée peut mandater toute personne pour exercer son droit d'accès à ses données médicales⁶¹¹, à condition que la personne mandatée n'ait pas de conflit d'intérêts et ne défende pas d'autres intérêts que ceux du mandant. En conséquence, l'accès aux informations médicales serait interdit aux compagnies d'assurance ou aux employeurs dépositaires d'un mandat valablement constitué.

⁶⁰⁸ Cf. Paragraphe 197.

⁶⁰⁹ Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, *loc. cit.*

⁶¹⁰ *Ibid.*

⁶¹¹ CE, 26 sept. 2005 n°270234, AJDA, 2006, n° 06, p. 308, note J.-P. Markus.

198. Au choix de la personne concernée, il existe deux modalités d'accès direct aux données médicales formalisées au sein de son dossier de soins. Premièrement, l'intéressé peut demander à consulter son dossier de soins en se rendant dans la structure sanitaire ou au cabinet du professionnel de santé qui l'a constitué. L'original de son dossier de soins doit alors être mis à sa disposition. Lorsque les données médicales du patient sont formalisées au sein d'un fichier informatisé, un exemplaire au format papier doit être imprimé. Dans le cas où le dossier informatisé est détenu par un établissement de santé, « *et si les dispositifs techniques de l'établissement le permettent, le demandeur peut également consulter [son dossier de soins] par voie électronique* »⁶¹². Secondement, l'intéressé peut en demander la délivrance d'une copie. Cette copie peut être remise en mains propres consécutivement à la consultation sur place, ou être envoyée à la personne concernée. Selon la volonté de l'intéressé, et dans les limites des possibilités techniques, « *les copies sont établies sur un support analogue à celui utilisé par le professionnel de santé ou l'établissement de santé, ou sur papier* »⁶¹³. Nous comprenons que si la personne concernée opte pour une copie de son dossier de soins sur papier, le responsable de traitement doit lui remettre en mains propres ou lui transmettre par envoi postal. Le cas échéant, les frais de reproduction et d'envoi peuvent être laissés à la charge du demandeur⁶¹⁴. Par ailleurs, si le dossier de soins est un fichier informatisé, nous déduisons que la copie peut être délivrée sur un support numérique ou par courrier électronique. En ce sens, les dispositions du RGPD⁶¹⁵ et du code des relations entre le public et l'administration⁶¹⁶ prévoient que le demandeur du droit d'accès à ses données personnelles peut demander à ce qu'elles lui soient fournies gratuitement par voie électronique. Seulement, les données médicales étant singulièrement sensibles et particulièrement exposées à des risques de piratage, est-il envisageable de communiquer un dossier de soins par messagerie électronique ?

⁶¹² Article R.1111-2 du code de la santé publique.

⁶¹³ *Ibid.*

⁶¹⁴ Article L.1111-7 alinéa 7 du code de la santé publique.

⁶¹⁵ Article 12.3 du RGPD.

⁶¹⁶ Article L.311-9 du code des relations entre le public et l'administration.

La CNIL considère que ce mode de communication ne constitue pas « *un moyen de communication sûr pour transmettre des données médicales nominatives* »⁶¹⁷. L'autorité administrative explique qu'« *une simple erreur de manipulation [...] peut conduire à divulguer à des destinataires non habilités des informations couvertes par le secret médical et à porter ainsi gravement atteinte à l'intimité de la vie privée des personnes* »⁶¹⁸. Partant, la CNIL recommande de « *recourir à une messagerie sécurisée intégrant un module de chiffrement des données [médicales]* »⁶¹⁹. Alors que les professionnels de santé devraient systématiquement utiliser des messageries sécurisées de santé telle que MSSanté⁶²⁰, les particuliers disposent majoritairement de boîtes mail non sécurisées et dont le service est généralement proposé par les GAFAM. A moins que le patient ne dispose d'un Espace numérique de santé auquel est intégrée une messagerie sécurisée pour communiquer avec les professionnels de santé⁶²¹, il convient de privilégier l'envoi de la copie du dossier de soins par lettre recommandée avec accusé de réception en mentionnant le caractère confidentiel du courrier.

199. Toutefois, si le demandeur ne précise pas les modalités d'exercice de son droit d'accès, le responsable de traitement doit l'informer des différentes possibilités de communication du dossier de soins et lui indiquer celles « *qui seront utilisées à défaut de choix de sa part* »⁶²² au terme des délais prescrits par le code de la santé publique. En effet, l'absence de choix quant au mode d'exercice du droit d'accès aux données médicales ne dispense pas le responsable de traitement de satisfaire à cette demande. Par conséquent, le responsable de traitement doit obligatoirement communiquer le dossier de soins du patient dans les huit jours à compter de la réception de la demande. Lorsque les informations demandées datent de plus de cinq ans à compter de leur constitution, ou lorsque la

⁶¹⁷ CNIL, *Données de santé, messagerie électronique et fax*, 01 décembre 2015. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 03 septembre 2020.

⁶¹⁸ *Ibid.*

⁶¹⁹ *Ibid.*

⁶²⁰ Selon l'ANS, « *MSSanté est un espace de confiance au sein duquel les professionnels habilités à échanger des données de santé, en ville comme à l'hôpital, peuvent s'échanger par mail des données de santé de manière dématérialisée en toute sécurité.* ».

⁶²¹ Article L.1111-13-1 II 5° du code de la santé publique.

⁶²² Article R.1111-3 du code de la santé publique.

communication départementale des soins psychiatriques est saisie, le législateur a porté ce délai à deux mois⁶²³.

Dans un référentiel publié en juillet 2020, la CNIL préconise de conserver les dossiers de soins « *en base active, pendant une durée de cinq ans à compter de la dernière intervention sur le dossier du patient, puis, à l'issue de cette période, sous la forme archivée sur un support distinct [du dossier actif] pendant quinze ans* »⁶²⁴. En raison de leur archivage, les dossiers de soins datant de plus de cinq ans à compter de leur constitution ne sont plus immédiatement disponibles et accessibles ni au professionnel de santé, ni à la personne concernée. Compte tenu de la complexité de la demande, le législateur européen admet également que la communication des données personnelles puisse exceptionnellement être prorogée⁶²⁵. La prolongation du délai de communication des données médicales semble alors justifiée par les difficultés à extraire des données archivées, notamment lorsque leur conservation est externalisée auprès d'un hébergeur tiers et constitue une activité d'hébergement au sens des dispositions de l'article R.1111-9 du code de la santé publique. Le cas échéant, la personne concernée peut-elle exercer son droit d'accès directement auprès de l'hébergeur de données de santé ?

200. Il ressort des dispositions du code de la santé publique que seul le responsable de traitement pour le compte duquel les données produites à l'occasion d'un acte de prévention, de diagnostic ou de soins ont été hébergées peut y accéder. Ainsi, lorsque l'hébergeur de données de santé conserve des dossiers de soins pour le compte d'un établissement ou d'un professionnel de santé, le patient ne peut directement y accéder. Les dispositions de l'article L.1111-8 du code de la santé publique explicitent que « *l'accès aux données ayant fait l'objet d'un hébergement s'effectue selon les modalités fixées dans le contrat [d'hébergement conclu entre l'hébergeur et le responsable de traitement] dans le respect des articles L. 1110-4 et L. 1111-7* » du même code. Autrement dit, lorsque les données médicales du patient ont fait l'objet d'un hébergement, ce dernier ne peut exercer son droit d'accès qu'auprès du responsable de traitement à l'origine de la constitution de son dossier de soins, conformément aux modalités décrites ci-avant. Il en résulte que le patient ne peut accéder à son dossier de

⁶²³ Article L.1111-7 al. 2 du code de la santé publique.

⁶²⁴ CNIL, Délibération n°2020-081 du 18 juin 2020, *loc. cit.*

⁶²⁵ Article 12.3 du RGPD.

soins hébergé, sur support électronique comme sur support papier, que par l'intermédiaire du responsable de traitement déposant.

201. De la même manière que pour les dossiers médicaux hospitaliers et les fiches d'observation personnelles, l'accès aux données médicales formalisées au sein du DMP n'est, sauf exception, réservé qu'au titulaire de ce dispositif⁶²⁶. Conformément au droit d'accès aux informations médicales instauré à l'article L.1111-7 du code de la santé publique, le titulaire du DMP dispose d'un droit d'accès direct aux données qu'il contient et peut procéder à leur extraction⁶²⁷. Son accès direct se fait « *par voie électronique depuis son espace numérique de santé* »⁶²⁸ auquel il se connecte par des moyens d'identification et d'authentification conformes aux référentiels élaborés par l'Agence du numérique en santé (ANS)⁶²⁹. Dans l'hypothèse où le titulaire du DMP ne bénéficie pas d'une connexion à l'Internet, il peut exercer son droit d'accès aux données médicales qu'il contient « *par l'intermédiaire de l'organisme d'assurance maladie auquel il est rattaché* »⁶³⁰. Quelle que soit la modalité de l'accès au DMP, l'identification de la personne concernée est vérifiée. Ainsi, la préservation de la confidentialité des informations communiquées semble raisonnablement protégée.

202. Si le principe veut que le droit d'accès aux données médicales soit exercé par la personne concernée, cela suppose qu'elle en soit juridiquement capable. La capacité juridique peut être définie comme l'aptitude à être titulaire de droits subjectifs et à les exercer. Seulement, bien qu'ils jouissent de la personnalité juridique, le code civil précise que les mineurs non émancipés et les majeurs protégés sont frappés d'une incapacité d'exercice⁶³¹. Cela signifie que, pour exercer ses droits, le mineur non émancipé doit être représenté par les titulaires de l'autorité parentale ou par son tuteur, et le majeur protégé doit être assisté ou représenté par son représentant légal. Dès lors, le patient juridiquement incapable peut-il accéder directement à ses données médicales contenues dans son dossier médical ?

⁶²⁶ Article L.1111-19 du code de la santé publique.

⁶²⁷ Article R.1111-45 du code de la santé publique.

⁶²⁸ Article R.1111-45 du code de la santé publique.

⁶²⁹ Article R.1111-32 alinéa 1 du code de la santé publique.

⁶³⁰ Article R.1111-35 alinéa 1 du code de la santé publique.

⁶³¹ Article 1146 du code civil.

Paragraphe 2 : L'exercice du droit d'accès de la personne juridiquement incapable

203. Tandis que l'autodétermination informationnelle du majeur protégé a été augmentée par le législateur, celle accordée au mineur non émancipé demeure relative. En effet, le majeur faisant l'objet d'une mesure de protection juridique avec assistance ou représentation jouit d'un droit d'accès direct aux données médicales formalisées dans ses dossiers médicaux (B). A l'inverse, le mineur ne peut jamais y accéder que par l'intermédiaire de ses représentants légaux (A).

A) *L'accès indirect aux données médicales du mineur*

204. Les dispositions de l'article L.1111-7 du code de la santé publique explicitent que « *le droit d'accès [aux informations concernant la santé du mineur] est exercé par le ou les titulaires de l'autorité parentale* ». En effet, lorsque le patient est mineur, les droits qui lui sont accordés par la loi du 4 mars 2002⁶³² sont exercés par les personnes titulaires de l'autorité parentale. Depuis son entrée en vigueur, « *le code de la santé publique permet aux titulaires de l'autorité parentale de bénéficier d'un droit à l'information concernant la santé de leur enfant ainsi que d'un droit d'accès à cette information, aujourd'hui formalisée dans le dossier médical* »⁶³³. Il s'ensuit que les titulaires de l'autorité parentale reçoivent l'information médicale, *a priori*⁶³⁴ comme *a posteriori*, de façon à pouvoir consentir aux décisions concernant la santé de leur enfant non émancipé. Néanmoins, quel que soit l'âge du mineur, les professionnels de santé ont l'obligation de lui délivrer une information adaptée à son degré de maturité⁶³⁵. Bien que le mineur soit destinataire de l'information médicale, il n'en demeure pas moins que « *seul le mineur émancipé accède seul à son dossier, pour les autres, les titulaires de l'autorité parentale sont les seuls à disposer du droit d'accès* »⁶³⁶. Compte tenu de ce qui précède, seule l'investiture de l'autorité parentale constitue une condition *sine qua non* au droit d'accès aux données médicales du mineur. En ce sens, la

⁶³² Loi n° 2002-303 du 4 mars 2002, *op. cit.*

⁶³³ RIVIERE (V.), *Refus par un mineur de la communication de son dossier médical*, *loc. cit.*

⁶³⁴ Article L.1111-2 II du code de la santé publique.

⁶³⁵ *Ibid.*

⁶³⁶ NICOLAS (G.), *L'accès au dossier hospitalier par le patient et sa famille : les cas particuliers (patient mineurs, majeurs protégés, patients décédés)*, RGDM, 2010, n°37, p. 189.

CADA affirme que « *le parent qui ne dispose plus de l'exercice de l'autorité parentale demeure titulaire de celle-ci au sens des dispositions de l'article L1111-7 du code de la santé publique* »⁶³⁷. Par conséquent « *seul le parent qui s'est vu retirer cette autorité en application des articles 378 et 378-1 du code civil doit être regardé comme étant privé de l'autorité parentale et, par conséquent, du droit d'obtenir la communication des informations médicales relatives à son enfant mineur* »⁶³⁸. La perte de l'exercice de l'autorité parentale, et non de sa détention, est sans incidence sur le droit d'accès aux données médicales du mineur.

205. L'exercice du droit d'accès aux données médicales du mineur ne pose pas de difficulté lorsqu'un seul parent est investi de l'autorité parentale. Le cas échéant, ce droit est exercé par cet unique parent. Cependant, lorsque les deux parents sont détenteurs de l'autorité parentale, un seul des parents peut-il demander l'accès aux données médicales du mineur ? Dans une décision relative à l'accès au dossier médical d'un mineur par l'un des titulaires de l'autorité parentale, le défenseur des droits a spécifié que « *chacun des titulaires exerce son droit indépendamment de l'autre. [...] Dans ce cadre, Monsieur X peut accéder aux éléments du dossier médical de sa fille sans avoir à obtenir la signature de la mère de son enfant* »⁶³⁹. Concrètement, tout parent détenteur de l'autorité parentale peut exercer seul le droit d'accès aux données médicales formalisées dans le dossier de soins de son enfant. Le droit d'accès aux données médicales du mineur peut être considéré comme un acte usuel⁶⁴⁰ pouvant être exercé par l'un des deux détenteurs de l'autorité parentale. Si l'un des deux titulaires de l'autorité parentale a le droit de recevoir seul l'information médicale délivrée *a priori* par le professionnel de santé, il peut également accéder à cette information formalisée *a posteriori* dans le dossier de soins du mineur. Ainsi, chaque titulaire de l'autorité parentale bénéficie d'un droit d'accès aux données médicales du mineur qui lui est strictement personnel.

206. Tandis que le législateur réserve l'exercice du droit d'accès aux données médicales du mineur aux titulaires de l'autorité parentale, qu'en est-il lorsqu'il ne reste ni père ni mère en état de l'exercer ? L'exercice de ce droit d'accès peut-il être dévolu au tuteur du

⁶³⁷ CADA, avis, 18 septembre 2014, n°20142924.

⁶³⁸ *Ibid.*

⁶³⁹ Défenseur des droits, 3 novembre 2017, n°2017-290.

⁶⁴⁰ En vertu de l'article 372-2 du code civil, « *chacun des parents est réputé agir avec l'accord de l'autre, quand il fait seul un acte usuel de l'autorité parentale relativement à la personne de l'enfant.* ».

mineur placé sous tutelle⁶⁴¹ ? Les dispositions de l'article L.1111-2 du code de la santé publique énoncent que le droit à l'information médicale peut être exercé par le tuteur du mineur. Si le tuteur du mineur est destinataire de l'information médicale *a priori*, ne pourrait-il pas accéder aux données médicales formalisées *a posteriori* dans ses dossiers médicaux ? Il en ressort que le secret protégeant les informations médicales relatives au mineur n'est pas opposable au tuteur. De plus, en vertu de l'article 408 du code civil « *le tuteur prend soin de la personne du mineur et le représente dans tous les actes de la vie civile, sauf les cas dans lesquels la loi ou l'usage autorise le mineur à agir lui-même* ». Etant donné que le mineur n'est pas légalement autorisé à obtenir la communication de ses données médicales, il apparaît que le droit d'accès à son dossier de soins ne peut être exercé que par son tuteur.

207. Compte tenu de ce qui précède, le droit d'accès aux données médicales du mineur ne peut être exercé que par les titulaires de l'autorité parentale ou par le tuteur. En d'autres termes, le mineur ne peut directement exercer ce droit. Néanmoins, le législateur lui a octroyé une modeste autodétermination informationnelle sur les éléments immatériels de son corps humain formalisés dans son dossier de soins⁶⁴². En premier lieu, le mineur peut demander au responsable de traitement que ses représentants légaux n'y accèdent que par l'intermédiaire d'un médecin⁶⁴³. Alors que le mineur ne peut accéder à ses dossiers médicaux que par l'intermédiaire de ses représentants légaux, « *la loi lui reconnaît le droit de demander la médiation d'un médecin* »⁶⁴⁴. Ainsi, le mineur peut assister à la communication de ses données médicales, *a fortiori* lorsqu'elle intervient indirectement au moyen d'un professionnel médical. Certainement, le mineur bénéficie du droit de recevoir l'information médicale délivrée par les professionnels de santé.

⁶⁴¹ En vertu de l'article 373-5 du code civil, « *s'il ne reste plus ni père ni mère en état d'exercer l'autorité parentale, il y aura lieu à l'ouverture d'une tutelle ainsi qu'il est dit à l'article 390 ci-dessous.* ».

⁶⁴² Voir : DUJARDIN (V.), *La personne mineure*, LEH, 2005.

⁶⁴³ Article L.1111-7 alinéa 5 du code de la santé publique : « *A la demande du mineur, cet accès a lieu par l'intermédiaire d'un médecin.* ».

⁶⁴⁴ NICOLAS (G.), *L'accès au dossier hospitalier par le patient et sa famille : les cas particuliers (patient mineurs, majeurs protégés, patients décédés)*, *op. cit.*, p. 189.

208. En deuxième lieu, le mineur peut s'opposer à ce que ses représentants légaux accèdent à ses données médicales lorsque les soins lui ont été prodigués à leur insu⁶⁴⁵. Par la loi du 4 mars 2002, le législateur a généralement reconnu le droit au secret médical au profit du mineur qui le revendique. Depuis, le mineur a droit à des soins confidentiels, sans que ses représentants légaux n'en soient informés et sans que leur consentement ne soit requis⁶⁴⁶. La préservation du secret vis-à-vis des représentants légaux d'un mineur est indispensable à la sauvegarde de la confiance entre ce dernier et le professionnel de santé. Pilier de la relation médicale, « *il n'y a pas de médecine sans confiance, de confiance sans confiance, de confiance sans secret* »⁶⁴⁷. L'instauration de la confiance à travers le secret professionnel médical est davantage essentielle lorsque le patient est une personne mineure en phase d'adolescence. Forte de son expérience de pédiatre, Caroline Rey-Salmon déclare que « *les mineurs qui réclament ces soins confidentiels peuvent souffrir de mauvaises relations avec leurs parents. La revendication de la confidentialité peut alors traduire des conflits, notamment sur des convictions morales ou religieuses ; elle peut aussi renvoyer à la peur de la réprobation par rapport à certaines conduites, particulièrement en matière de sexualité ou de consommations de produits. Mais, pour un certain nombre d'adolescents, cette revendication renvoie à un réel désir d'intimité.* »⁶⁴⁸. Si le secret n'était pas garanti au mineur, celui-ci pourrait renoncer à consulter par crainte que ses données médicales ne soient révélées.

209. Par suite, l'article R.1111-6 du code de la santé publique dispose que le mineur qui souhaite garder le secret vis-à-vis de ses représentants légaux peut s'opposer à ce qu'ils accèdent à ses données médicales générées dans ce contexte. Afin de ne commettre aucun impair, cette opposition doit être expressément consignée au sein du dossier médical hospitalier ou de la fiche d'observation personnelle constitué pour le mineur⁶⁴⁹. Cette

⁶⁴⁵ DEKEUWER-DEFOSSEZ (F.), *L'autorité parentale à l'épreuve de la loi Kouchner*, RGDM, 2004, n° 12, p. 101 à p. 102 ; KIMMEL-ALCOVER (A.), *L'autorité parentale à l'épreuve de la santé des mineurs: chronique d'un déclin annoncé*, RDSS, 2005, n° 02 p. 265 ; VIALLA (F.), FAURE (M.), MARTINEZ (E.), BOURRET (R.), VAUTHIER (J.-P.), *Mineur et secret médical – Le secret sur son état de santé demandé par le mineur à l'égard de ses parents : de la reconnaissance d'un droit à sa mise en œuvre concrète*, Médecine & Droit, 2015, n° 133, p. 79 à p. 104.

⁶⁴⁶ Articles L.1111-5 et L.1111-5-1 du code de la santé publique.

⁶⁴⁷ PORTES (L.), *À la recherche d'une éthique médicale*, Paris, Masson & Cie, 1964, p. 153.

⁶⁴⁸ REY-SALMON (C.), *Secret médical et personnes vulnérables : le cas du mineur*, Recueil Dalloz, 2009, n°39, p. 2651.

⁶⁴⁹ *Ibid.*

opposition peut concerner les deux titulaires de l'autorité parentale ou l'un des deux. En effet, la CADA a admis que « *l'opposition expresse et écrite d'un mineur empêche la communication du dossier au père* »⁶⁵⁰ alors que le mineur n'a pas souhaité opposer le secret à la mère. En conséquence, le responsable de traitement doit consciencieusement vérifier qu'aucune mention selon laquelle le mineur s'oppose à la communication de ses éléments immatériels du corps humain ne soit apposée en marge de son dossier de soins. Le cas échéant, le responsable de traitement doit s'assurer du périmètre de l'opposition ou de la limitation sollicitée par le mineur. De cette façon, le responsable de traitement veillera à ne pas divulguer les données médicales générées à l'occasion d'un acte dispensé dans le secret.

210. A l'instar de l'accès aux informations médicales détenues par les professionnels et les établissements de santé, le droit d'accès au DMP est exercé par les titulaires de l'autorité parentale ou le tuteur du mineur⁶⁵¹. Leur liberté d'accès aux données médicales du mineur *via* le portail du DMP a posé des difficultés jusqu'à l'intervention du législateur à l'occasion de la loi relative à l'organisation et à la transformation du système de santé⁶⁵². Avant le 1^{er} janvier 2022⁶⁵³, la volonté du mineur de garder le secret sur son état de santé, et de s'opposer à la communication de ses informations médicales à ses représentants légaux, n'était pas prise en compte dans le cadre du DMP. En effet, les professionnels de santé avaient l'obligation d'alimenter le DMP à l'occasion de tout acte médical ou soignant et, conséquemment, d'y transposer les informations médicales couvertes par ce secret sans que la mention du refus du mineur ne puisse être apposée.

Désormais, « *la personne mineure qui souhaite garder le secret sur toute donnée relative à l'un des actes [prodigués dans le secret] est informée par le professionnel qui la prend en charge de son droit de s'opposer à la mention de ces données dans un ou plusieurs des éléments figurant dans son espace numérique de santé* »⁶⁵⁴. Il en advient que le mineur ayant bénéficié d'actes délivrés en toute confidentialité peut demander à ce que les données médicales collectées à cette occasion ne soient pas renseignées dans son DMP. Plus

⁶⁵⁰ CADA, avis, 25 août 2005, n°20053225.

⁶⁵¹ Article R.1111-40 alinéa 5 du code de la santé publique.

⁶⁵² Article 45 de la loi n°2019-774 du 24 juillet 2019, *loc. cit.*

⁶⁵³ Date d'entrée en vigueur des dispositions de l'article 45 de la loi n°2019-774 du 24 juillet 2019.

⁶⁵⁴ Article R.1111-33 du code de la santé publique.

précisément, les dispositions réglementaires relatives au DMP énoncent que « *sans préjudice des dispositions de l'article R. 1111-33 [du code de la santé publique], lorsque le titulaire est une personne mineure, il peut demander au professionnel ou à l'établissement de santé qui alimente son dossier médical partagé que les données relatives à l'un des actes [prodigués dans le secret] ne puissent être consultées par son représentant légal* »⁶⁵⁵. Faut-il ici comprendre que le mineur ayant reçu des actes sanitaires à l'insu de ses représentants légaux dispose d'une option entre l'absence d'alimentation de son DMP ou le masquage de ses données médicales ?

L'opportunité de ce choix, dont l'enjeu réside dans la traçabilité de l'histoire médicale du patient, semble appartenir au mineur. En effet, il existe des informations médicales, générées dans un contexte particulier, que le patient devenu majeur ne souhaiterait pas se remémorer tout au long de sa vie par leur inscription dans son DMP. En tout état de cause, lorsque la personne mineure a exprimé la volonté de garder le secret sur son état de santé à l'égard de ses représentants légaux, « *l'organisme d'assurance maladie auquel elle est rattachée ne transfère pas dans son espace numérique de santé les données relatives au remboursement de ces actes et des produits de santé prescrits à l'occasion de ces actes* »⁶⁵⁶. Dans le cas contraire, l'inscription du libellé de l'acte remboursé par l'Assurance maladie dans son DMP aurait pour effet de révéler, aux représentants légaux du patient mineur, la nature de la prestation sanitaire dispensée à leur insu.

211. Au demeurant, Virginie Rivière considère que ce droit à la confidentialité des soins et des informations médicales relatives au patient mineur constitue un « *paradoxe* »⁶⁵⁷. L'auteur constate qu'« *aujourd'hui, le mineur dispose de la faculté de limiter l'accès à son dossier médical, mais ne dispose pas pour autant d'un droit d'accès direct à son dossier médical* »⁶⁵⁸. D'une certaine façon, nous pouvons conclure que le mineur dispose d'une maîtrise modérée de ses données médicales confidentielles. En effet, les représentants légaux exercent les droits du patient mineur concerné par le traitement de ses données médicales⁶⁵⁹.

⁶⁵⁵ Article R.1111-50 du code de la santé publique.

⁶⁵⁶ Article R.1111-33 du code de la santé publique.

⁶⁵⁷ RIVIERE (V.), *Refus par un mineur de la communication de son dossier médical*, op. cit., p. 247.

⁶⁵⁸ *Ibid.*

⁶⁵⁹ Article 70 de la loi Informatique et Libertés modifiée.

B) L'accès direct aux données médicales du majeur protégé

212. Une personne majeure peut faire l'objet d'une mesure de protection dès lors qu'elle se trouve « *dans l'impossibilité de pourvoir seule à ses intérêts en raison d'une altération, médicalement constatée, soit de ses facultés mentales, soit de ses facultés corporelles de nature à empêcher l'expression de sa volonté* »⁶⁶⁰. La mesure de protection juridique ordonnée par le juge doit être proportionnée et individualisée en fonction du degré d'altération des facultés de l'intéressé. C'est pourquoi il existe trois mesures de protection juridique qui se distinguent selon leur degré d'assistance ou de représentation. L'identification de la mesure de protection permet de déterminer qui du majeur protégé ou de son protecteur exercera le droit d'accès aux données médicales.

Premièrement, le majeur vulnérable peut être placé sous sauvegarde de justice⁶⁶¹. Il s'agit d'une protection temporaire⁶⁶² pendant laquelle la personne conserve le plein exercice de ses droits et de ses prérogatives⁶⁶³. Simplement, les actes passés pendant la durée de la mesure de sauvegarde pourront être rescindés, réduits ou annulés selon les circonstances dans lesquelles ils auront été contractés⁶⁶⁴. Ainsi, le patient placé sous sauvegarde de justice exerce seul le droit d'accéder à ses dossiers médicaux. Deuxièmement, le majeur vulnérable peut être placé sous curatelle⁶⁶⁵. La curatelle est une mesure de conseil et de contrôle par laquelle la personne protégée se fait assister par un curateur dans les actes importants de la vie civile. Néanmoins, le majeur placé sous curatelle conserve sa capacité juridique et prend seul les décisions concernant sa personne dans la mesure où son état le permet⁶⁶⁶. Dans le cas contraire, le juge peut prévoir que le majeur placé sous curatelle recevra l'assistance d'un curateur pour les actes relatifs à sa personne. La curatelle correspond donc à une mesure de protection juridique avec assistance. Troisièmement, le majeur vulnérable peut être placé

⁶⁶⁰ Article 425 du code civil.

⁶⁶¹ Voir : LOISEAU (G.), *Le droit des personnes, op. cit.*, p. 58 à p. 60.

⁶⁶² Article 439 du code civil.

⁶⁶³ Article 435 du code civil.

⁶⁶⁴ *Ibid.*

⁶⁶⁵ LOISEAU (G.), *Le droit des personnes, op. cit.*, p. 57.

⁶⁶⁶ Article 440 du code civil.

sous tutelle⁶⁶⁷. La tutelle constitue une mesure de protection juridique avec représentation, par laquelle le majeur est représenté par son tuteur, de manière continue, dans les actes de la vie civile⁶⁶⁸. Le majeur sous tutelle ne peut donc agir seul. Toutefois, le juge peut prévoir que la représentation du majeur sous tutelle est nécessaire pour l'ensemble des actes touchant à sa personne, pour seulement certains d'entre eux, ou pour une série d'actes énumérés dans la décision de mise sous tutelle.

213. Depuis 2007⁶⁶⁹, le législateur a accordé davantage d'autonomie aux majeurs protégés. Dans ce prolongement, la loi de programmation et de réforme de la justice⁶⁷⁰ a considérablement affermi les droits fondamentaux des majeurs protégés. Seulement, les dispositions du code de la santé publique, qui encadrent le droit d'accès aux informations médicales formalisées dans le dossier de soins du majeur protégé, étaient dérogatoires au droit commun de la protection des personnes prescrit par le code civil. Alors que le régime général du code civil accordait plus d'autonomie aux personnes protégées, les règles du code de la santé publique leur accordaient davantage de protection. En conséquence, le patient juridiquement protégé ne pouvait exercer le droit d'accès à ses dossiers médicaux, lesquels étaient exclusivement communicables à l'organe en charge de sa protection. Afin d'harmoniser les textes traitant de la protection des majeurs, l'ordonnance du 11 mars 2020⁶⁷¹ a coordonné les « *dispositions du code de la santé publique qui font référence aux personnes protégées avec les règles du code civil* »⁶⁷². Désormais, le degré de la mesure de protection n'a plus aucune incidence sur l'exercice du droit d'accès direct du patient à ses données médicales détenues par les établissements et les professionnels de santé. Le majeur faisant l'objet d'une mesure d'assistance telle que la curatelle ou d'une mesure de représentation

⁶⁶⁷ LOISEAU (G.), *Le droit des personnes, op. cit.*, p. 56.

⁶⁶⁸ Article 459 du code civil.

⁶⁶⁹ Loi n°2007-308 du 5 mars 2007 portant réforme de la protection juridique des majeurs, *JORF* n°56, 7 mars 2007, texte n° 12.

⁶⁷⁰ Loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, *JORF* n°71, 24 mars 2019, texte n°2.

⁶⁷¹ Ordonnance n° 2020-232 du 11 mars 2020 relative au régime des décisions prises en matière de santé, de prise en charge ou d'accompagnement social ou médico-social à l'égard des personnes majeures faisant l'objet d'une mesure de protection juridique, *JORF* n°6, 12 mars 2020, texte n° 3.

⁶⁷² Rapport au Président de la République relatif à l'ordonnance n° 2020-232 du 11 mars 2020 relative au régime des décisions prises en matière de santé, de prise en charge ou d'accompagnement social ou médico-social à l'égard des personnes majeures faisant l'objet d'une mesure de protection juridique, *JORF* n°61, 12 mars 2020, texte n° 2.

telle que la tutelle bénéficie donc du droit d'accéder directement à son dossier de soins. Le renforcement du droit à l'information *a priori* comme *a posteriori* du majeur protégé tend à affirmer son droit à l'autodétermination informationnelle. En effet, son incapacité juridique ne peut le déposséder du droit de prendre connaissance de ses informations personnelles, *a fortiori* lorsqu'elles touchent au plus profond de son intimité.

214. En revanche, le degré de la mesure de protection retentit sur l'accès aux données médicales du majeur par l'organe en charge de sa protection. En effet, les dispositions de l'article L.1111-7 du code de la santé publique opèrent une distinction entre les mesures de protection avec assistance et celles avec représentation.

215. Le législateur explicite que dans le cas où « *la personne majeure fait l'objet d'une mesure de protection juridique avec assistance, la personne chargée de l'assistance peut accéder à ces informations avec le consentement exprès de la personne protégée* »⁶⁷³. Par principe, le patient faisant l'objet d'une mesure d'assistance conserve la confidentialité de son état de santé à l'égard de la personne chargée de l'assister. A l'instar de l'information médicale, l'accès du curateur aux éléments immatériels du corps humain du patient lui est permis à titre exceptionnel : lorsque le patient protégé l'y autorise expressément. Autrement dit, le curateur n'étant pas destinataire de l'information médicale, il ne peut bénéficier du droit – corollaire – d'accéder aux informations médicales du majeur protégé. Le patient faisant l'objet d'une mesure d'assistance peut donc autoriser son curateur à accéder directement aux données médicales qui le concernent, *a priori* comme *a posteriori*. Le consentement du patient protégé à la révélation des informations médicales le concernant délie le professionnel de santé de l'obligation de secret qui lui incombe. D'une certaine façon, ce consentement exprès à la communication de ses données médicales correspond au mandat que le patient est autorisé à donner à toute personne bienveillante à son égard⁶⁷⁴. A l'exclusion de l'hypothèse où elle est expressément mandatée à cet effet, la personne chargée de l'assistance du patient ne peut revendiquer aucun droit d'accès aux données médicales relatives à la personne qu'elle assiste.

⁶⁷³ Article L.1111-7 alinéa 2 du code de la santé publique.

⁶⁷⁴ Cf. Paragraphe 197.

216. A l'opposé, le droit à l'information médicale ainsi que le droit d'accéder aux données de la personne faisant l'objet d'une mesure de représentation sont dus à son représentant légal. Effectivement, « *lorsque la personne majeure fait l'objet d'une mesure de protection juridique avec représentation relative à la personne, la personne en charge de la mesure a accès à ces informations* »⁶⁷⁵ dans les mêmes conditions que le patient lui-même. Lorsque le patient fait l'objet d'une mesure de représentation, son représentant légal peut exercer le droit d'accès à ses données médicales sans qu'il ne puisse s'y opposer. Quelle que soit la catégorie de l'acte dispensé au patient représenté juridiquement, il ne subsiste aucun secret entre le représentant légal et la personne protégée, quand bien même elle souhaiterait garder le secret sur son état de santé. Bien que cette transparence absolue puisse sembler attentatoire à la vie privée du patient représenté, elle apparaît néanmoins primordiale. Si la personne en charge de la représentation du patient est destinataire de l'information médicale⁶⁷⁶, c'est afin de consentir, de façon éclairée, aux décisions médicales la concernant⁶⁷⁷.

217. Alors que les majeurs protégés peuvent directement accéder à leur dossier de soins, jouissent-ils d'un accès direct à leur DMP ? Le contenu de ces deux catégories de dossiers médicaux est sensiblement identique⁶⁷⁸. En effet, le DMP doit être alimenté par tous les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins générés, par les professionnels de santé, à l'occasion de chaque acte ou consultation sanitaire. Ces mêmes éléments doivent également être formalisés dans le dossier de soins du patient. En effet, le professionnel de santé a l'obligation de consigner les informations médicales dont il a connaissance dans le dossier de soins du patient. A défaut, ce manquement est constitutif d'une faute dans l'organisation du service pouvant engager la responsabilité du professionnel ou de l'établissement de santé⁶⁷⁹. Ainsi, toute donnée médicale relative au patient, produite à l'occasion de sa prise en charge sanitaire, doit être formalisée dans son dossier de soins. Tandis que le dossier de soins s'avère plus riche que le DMP, toute donnée médicale colligée dans le DMP semble nécessairement apparaître dans le dossier de soins du patient. Dès lors, il serait incohérent que le majeur protégé ne puisse directement accéder à son DMP alors

⁶⁷⁵ Article L.1111-7 al.2 du code de la santé publique.

⁶⁷⁶ Article L.1111-2 III du code de la santé publique.

⁶⁷⁷ Article L.1111-4 al. 8 du code de la santé publique.

⁶⁷⁸ Cf. Paragraphes 84 et 93.

⁶⁷⁹ TA Bordeaux, 14 novembre 1990, n° 9000617, Rec. Lebon T., p. 974.

qu'il est en droit d'obtenir la communication de son dossier de soins. Pourtant, le code de la santé publique n'encadre pas les conditions d'accès au DMP de la personne protégée. En effet, le pouvoir exécutif est venu préciser que « *lorsque le titulaire du dossier médical partagé est [...] une personne majeure faisant l'objet d'une mesure de protection juridique, les droits énoncés à la présente section [relative au DMP] sont mis en œuvre conformément* »⁶⁸⁰ au droit commun du code civil et aux règles ordinairement spécifiques du code de la santé publique. Il en ressort que peuvent accéder au DMP : les patients faisant l'objet d'une mesure d'assistance ou de représentation, l'organe en charge de la représentation du titulaire du DMP et, s'il l'y a été autorisé, l'organe en charge de son assistance.

218. En outre, l'article 2 des conditions générales d'utilisation du DMP précisent que « *les personnes faisant l'objet d'une mesure de protection juridique accèdent [...] à leur DMP sous la responsabilité de leur(s) représentant(s) légal(aux)* »⁶⁸¹. Ces dispositions paraissent surprenantes dès lors que le majeur protégé profite pleinement du droit d'accéder, seul et directement, à ses données médicales. Cependant, l'accès au DMP n'est pas limité aux seules données médicales qu'il contient. En effet, l'accès au DMP permet notamment de renseigner des informations, d'autoriser ou d'opposer l'accès des professionnels de santé concourant à la prise en charge de son titulaire. En tant qu'outil de démocratie sanitaire, le DMP permet donc au patient de participer activement à son parcours de santé et d'opérer des choix pouvant l'impacter⁶⁸². S'il semble évident que les personnes faisant l'objet d'une protection juridique puissent librement accéder aux données personnelles contenues dans leur DMP, la formation à l'utilisation de cet outil numérique pourrait être supervisée par la personne en charge de leur protection. L'appréhension du DMP par une personne dont les facultés mentales sont altérées requiert un accompagnement dont la responsabilité pourrait revenir à son protecteur. En effet, les actions effectuées sur le DMP pourraient engendrer des conséquences médicales rendant nécessaires la protection de l'intéressé. Néanmoins, cet accompagnement ne devrait pas avoir pour effet de restreindre le droit d'accès direct du majeur protégé. L'exercice du droit d'accès direct de ce dernier ne devrait jamais être soumis à aucune autorisation.

⁶⁸⁰ Article R.1111-40 alinéa 5 du code de la santé publique.

⁶⁸¹ Article 2 des conditions générales d'utilisation du service DMP pour les bénéficiaires de l'assurance maladie.

⁶⁸² Cf. Paragraphes 81 à 83, 289, 293.

219. Même si l'article 70 de la loi Informatique et Libertés modifiée affirme que « *sont destinataires de l'information et exercent les droits de la personne concernée par le traitement [...] la personne chargée d'une mission de représentation dans le cadre d'une tutelle, d'une habilitation familiale ou d'un mandat de protection future, pour les majeurs protégés dont l'état ne leur permet pas de prendre seuls une décision personnelle éclairée* », les majeurs protégés exercent personnellement et directement leur droit d'accès aux données médicales consignées au sein de leurs dossiers médicaux. Le droit d'accès aux éléments immatériels de leur corps humain peut alors être regardé comme un droit subjectif et fondamental. Cependant, l'exercice de ce droit n'est pas absolu. En effet, il peut être assorti de tempéraments.

Section 2 : Les limitations de l'accès direct aux données médicales consignées dans les dossiers médicaux

220. Le droit pour le patient d'accéder directement aux données médicales consignées dans ses dossiers médicaux connaît des restrictions. Tout d'abord, l'accès à une donnée suppose qu'elle soit préalablement retranscrite au sein d'un support capable de l'héberger. En effet, l'intangibilité d'une information fait obstacle à sa communication (**Paragraphe 1**). Ensuite, l'exercice du droit d'accès ne « *doit pas porter atteinte au droit des tiers* »⁶⁸³. En conséquence, les données personnelles se rapportant à autrui ne peuvent être rendues accessibles au patient, quand bien même elles feraient l'objet d'une formalisation au sein de ses dossiers médicaux (**Paragraphe 3**). Finalement, le législateur a entendu limiter l'accès direct du patient aux informations médicales les plus délicates. Le cas échéant, le droit d'accéder aux données concernant sa santé peut être exercé par l'intermédiaire d'un accompagnant (**Paragraphe 2**).

Paragraphe 1 : Le principe d'accès aux seules informations formalisées

221. Le patient jouit du droit d'accéder à ses données médicales détenues par les établissements et les professionnels de santé. Néanmoins, le législateur a conditionné la disponibilité et la communicabilité de l'information médicale à sa mise en forme (**A**). Seule

⁶⁸³ CNIL, *Le droit d'accès : connaître les données qu'un organisme détient sur vous*. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 17 septembre 2020.

une information médicale formalisée par un responsable de traitement à l'occasion de la prise en charge sanitaire du patient peut donc devenir accessible (B).

A) L'accès aux informations formalisées en considération de leur fonction

222. Antérieurement à la loi du 31 janvier 2007⁶⁸⁴, l'accès aux données médicales détenues par les établissements et les professionnels de santé était soumis à une double condition. Dans sa version en vigueur jusqu'au 1^{er} avril 2007, l'article L.1111-7 du code de la santé publique disposait que « *toute personne a accès à l'ensemble des informations concernant sa santé détenues par des professionnels et établissements de santé, qui sont formalisées et ont contribué à l'élaboration et au suivi du diagnostic et du traitement ou d'une action de prévention* »⁶⁸⁵. En premier lieu, l'accessibilité de la donnée dépendait de son implémentation préalable au sein du dossier de soins du patient. L'Agence nationale d'accréditation et d'évaluation en santé (ANAES) affirmait que « *la tenue du dossier doit permettre de répondre à toute demande de consultation ou de transmission d'informations émanant de professionnels de santé comme de la personne* »⁶⁸⁶. Pour ainsi dire, le droit d'accès direct aux informations médicales formalisées résulte des obligations légales et déontologiques de constitution des dossiers de soins du patient⁶⁸⁷. En second lieu, il était également nécessaire que les informations mises en forme par le professionnel de santé comportent une plus-value médicale. En définitive, pouvait être communiquée au patient la donnée médicale consignée dans son dossier de soins à condition qu'elle eût contribué à la prise en charge sanitaire.

223. Cette double condition correspondait à la volonté du législateur d'exclure l'accès du patient aux notes personnelles prises par le médecin⁶⁸⁸. De cette façon, ces notes demeuraient personnelles au médecin tant qu'elles ne contribuaient pas à l'établissement du diagnostic ou de la thérapeutique et qu'elles n'étaient pas formalisées au sein du dossier de soins du patient.

⁶⁸⁴ Loi n° 2007-131 du 31 janvier 2007 relative à l'accès au crédit des personnes présentant un risque aggravé de santé, *JORF* n°27, 1 février 2007, p. 1945.

⁶⁸⁵ Version de l'article L.1111-7 du code de la santé publique en vigueur du 5 mars 2002 au 1^{er} février 2007.

⁶⁸⁶ Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, *loc. cit.*

⁶⁸⁷ Cf. Paragraphes 104 et 109.

⁶⁸⁸ Voir : EVIN (C.), CHARLES (C.), DENIS (J.-J.), *Rapport n°3263 du 26 septembre 2001, loc. cit.*

En 2004, le juge administratif a ainsi décidé que « *les notes manuscrites du médecin traitant qui ont contribué à l'élaboration et au suivi du diagnostic et du traitement de l'intéressée [...] et qui ont été conservées par l'hôpital font partie du dossier médical* »⁶⁸⁹. Précisément, soit la note prise par le médecin contribuait à la prise en charge médicale et ne lui était plus personnelle : le cas échéant, elle faisait partie intégrante du dossier médical et devenait un élément communicable ; soit la note prise par le médecin ne contribuait pas à la prise en charge médicale du patient et lui demeurait personnelle et non communicable. Ainsi, les notes personnelles prises par le professionnel de santé pouvaient ne jamais être communiquées au patient dès lors qu'elles ne participaient pas à la prise en charge médicale. L'effectivité du droit d'accès dépendait donc de la formalisation des données médicales au sein des dossiers médicaux du patient. Seulement, une donnée médicale ne peut y être implémentée qu'en fonction de sa plus-value technique dans le cadre de la prise en charge sanitaire du patient.

B) L'abandon du critère de fonctionnalité de l'information formalisée

224. La loi du 31 janvier 2007⁶⁹⁰ a modifié les dispositions de l'article L.1111-7 du code de la santé publique. Depuis, « *le patient a accès aux informations détenues par les établissements et les professionnels de santé et ce, à quelque titre que ce soit* »⁶⁹¹. Johanne Saison-Demars et Nora Boughriet affirment qu'il « *n'est plus nécessaire qu'une note personnelle ait contribué à l'élaboration et au suivi du diagnostic ou du traitement pour pouvoir être transmise. Il en résulte que l'exception des notes personnelles a été supprimée* »⁶⁹². Seule la formalisation de l'information relative à la santé du patient conditionne désormais sa communicabilité, peu importe la raison de sa détention par les établissements et les professionnels de santé. Dès lors, il convient de clarifier la signification du verbe formaliser afin de délimiter les contours de cette condition *sine qua non*. En effet, la lettre de l'article susmentionné conditionne le droit d'accès aux seules informations formalisées sans en préciser l'acceptation.

⁶⁸⁹ CAA Paris, 30 sept. 2004, n°03PA01769 : RDS, 2015, n° 05, p. 201, obs. F. Vialla.

⁶⁹⁰ Loi n° 2007-131 du 31 janvier 2007, *loc. cit.*

⁶⁹¹ SAISON-DEMARS (J.), BOUGHRIET (N.), *Les notes personnelles des médecins : un point d'incertitude dans la détermination du contenu transmissible du dossier*, RGDM, 2014, n°53, p. 44.

⁶⁹² *Ibid.*

Par définition, formaliser signifie « *mettre en forme, donner une forme définie à quelque chose* »⁶⁹³. Formaliser une information revient donc à l'intégrer dans un support au sein duquel elle sera enregistrée et, le cas échéant, organisée ou structurée. La formalisation d'une information équivaut alors à un traitement de données conformément à la définition de l'article 4.2 du RGPD. Concrètement, les informations médicales formalisées correspondent à celles « *auxquelles est donné un support (écrit, photographie, enregistrement, etc.) avec l'intention de les conserver et sans lequel elles seraient objectivement inaccessibles* »⁶⁹⁴. Le critère de la formalisation de la donnée est indispensable tant à son accès qu'à sa transmission. Effectivement, sans support matériel, l'information immatérielle demeure insaisissable. C'est pourquoi les informations orales ou celles qui ne pourraient être considérées comme formalisées échappent au dispositif de l'article L.1111-7 du code de la santé publique⁶⁹⁵, à moins qu'elles ne soient enregistrées sur un dictaphone ou tout autre support permettant une captation audio. La jurisprudence apprécie le critère de la formalisation d'une information médicale de façon extensive. Il a ainsi été jugé qu'étaient communicables les informations médicales formalisées au moyen de photographies⁶⁹⁶, de documents manuscrits ou dactylographiés⁶⁹⁷, de moulages dentaires⁶⁹⁸ ou encore de bandes d'enregistrement audiovisuelles⁶⁹⁹. Les informations reportées dans le DMP sont également des données formalisées dans la mesure où elles sont structurées et enregistrées au sein de ce support numérique. Compte tenu de ce qui précède, il convient d'opter pour une approche littérale du critère de *formalisation* de l'information médicale.

225. Plus généralement, toute donnée personnelle relative à une personne physique devient effectivement accessible et communicable dès l'instant où elle est mise en forme sur un support. Il résulte que les notes personnelles du médecin contenant des informations relatives au patient doivent lui être communiquées quand bien même elles n'auraient pas contribué à

⁶⁹³ Dictionnaire Larousse, disponible en ligne sur le site [www.larousse.fr]. Consulté le 01 septembre 2020.

⁶⁹⁴ Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, *op. cit.*

⁶⁹⁵ LALLET (A.), NGUYEN DUY (P.), *op.cit.*, § 475.

⁶⁹⁶ CADA, 24 janvier 2013, conseil n°20130176.

⁶⁹⁷ CAA Paris, 30 septembre 2004, n°03PA01769, obs. F. Violla, RDS, 2015, n° 05, p. 201 ; CADA, 15 avril 2004, avis n°20041645.

⁶⁹⁸ CADA, 5 mars 2015, avis n°20150002.

⁶⁹⁹ CAA Marseille, 25 juin 2009, n°07MA02024.

sa prise en charge médicale. En effet, la prise de notes par le médecin correspond à une mise en forme d'informations contenues sur un support dans le cadre d'une activité professionnelle. A ce titre, Caroline Zorn-Macrez déclare que « *les notes personnelles du médecin constituent un traitement de données à caractère personnel* »⁷⁰⁰ dont il est responsable. Assurément, la formalisation de notes personnelles constitue un traitement de données personnelles entrant dans le champ d'application matériel du droit des données à caractère personnel⁷⁰¹.

Le droit d'accès aux données personnelles est exigible à l'égard de tout responsable de traitement. Exceptionnellement, l'exercice de ce droit peut être limité lorsque cette restriction est nécessaire et proportionnée pour éviter d'entraver des enquêtes, des recherches ou des procédures administratives ou judiciaires, pour éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes, aux poursuites ou à l'exécution de sanctions pénales, pour protéger la sécurité publique, pour protéger la sécurité nationale ou pour protéger les droits et libertés d'autrui⁷⁰². Hormis ces cinq limitations concernant les fichiers de police, la sûreté de l'Etat ou les droits et libertés d'autrui, le droit d'accès aux données personnelles est un droit absolu auquel le responsable de traitement ne peut s'opposer. Dès lors, pourquoi le médecin responsable des « notes personnelles », bénéficierait-il d'une dérogation spéciale à laquelle aucun autre responsable de traitement ne pourrait prétendre ?

Seules les cinq exceptions instituées à l'article 107 de la loi Informatique et Libertés peuvent légitimer une restriction au droit d'accès conféré par l'article 15 du RGPD. Or, aucune de ces cinq exceptions ne justifierait une restriction du droit, pour la personne concernée, d'accéder aux notes personnelles constituées par son médecin dans le cadre professionnel de sa prise en charge sanitaire. Que les notes du médecin portent sur la santé ou sur la vie privée du patient, la personne concernée par ce traitement devrait donc jouir d'un droit d'accès à l'ensemble des données qui la concernent, quelle que soit la nature du fichier au sein duquel elles sont formalisées. *In fine*, les notes personnelles du médecin sont définitivement des données personnelles au patient. Elles lui sont donc communicables de

⁷⁰⁰ ZORN-MACREZ (C.), *Les « notes personnelles » du médecin ? : les conséquences d'un décret d'arrière-garde*, RDS, 2012, n° 49, p. 583.

⁷⁰¹ Article 2 du RGPD ; Article 2 de la loi Informatique et Libertés modifiée.

⁷⁰² Article 107 I de la loi Informatique et Libertés modifiée.

plein droit en vertu de l'article 15 du RGPD⁷⁰³. Par suite, le droit d'accès aux données personnelles doit être élargi aux « *notes préparatoires telles les notes d'un étudiant ou les réflexions personnelles du médecin* » qui ne font pas partie du dossier médical⁷⁰⁴ mais qui sont, par ailleurs, formalisées au sein d'un support. En cas de refus du médecin responsable de traitement, le patient serait fondé à adresser une plainte auprès de la CNIL dans l'espoir d'obtenir l'exécution de son droit⁷⁰⁵.

226. L'abandon du critère de la fonction de l'information communicable au profit de sa formalisation a eu pour effet de rendre les notes personnelles du médecin accessibles au patient. Cependant, le droit d'accès du patient à ses données formalisées au sein des notes personnelles du médecin a été remis en cause par la réforme de l'article 45 du code de déontologie médicale. En effet, par un décret du 7 mai 2012⁷⁰⁶, les pouvoirs publics se sont assurés que « *les notes personnelles du médecin ne sont ni transmissibles ni accessibles au patient et aux tiers* »⁷⁰⁷. La rectification du périmètre des informations médicales communicables au patient manifeste la volonté de garantir l'inaccessibilité des notes personnelles du médecin. Seulement, « *le code de déontologie introduit une précision qui, non seulement est contraire aux dispositions figurant dans la partie législative du code de la santé publique* »⁷⁰⁸, mais également aux dispositions de la loi Informatique et Libertés et du RGPD. En effet, le simple fait que le médecin formalise une information personnelle suffit à la rendre accessible à la personne concernée dans la mesure où cette action répond à la définition d'un traitement de données. Force est de remarquer que « *le décret nouveau a [...] créé une contradiction fondamentale entre l'intransmissibilité des notes personnelles du médecin et le droit de la personne à un accès direct à ses informations de santé* »⁷⁰⁹. Néanmoins, en vertu du principe de la hiérarchie des normes, les dispositions réglementaires

⁷⁰³ Dans ce contexte, l'article L.1111-7 du code de la santé publique ne peut être applicable dans la mesure où toute donnée concernant la santé du patient doit être formalisée dans son dossier de soins. Les notes personnelles du médecin ne peuvent donc contenir que des données n'ayant pas de plus-value médicale.

⁷⁰⁴ EVIN (C.), CHARLES (C.), DENIS (J.-J.), *Rapport n°3263 du 26 septembre 2001, loc. cit.*

⁷⁰⁵ Cf. Paragraphe 192.

⁷⁰⁶ Décret n° 2012-694 du 7 mai 2012 portant modification du code de déontologie médicale, *JORF* n°108, 8 mai 2012, p. 8479.

⁷⁰⁷ Article 4127-45 du code de la santé publique.

⁷⁰⁸ LAUDE (A.), *Le code de déontologie médicale enfin modifié !*, Recueil Dalloz, 2012, n°26, p.1694.

⁷⁰⁹ ZORN-MACREZ (C.), *Les « notes personnelles » du médecin ? : les conséquences d'un décret d'arrière-garde, op. cit., p. 583.*

ne peuvent déroger aux dispositions législatives. En conséquence, la norme déontologique selon laquelle les notes personnelles du médecin seraient intransmissibles est *contra legem*.

227. Emprunte d'un réalisme légitimé par sa qualité d'avocat, Caroline Zorn-Macrez⁷¹⁰ a invité le législateur à procéder à la modification de ce texte dans l'optique d'une mise en conformité à la législation nationale et européenne. Seulement, ces dispositions illégales⁷¹¹ demeurent actuellement en vigueur. En dépit du fait que la jurisprudence soit subordonnée à la loi, les juges⁷¹² et la CADA⁷¹³ conditionnent toujours la communicabilité de l'information médicale à sa fonction. A l'instar du pouvoir réglementaire, les praticiens du droit marquent également leur opposition à la communication des notes personnelles. Il en advient qu'en pratique, la personnalisation des notes du médecin prime illégalement sur la personnalité des informations relatives à un individu. Seulement, les notes personnelles du médecin sont constituées d'informations personnelles au patient concerné, à l'égard desquelles il dispose de droits attachés à sa personne⁷¹⁴. Il en résulte que la sauvegarde du caractère personnel des notes du médecin porte atteinte à la transparence des informations⁷¹⁵ et des droits appartenant à la personne concernée sur ses données personnelles.

228. Les dispositions du RGPD rappellent qu' « *une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel, ainsi que de prévoir, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations* »⁷¹⁶. Afin de dénouer la problématique de l'accès aux données formalisées au sein des notes personnelles du médecin, il serait opportun que la CNIL se saisisse du sujet. A cette occasion, cette autorité pourrait surveiller et contrôler la licéité des traitements ayant pour

⁷¹⁰ *Ibid.*

⁷¹¹ MORET-BAILLY (J.), *La déontologie médicale, de la résistance à la contre-offensive (à propos du décret du 7 mai 2012 portant modification du code de déontologie médicale)*, RDSS, 2012, n°06, p. 1076.

⁷¹² TA d'Amiens n°1200264, 24 octobre 2013; TA de Melun n°1504175, 16 octobre 2015.

⁷¹³ CADA, 21 février 2013, avis n°20130447.

⁷¹⁴ Cf. Paragraphe 356.

⁷¹⁵ Article 12 du RGPD.

⁷¹⁶ Considérant 11 du RGPD.

finalité la constitution de notes personnelles, et notamment veiller à l'information de la personne concernée quant au droit d'accès aux données traitées pour cette finalité. Par ailleurs, cette saisine pourrait inciter le législateur à conformer le code de déontologie médicale à la loi. Depuis l'entrée en vigueur du RGPD, les citoyens européens ont pris conscience de l'importance du droit fondamental à la protection de leurs données à caractère personnel. Il serait louable que l'Homme de loi l'intègre à son tour.

En outre, il convient de préciser que cette réforme ne remet pas en question la communicabilité de la *fiche d'observation personnelle* qui demeure accessible dans le respect des dispositions de l'article L.1111-7 du code de la santé publique. Il est utile de rappeler que les notes personnelles ne peuvent contenir aucun élément nécessaire aux décisions diagnostiques et thérapeutiques du patient⁷¹⁷. Le cas échéant, ces éléments doivent être formalisés au sein du dossier de soins du patient pris en charge en médecine de ville : la fiche d'observation personnelle. Effectivement, la fonction de la donnée médicale ne permet pas de déterminer son caractère communicable mais de distinguer les informations à formaliser au sein des dossiers médicaux eu égard au principe de minimisation des données⁷¹⁸.

Paragraphe 2 : L'accès indirect aux informations requérant un accompagnement

229. Les données médicales formalisées dans les dossiers médicaux du patient correspondent à des éléments physiques, psychiques et biologiques collectés par les professionnels de santé à l'occasion de sa prise en charge sanitaire. Les dossiers médicaux comportent donc des informations techniques et complexes, auxquelles les patients ont le droit d'accéder, mais dont la lecture peut s'avérer incompréhensible pour le profane (**A**). Partant, un accès indirect par l'intermédiaire d'un tiers accompagnant peut être recommandé, notamment lorsque le patient souffre d'une pathologie grave. En effet, il convient de prémunir le patient contre ses informations les plus angoissantes (**B**). Dès lors, l'accompagnement dans l'accès à l'information médicale *a posteriori* devrait relever d'un devoir déontologique incombant au professionnel de santé.

⁷¹⁷ Cf. Paragraphe 71.

⁷¹⁸ Cf. Paragraphe 72.

A) Les dangers de l'accès direct à des données médicales ésotériques

230. Le droit à l'information médicale constitue la clé de voûte des droits des malades. Consécration de la transparence dans la relation médicale, ce droit prééminent est renforcé par le droit d'accès direct du patient aux éléments immatériels de son corps humain. S'il n'existe pas de secret entre les professionnels de santé et les malades, les informations médicales doivent cependant leur être délivrées de façon claire, loyale, et surtout, appropriée. D'abord, la clarté de l'information médicale implique qu'elle soit vulgarisée et simplifiée en fonction des capacités de compréhension du patient. Le professionnel de santé doit alors s'assurer que le malade a bien saisi chacune des explications données. Ensuite, la loyauté de l'information médicale suppose l'honnêteté du praticien qui se doit d'être transparent. Enfin, l'information médicale doit être adaptée à la personnalité du patient, à sa pathologie et à ses caractères particuliers. Lorsqu'elle est délivrée en amont de l'acte sanitaire, l'information médicale doit donc être nuancée par le professionnel de santé.

231. Cependant, lorsque le patient exerce son droit à l'information médicale *a posteriori* via l'accès à ses données médicales, il perçoit directement des informations formulées en des termes médicaux, sans adaptation ni interprétation. Le patient pourrait alors prendre connaissance, en toute transparence, d'une information préalablement délivrée partiellement. Pourtant, l'institution du droit d'accès direct du patient aux informations concernant sa santé « ne saurait dispenser le professionnel de santé de son devoir de communiquer régulièrement à la personne les informations pertinentes concernant sa santé, ce qui devrait limiter les demandes d'accès au dossier et rendre improbable la découverte fortuite d'informations significatives lorsque la personne souhaite accéder à son dossier »⁷¹⁹. Néanmoins, la transparence de l'information médicale préalable peut s'avérer épineuse à délivrer. Un diagnostic lourd ou un pronostic péjoratif peut s'avérer ardu à expliciter. C'est pourquoi, les médecins optent parfois pour une explication épurée, en tenant compte de la psychologie du patient. En revanche, dans le cadre d'un accès direct aux données médicales, la personnalité du patient ne peut être considérée. Seulement, l'accès direct aux informations scientifiques et techniques, retranscrivant la réalité d'une condition physiologique, peut engendrer des conséquences physiques et psychiques préjudiciables pour la santé de la personne concernée.

⁷¹⁹ Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, *loc. cit.*

En effet, une mauvaise nouvelle « *peut être ressentie comme une condamnation à mort, mais aussi [comme] une condamnation à mal vivre* »⁷²⁰. Or, il a été prouvé que l'optimisme et la bonne santé mentale jouaient un rôle prépondérant dans le processus de guérison du patient. En effet, une personne psychologiquement déprimée produit moins de défenses immunitaires qu'une personne dont le moral est propice. Le choc de la découverte d'un pronostic défavorable pourrait alors amoindrir les chances de guérison du malade.

B) La nécessaire préservation du patient à l'égard de ses données médicales

232. Les dangers de l'accès direct à des informations techniques ont été signalés par le Conseil national de l'Ordre des médecins à l'occasion de son audition sur le projet de loi sur les droits des malades. Afin de pallier cet écueil, il est apparu nécessaire « *de réfléchir à la possibilité législative de protéger le patient contre les dommages personnels qu'entraînerait l'accès à la connaissance du pronostic grave ou psychiatriquement délicat* »⁷²¹. Cette alerte a été prise en compte par le législateur. En effet, les dispositions de l'article L.1111-7 du code de la santé publique prévoient que « *la présence d'une tierce personne lors de la consultation de certaines informations peut être recommandée par le médecin les ayant établies ou en étant dépositaire, pour des motifs tenant aux risques que leur connaissance sans accompagnement ferait courir à la personne concernée* ». Seulement, la présence d'une tierce personne étrangère au corps médical pourrait s'avérer insuffisante eu égard à la spécificité des informations médicales non vulgarisées. Dans l'hypothèse où l'état de santé du patient est délétère, il serait judicieux que l'accompagnant soit un professionnel de santé. Dans ce contexte, il lui incomberait un devoir d'accompagnement dans l'accès aux informations concernant la santé du patient. De cette façon, le traumatisme vécu par le patient pourrait être atténué par le soignant. Même si dans cette hypothèse la consultation des informations n'a pas lieu par l'intermédiaire d'un médecin, le droit d'accès direct du patient à ses données médicales peut être limité au profit d'un accès en présence d'une tierce personne, et idéalement d'un professionnel de santé chargé d'adapter et d'expliquer des

⁷²⁰ HAS, *Annouer une mauvaise nouvelle*, Service évaluation des pratiques, février 2008, p. 4.

⁷²¹ EVIN (C.), CHARLES (C.), DENIS (J.-J.), *Rapport n°3263 du 26 septembre 2001*, loc. cit.

informations redoutables. Certainement, les éléments immatériels du corps humain, propres à la physiologie d'un individu, révèlent techniquement un état de santé.

233. La protection du patient à l'égard de ses informations dommageables a également été assurée dans le cadre de l'accès à son DMP. A l'occasion de l'alimentation du DMP, « lorsqu'un professionnel estime qu'une donnée sur l'état de santé versée dans le dossier médical partagé ne doit pas être portée à la connaissance du patient sans accompagnement, il peut rendre cette donnée provisoirement inaccessible au titulaire du dossier en attendant qu'elle soit délivrée à ce dernier par un professionnel de santé lors d'une consultation d'annonce »⁷²². Lorsque l'accès aux données médicales intervient par le biais du DMP, le pouvoir exécutif impose que le tiers accompagnant soit un professionnel de santé. L'accès indirect aux données du DMP par cet intermédiaire permet d'humaniser la relation médicale à travers le colloque singulier⁷²³. Assurément, l'éthique médicale exige que la connaissance d'une information sensible soit accompagnée d'empathie, de bienveillance, de communication, de patience et d'écoute. Il serait impitoyable de laisser le patient affronter seul une mauvaise nouvelle. La disponibilité et la présence du professionnel de santé apparaît donc primordiale et la limitation de l'accès des informations contenues dans le DMP justifiée.

234. Toutefois, la limitation de l'accès direct aux informations requérant un accompagnement n'est pas absolue. Effectivement, la restriction de l'accès aux informations redoutables est instituée dans l'intérêt du patient, qui peut refuser l'accompagnement proposé⁷²⁴. Effectivement, l'accompagnement d'une tierce personne ne relève que d'une recommandation formulée par le médecin dépositaire des informations médicales délicates. En outre, lorsque le patient ne répond pas à la proposition d'accompagnement, ses informations médicales lui sont communiquées huit jours après la demande d'accès⁷²⁵. De la même façon, lorsque le titulaire du DMP ne consulte pas un médecin pouvant l'accompagner

⁷²² Article R.1111-53 alinéa 1 du code de la santé publique.

⁷²³ Empruntée à Louis Portes, le colloque singulier est une notion définie par Georges Duhamel, médecin et écrivain français, en 1937, comme « *la rencontre d'une confiance et d'une conscience* ». Le colloque singulier est la pierre angulaire de la relation malade-soignant.

⁷²⁴ Article R.1111-4 du code de la santé publique.

⁷²⁵ *Ibid.*

dans l'accès à l'information rendue inaccessible dans le délai d'un mois après son versement, elle devient automatiquement accessible⁷²⁶.

235. Si le refus de l'accompagnement ne fait, en principe, pas obstacle au droit d'accès direct aux informations concernant la santé du patient, certaines informations ne sont accessibles qu'indirectement par l'intermédiaire d'un médecin. En premier lieu, les résultats d'examen des caractéristiques génétiques ne peuvent être communiquées à la personne concernée que par le médecin l'ayant prescrit⁷²⁷. Cette dérogation à l'article L.1111-7 du code de la santé publique est justifiée par la nature particulière des données génétiques. En effet, Isabelle De Lamberterie explique que « *les données génétiques se distinguent sur plusieurs points des données de santé traditionnelles : elles ne sont pas uniquement personnelles, elles ont un pouvoir prédictif* »⁷²⁸. L'auteur précise que les données médicales « *que l'on obtient des examens médicaux n'informent que sur l'état de santé du malade à un instant donné, les données génétiques informent sur l'avenir* »⁷²⁹. La prise de connaissance des données génétiques peut donc bouleverser le cours de la vie du patient et remettre en cause sa perception du futur. De surcroît, la lecture et la compréhension des données génétiques requiert une expertise. L'information et l'accompagnement du médecin apparaît essentiel eu égard à la particularité de cette catégorie de données personnelles.

236. En deuxième lieu, l'accès aux informations collectées dans le cadre d'une admission en soins psychiatriques sans consentement peut être subordonné à la présence d'un médecin désigné par le patient. Toutefois, cet accès indirect ne peut intervenir qu'à titre exceptionnel lorsque la connaissance de ces informations entraînerait des dangers pour la personne concernée⁷³⁰. En effet, la présence d'un médecin est requise « *en cas de risques liés à une gravité particulière appréciée en liant la nature des informations présentes dans le dossier à l'état de santé de la personne* »⁷³¹. La décision de limitation du droit d'accès direct doit

⁷²⁶ Article R.1111-53 alinéa 2 du code de la santé publique.

⁷²⁷ Article L.1131-1-3 du code de la santé publique.

⁷²⁸ DE LAMBERTERIE (I.), *Débat éthique et juridique relatif à l'accès aux données génétiques*, Revue internationale d'éthique sociétale et gouvernementale, vol. 6, Éthique publique, 2004, n° 2, § 12.

⁷²⁹ *Ibid.*

⁷³⁰ Article L.1111-7 alinéa 4 du code de la santé publique.

⁷³¹ MONTET (I.), *Le dossier médical en psychiatrie ambulatoire*, L'information psychiatrique, vol. 84, 2008, n°4, p. 358 à p. 359.

être prise par le directeur de l'établissement de soins psychiatriques⁷³². Néanmoins, il est important de préciser que le directeur de l'établissement « *ne peut de lui-même limiter l'étendue de l'information médicale délivrée au malade : il peut seulement décider du cadre (présence d'un médecin) dans lequel aura lieu la communication de cette information* »⁷³³. Le cas échéant, le patient est informé de cette limitation et peut accepter d'accéder à ses informations par l'intermédiaire du médecin de son choix. Néanmoins, le patient peut refuser cet accès indirect et saisir la Commission départementale des hospitalisations psychiatriques. La CDHP est chargée de statuer sur les modalités d'accès aux informations relatives à la santé de la personne hospitalisée sous contrainte dans un délai de deux mois à compter de sa saisine. L'avis contraignant de la commission s'impose au patient et au directeur de l'établissement de santé mentale. A ce titre, la commission peut affirmer la nécessité d'un accès indirect par l'intermédiaire d'un médecin, ou accorder au patient un droit d'accès direct aux informations recueillies dans le cadre de son hospitalisation sous contrainte.

237. Force est de constater que « *les patients faisant l'objet d'une hospitalisation sous contrainte ne disposent pas d'un droit absolu d'accéder directement à leur dossier médical* »⁷³⁴. Cependant, la limitation de ce droit est contrôlée par une instance indépendante devant statuer dans l'intérêt du patient. Frédéric Dieu déclare qu'il « *prévaut ainsi une conception finaliste ou fonctionnelle de l'accès à l'information médicale, commandé par l'intérêt du malade, et non une conception absolue* »⁷³⁵. En ce sens, François Vialla ajoute qu'il convient de « *prémunir [la personne] contre la violence éventuelle des révélations auxquelles elle pourrait accéder en consultant son dossier. La lecture du dossier n'est pas un acte neutre et certains éléments peuvent se révéler difficilement acceptables, dans le champ de la santé mentale, notamment.* »⁷³⁶. La consultation des informations psychiatriques par

⁷³² CE, 10 avril 2009, n° 289794, Rivoallan, Rec. Lebon, 2009, p. 752 ; RDSS, 2009, n° 04, p. 688, note F. Dieu ; RDS, 2009, n°30, p. 343, obs. F. Vialla.

⁷³³ DIEU (F.), *Hospitalisation sous contrainte et encadrement thérapeutique de l'information délivrée au malade*, RDSS, 2009, n°04, p. 693.

⁷³⁴ DIEU (F.), *op. cit.*, p. 690.

⁷³⁵ DIEU (F.), *op. cit.*, p. 694.

⁷³⁶ VIALLA (F.), *Les restrictions à l'accès au dossier médical*, RDS, 2009, n°30, p. 343.

l'intermédiaire du médecin permet, là encore, d'estomper le traumatisme de la révélation dont le patient pourrait souffrir⁷³⁷.

238. La question de la révélation importune d'informations psychiatriques délicates se pose dans le cadre de l'accès direct au DMP. Dans l'hypothèse où la commission pourrait enjoindre une communication indirecte, le professionnel de santé est-il tenu d'alimenter le DMP du patient hospitalisé sous contrainte ? Le cas échéant, le titulaire du DMP pourrait accéder à des informations dommageables. De surcroît, la limitation de l'accès aux informations collectées en cours de l'hospitalisation en psychiatrie n'est pas décidée par le professionnel de santé qui en est le producteur mais par le directeur de l'établissement. Au moment de l'alimentation du DMP, le professionnel de santé ne peut anticiper l'inaccessibilité ultérieure d'une information versée. De plus, l'information inscrite dans ce dossier médical numérique ne peut être rendue inaccessible que provisoirement. En effet, elle devient directement accessible dans un délai d'un mois après qu'elle ait été versée dans le DMP. Or, l'avis de la CDHP s'imposant aux parties, une information ne peut être rendue directement accessible au patient dans l'hypothèse où il a été décidé que le droit d'accès ne pouvait être exercé que par l'intermédiaire d'un médecin. Le pouvoir exécutif devrait alors préciser les règles d'intégration, dans le DMP, des informations collectées dans le cadre d'une admission en soins psychiatriques sans consentement.

239. Si la limitation du droit d'accès direct aux informations recueillies à l'occasion de l'hospitalisation sous contrainte a pour effet de protéger le patient, la restriction de ce droit a également vocation à protéger les tiers à l'origine de l'hospitalisation forcée du malade mental.

Paragraphe 3 : Le secret des données personnelles concernant les tiers

240. Tandis que la relation de soins est par nature bipartite⁷³⁸, il arrive qu'un tiers⁷³⁹ se trouve impliqué dans la prise en charge sanitaire du patient. Des données personnelles

⁷³⁷ CE, 10 avril 2009, n° 289794, Rivoallan, Rec. Lebon, 2009, p. 752 ; RDSS, 2009, n° 04, p. 688, note F. Dieu ; RDS, 2009, n°30, p. 343, obs. F. Vialla.

⁷³⁸ Entre les professionnels d'une part, et le malade d'autre part.

⁷³⁹ Selon la CADA, avis n° 20062245, 11 mai 2006 : sont considérées comme des tiers les autres personnes que le malade.

concernant le tiers peuvent alors être consignées dans le dossier médical du patient. Le cas échéant, le patient ne bénéficie pas de la qualité de personne concernée à l'égard des données se rapportant au tiers et ne peut y accéder. Assurément, les données personnelles à un tiers ne sont transmissibles qu'au principal intéressé (A). De la même façon, le législateur a restreint l'accès du patient aux informations le concernant dès lors qu'elles ont été recueillies par le professionnel de santé auprès d'un tiers à la relation médicale (B).

A) La protection des données médicales relatives aux tiers à la relation sanitaire

241. Compte tenu des dispositions de l'article L.1111-7 du code de la santé publique, « toute personne a accès à l'ensemble des informations concernant sa santé [...] à l'exception des informations [...] concernant un tel tiers ». Aussi étonnant que cela puisse paraître, des informations relatives à des tiers peuvent être formalisées au sein du dossier de soins du patient dès lors qu'elles s'avèrent pertinentes et nécessaires à la prise en charge médicale. A titre d'exemple, le professionnel de santé peut collecter des informations concernant un tiers à la prise en charge médicale consécutivement à un examen portant sur les caractéristiques génétiques du patient. Par ailleurs, le patient peut révéler, au professionnel de santé, des informations relatives à des antécédents familiaux ou liées aux relations qu'il entretient avec des tiers.

242. L'accès aux informations concernant les tiers est particulièrement controversé lorsque le droit d'accès aux informations médicales du patient est exercé par ses représentants légaux, *a fortiori* par les titulaires de l'autorité parentale. En effet, le dossier médical d'un patient mineur peut contenir des informations pouvant impliquer les personnes avec lesquelles il entretient des rapports biologiques ou intimes et dont la révélation pourrait bouleverser la stabilité de sa vie familiale. Pourtant, les représentants légaux du mineur exercent le droit d'accès en représentation de l'enfant. Dans ce contexte, ils pourraient prendre connaissance d'informations relatives à d'autres personnes physiques que le mineur au nom duquel ils agissent. Par conséquent, ces derniers devraient être contraints par les restrictions du droit d'accès opposables à la personne concernée. Alors, les titulaires de l'autorité parentale ne pourraient accéder aux informations concernant les tiers bien qu'elles soient formalisées au sein du dossier médical du mineur.

243. Néanmoins, par un avis du 6 décembre 2018, la CADA a enjoint les Hôpitaux du Pays du Mont-Blanc à communiquer, aux titulaires de l'autorité parentale, des documents comportant des propos concernant des tiers, tenus par leur fille à l'occasion de son hospitalisation en service de pédiatrie, sans qu'ils ne soient préalablement occultés⁷⁴⁰. Il n'est pas rare que des adolescents confient, aux professionnels de santé, des informations relatives aux comportements de leurs proches ou aux relations qu'ils entretiennent avec ces derniers. Dans cette affaire, la CADA a estimé que la communication des mentions concernant les tiers n'était pas susceptible de porter atteinte au bien-être de l'enfant. L'autorité administrative a donc émis « *un avis favorable à la communication des documents sollicités non occultés* »⁷⁴¹. Le raisonnement retenu par la commission nous semble aberrant. Assurément, cet avis ne tient pas en compte l'exception de l'inaccessibilité aux informations concernant les tiers à la prise en charge médicale. Pourtant, le droit d'accès aux documents administratifs, prescrit à l'article L.311-6 du code des relations entre le public et l'administration, s'exerce dans les limites de l'article L.1111-7 du code de la santé publique auquel il renvoie. En conséquence, quand « *la demande porte sur un document comportant des mentions qui ne sont pas communicables [...] mais qu'il est possible d'occulter ou de disjoindre, le document est communiqué au demandeur après occultation ou disjonction de ces mentions* »⁷⁴². Il en résulte que les propos du patient, se rapportant à des tiers, doivent toujours être occultés et ne peuvent jamais être communiqués à ses représentants légaux.

244. Si les informations concernant les tiers à la prise en charge thérapeutique sont exclues du droit d'accès aux informations concernant la santé du patient, il n'en demeure pas moins que le tiers est directement concerné par les informations formalisées dans le dossier médical d'une personne tierce à son égard. En conséquence, le tiers doit pouvoir accéder aux informations qui le concernent, bien qu'elles soient intégrées dans le dossier médical d'un autre individu. C'est ainsi que la CADA estime qu'« *une fois l'enfant né, le droit d'accès prévu à l'article L1111-7 [du code de la santé publique] s'étend aux éléments contenus dans le dossier de suivi prénatal, à condition, toutefois, que puissent être extraites de ce dossier des informations concernant exclusivement l'enfant à naître, à l'exclusion de tout élément*

⁷⁴⁰ CADA, avis n°20183141, 06 décembre 2018.

⁷⁴¹ *Ibid.*

⁷⁴² L.311-7 du code des relations entre le public et l'administration.

dont la divulgation porterait atteinte au secret médical de la mère »⁷⁴³. Effectivement, le tiers ne peut accéder aux informations relatives au titulaire du dossier médical mais uniquement aux informations qui lui sont personnelles.

De la même façon, la CADA considère que le dossier médical d'un mineur comportant l'analyse des caractéristiques génétiques de l'enfant et de ses deux parents ne peut être communiqué aux titulaires de l'autorité parentale qu'« *après occultation ou disjonction des informations médicales relatives aux parents, notamment leurs caractéristiques génétiques* »⁷⁴⁴. La CADA rappelle que « *les parents ne peuvent accéder à ces informations, pour ce qui concerne chacun d'eux, que dans le cadre d'une demande d'accès portant spécifiquement sur les informations concernant leur santé* »⁷⁴⁵. Manifestement, l'exception posée à l'article L.1111-7 du code de la santé publique octroie une protection aux informations concernant les tiers à la prise en charge thérapeutique. En effet, l'accès aux informations médicales concernant un tiers constituerait une ingérence dans la vie privée d'autrui et une violation de ses données à caractère personnel.

245. Afin d'éviter tout incident, les informations se rapportant à un tiers doivent être intégrées au sein d'un volet spécifique du dossier médical hospitalier⁷⁴⁶, séparément des informations n'impliquant que le patient. Dans l'hypothèse où le patient exercerait son droit d'accès aux informations détenues par les établissements de santé, le volet comportant 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* »⁷⁴⁷ ne lui serait alors pas communiqué.

A l'inverse du dossier médical hospitalier, l'architecture de la fiche d'observation personnelle n'est pas arrêtée. Il n'empêche que la distinction des informations incluant un tiers doit être observée. Si les informations impliquant un tiers n'ont pas à être obligatoirement compartimentées, il s'agit néanmoins « *de veiller à ne pas mentionner*

⁷⁴³ CADA, avis n°20183756, 10 janvier 2019.

⁷⁴⁴ CADA, conseil n° 20091209, 18 juin 2009.

⁷⁴⁵ *Ibid.*

⁷⁴⁶ Article R.1112-2 3° du code de la santé publique.

⁷⁴⁷ *Ibid.*

d'informations non transmissibles dans un document qui, par sa nature même, fait partie de ceux communicables au patient »⁷⁴⁸. Assurément, Coralie Leuzzi-Louchart insiste sur le fait que « rien n'interdit à un médecin de faire figurer des informations concernant des tiers extérieurs à la relation de soins, mais il doit veiller à ne pas les mentionner dans une pièce du dossier susceptible d'être communiquée au patient »⁷⁴⁹. Si le médecin venait, par imprudence ou négligence, à communiquer des données personnelles à un tiers, il encourrait une peine de trois ans d'emprisonnement et de 100 000 euros d'amende⁷⁵⁰. Le médecin doit donc se montrer particulièrement vigilant en sectorisant les informations colligées à l'occasion de la prise en charge médicale du patient afin de limiter les risques d'atteinte à la vie privée de la personne concernée.

B) L'atteinte au droit d'accéder à ses informations personnelles recueillies auprès d'un tiers

246. Compte tenu de la restriction envisagée à l'article L.1111-7 du code de la santé publique, le patient ne peut accéder à ses informations personnelles lorsqu'elles ont été recueillies auprès d'un tiers n'intervenant pas dans la prise en charge thérapeutique. Pourtant, à l'occasion d'une prise en charge médicale, le professionnel de santé peut être amené à collecter des informations relatives au patient auprès de ses proches, ou encore auprès de son employeur ou d'un enseignant. Le cas échéant, ces informations doivent être formalisées sur un document non-communicable au patient⁷⁵¹. Coralie Leuzzi-Louchart considère que « le secret des informations concernant une personne, préserve par là même le secret des confidences que tout usager peut porter à la connaissance d'un professionnel dans le cadre d'une relation établie lors de la prise en charge d'un membre de sa famille, ou de son entourage »⁷⁵². En d'autres termes, les informations recueillies auprès des tiers sont protégées par un secret professionnel opposable au patient. Cette position nous paraît

⁷⁴⁸ LEUZZI-LOUCHART (C.), *Des dossiers médicaux au dossier hospitalier : la définition du dossier médical par la réglementation du contenu*, RGDM, 2014, n°53, p. 41.

⁷⁴⁹ LEUZZI-LOUCHART (C.), *Des dossiers médicaux au dossier hospitalier : la définition du dossier médical par la réglementation du contenu*, op. cit., p. 40.

⁷⁵⁰ Article 226-22 du code pénal.

⁷⁵¹ Cf. supra.

⁷⁵² LEUZZI-LOUCHART (C.), *Des dossiers médicaux au dossier hospitalier : la définition du dossier médical par la réglementation du contenu*, op. cit., p. 39.

surprenante. En effet, quel que soit l'émetteur de l'information, les renseignements fournis par les tiers se rapportent au patient. Il s'ensuit que le patient dispose de la qualité de « personne concernée » par les informations recueillies auprès des tiers et formalisées dans un cadre professionnel⁷⁵³. A ce titre, le patient devrait être informé de cette collecte et bénéficier du droit d'accéder à ses informations personnelles, ne serait-ce que pour les vérifier et, le cas échéant, les corriger.

247. Assurément, lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable de traitement doit l'en informer « *dans un délai raisonnable après avoir obtenu les données à caractère personnel* »⁷⁵⁴. Il en ressort que l'établissement ou le professionnel de santé devrait informer le patient de tout recueil de données effectué auprès d'un tiers. En outre, parmi les informations fournies au patient, le responsable de traitement devrait également lui indiquer « *l'existence du droit de demander l'accès à celles-ci* »⁷⁵⁵, ainsi que « *la source d'où proviennent les données à caractère personnel* »⁷⁵⁶. Nous remarquons que l'exclusion de l'accès aux informations personnelles recueillies auprès de tiers à la prise en charge médicale va à l'encontre du droit à l'information de la personne concernée par le traitement de ses données personnelles.

S'il est inconcevable que le patient soit privé de l'accès aux informations qui le concernent, nous pouvons toutefois admettre que cette information fasse l'économie de « *la source d'où proviennent les données* »⁷⁵⁷. L'esprit de l'exception posée à l'article L.1111-7 du code de la santé publique tend à protéger l'identité du tiers informateur. Dès lors, il conviendrait de limiter la restriction des « *informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique* » à la seule identité de ces tiers. A l'instar des documents administratifs comportant des informations non communicables, l'identité du tiers informateur pourrait simplement être occultée sans que le secret ne soit opposé au principal intéressé. En effet, les données personnelles concernant les tiers doivent rester inaccessibles au patient dans la mesure où

⁷⁵³ Article 2.2 du RGPD.

⁷⁵⁴ Article 14.3 a du RGPD.

⁷⁵⁵ Article 14.2 c du RGPD.

⁷⁵⁶ Article 14.2 f du RGPD.

⁷⁵⁷ *Ibid.*

elles ne lui sont pas personnelles. En d'autres termes, les informations personnelles ne seraient accessibles qu'à la personne concernée à laquelle se rapportent les données qui font l'objet du traitement⁷⁵⁸.

248. L'occultation de l'identité du tiers permettrait notamment de protéger la personne à l'origine de l'hospitalisation psychiatrique sous contrainte d'un malade souffrant de troubles mentaux. En effet, lorsque l'état de santé mentale d'une personne impose des soins immédiats, mais que ses troubles mentaux rendent le recueil de son consentement impossible, son hospitalisation peut être demandée par un tiers⁷⁵⁹, par le préfet⁷⁶⁰ ou par un médecin n'exerçant pas dans l'établissement accueillant le malade⁷⁶¹. Dans ce contexte, la cour administrative d'appel de Nantes a jugé que « *l'administration était légalement tenue de refuser à la personne hospitalisée la communication de tout élément permettant l'identification de l'auteur de la demande de placement volontaire* »⁷⁶². Dès lors, nous devons considérer que « *l'identité du tiers demandeur constitue une « information relative à un tiers », non communicable au patient qui en ferait la demande* »⁷⁶³. Assurément, la révélation de l'identité de la personne à l'origine d'une hospitalisation sous contrainte pourrait lui être préjudiciable.

249. Cependant, Sophie Theron s'interroge de savoir si le patient « *peut avoir connaissance d'éléments non strictement médicaux mais lui permettant de mieux appréhender la situation de contrainte dans les soins dans laquelle il se trouve, comme l'identité du tiers ou des éléments de son dossier administratif* »⁷⁶⁴. Cette question est pertinente depuis la systématisation et l'obligation du contrôle judiciaire des hospitalisations

⁷⁵⁸ CE, 10^e et 9^e ch., 07 juin 2017, n°399446, Rec. Lebon, T. ; ADJA, 2017, n° 30, p. 1697 ; JCP A, 2017, n° 41, comm. 2238, note A. Vinot-Landais ; JCP A, 2017, n° 24, act. 444, F. Tesson ; Revue Communication Commerce électronique, 2017, n° 10, comm. 84, N. Metallinos ; AJ fam., 2017, n° 09, p. 497, N. Levillain.

⁷⁵⁹ Article L.3212-3 du code de la santé publique.

⁷⁶⁰ Article L.3213-1 du code de la santé publique.

⁷⁶¹ Article L.3212-1 du code de la santé publique.

⁷⁶² CAA Nantes, 3^e ch., 07 octobre 1999, n°96NT01287, Rec. Lebon T., Gaz. Pal., 2001, n° 44, p. 33, note P. Graveleau.

⁷⁶³ LEUZZI-LOUCHARTE (C.), *Des dossiers médicaux au dossier hospitalier : la définition du dossier médical par la réglementation du contenu*, op. cit., p. 40.

⁷⁶⁴ THERON (S.), *Les soins psychiatriques sans consentement*, Paris, Dunod, 2017, p. 165 à p. 167.

sous contrainte. Depuis l'entrée en vigueur de la loi du 5 juillet 2011⁷⁶⁵, l'hospitalisation complète d'un patient faisant l'objet de soins sans consentement ne peut se poursuivre sans que le juge des libertés et de la détention n'ait statué publiquement, après débat contradictoire⁷⁶⁶. La copie de la demande d'admission formée par le tiers et faisant apparaître son identité peut-elle être communiquée au patient dès lors qu'elle est versée aux débats⁷⁶⁷ ?

A l'occasion d'un conseil délivré le 21 mai 2015, la CADA a rappelé que les pièces élaborées dans le cadre d'une hospitalisation sans consentement, bien qu'elles soient versées dans le dossier au juge, demeurent soumises aux dispositions juridiques entourant le droit d'accès aux documents administratifs. En conséquence, la CADA considère, de façon constante, que le patient hospitalisé sous contrainte ne peut accéder à la demande d'hospitalisation formulée par un tiers lorsque la révélation de son identité pourrait lui porter préjudice⁷⁶⁸. Dans ces conditions, qu'en est-il du respect du principe du contradictoire ? Ce principe pourrait être respecté par la communication de la pièce controversée à l'avocat du patient, dont l'assistance ou la représentation est obligatoire. Karine Sferlazzo-Boubli envisage que la communication de la demande à l'avocat soit assortie « *soit de l'interdiction de la communiquer à la personne faisant l'objet de soins, soit de la communiquer à cette dernière mais en occultant les éléments portant sur l'identité du tiers* »⁷⁶⁹. La première proposition formulée par l'auteur semble préférable. En effet, la demande d'hospitalisation rédigée par le tiers ne comporte que les nom, prénoms, date de naissance et domicile de la personne qui demande les soins et de celle pour laquelle ils sont demandés, ainsi que la nature des relations qui les unissent ou, le cas échéant, leur degré de parenté. L'accès à ce document aurait pour seul effet de porter à la connaissance du patient l'identité du tiers à l'origine de l'hospitalisation sous contrainte. L'absence de communication de ce document ne priverait donc pas le patient d'informations personnelles ou médicales le concernant.

⁷⁶⁵ Loi n° 2011-803 du 5 juillet 2011 relative aux droits et à la protection des personnes faisant l'objet de soins psychiatriques et aux modalités de leur prise en charge, *JORF* n°155, 6 juillet 2011, p. 11705.

⁷⁶⁶ Articles L.3211-12-1 et L.3211-12-2 du code de la santé publique.

⁷⁶⁷ Article R.3211-12 du code de la santé publique.

⁷⁶⁸ CADA, conseil n°20151096, 21 mai 2015 ; CADA, avis n°20164178, 17 novembre 2016.

⁷⁶⁹ SFERLAZZO-BOUBLI (K.), *Le respect du contradictoire l'emporte sur la protection du tiers demandeur d'une hospitalisation sans consentement*, RDS, 2016, n° 73, p. 818.

250. En outre, les libertés individuelles de la personne hospitalisée sous contrainte étant fortement restreintes, il est primordial de veiller à la protection de leur droit à l'information, qu'il soit exercé *a priori* ou *a posteriori*, directement ou par l'intermédiaire d'un médecin. Même si la personne concernée ne peut connaître l'identité de la personne à l'initiative de son hospitalisation, il est humainement essentiel qu'elle puisse en comprendre les raisons. A cet effet, l'accès du patient concerné à ses données médicales⁷⁷⁰ garantit les droits à l'information et à la transparence de leur traitement⁷⁷¹.

⁷⁷⁰ Article L.1111-7 du code de la santé publique ; Article 15 du RGPD.

⁷⁷¹ Articles 12, 13 et 14 du RGPD.

Conclusion du chapitre

251. Dans le contexte d'une prise en charge sanitaire, nul ne peut être privé du droit d'accéder aux éléments immatériels de son corps humain. Seules les modalités de l'accès à ces informations peuvent faire l'objet d'aménagements, dans l'unique intérêt de la personne concernée. Autrement dit, le droit d'accès à ses données médicales est un droit subjectif et fondamental dont l'exercice ne peut être tronqué. En effet, l'atteinte au droit d'accès aux données médicales formalisées dans les dossiers médicaux du patient reviendrait à le priver du droit fondamental à l'information médicale. Or, le patient étant le seul titulaire du secret médical, aucune information connexe à sa santé ne peut lui être dissimulée.

252. De surcroît, les données médicales du patient étant strictement confidentielles, elles ne sont, par principe, accessibles et communicables qu'à la personne concernée. Néanmoins, l'accessibilité des données formalisées dans les dossiers médicaux du patient est étendue aux professionnels qui concourent à sa prise en charge sanitaire. Assurément, la dispensation des services de soins de santé repose certes sur les données médicales recueillies et produites au cours de l'examen clinique⁷⁷², mais également sur l'historique médical généré au fil du parcours de santé de l'intéressé. Seulement, eu égard au principe de l'autodétermination informationnelle dévolu à la personne concernée, le patient bénéficierait théoriquement de la maîtrise du partage de ses données médicales entre les différents professionnels concourant à sa prise en charge sanitaire. En tant que titulaire de ses données médicales, « *le patient conserve [consécutivement] la maîtrise du secret professionnel médical imposé aux professionnels de santé et relatif aux informations le concernant* »⁷⁷³. Par conséquent, le patient semblerait décider de leur communication et de leur circulation dans le cadre de son parcours de santé. Le cas échéant, comment assurer la coordination et la continuité de ses soins ?

⁷⁷² Cf. Paragraphes 51 à 53.

⁷⁷³ SAINT MARTIN (A.), *Le secret médical et le patient (I) le patient (a priori) maître du secret professionnel médical*, op. cit., p. 109.

Chapitre 2 :

L'accès des professionnels aux données médicales du patient

« Le développement des nouvelles technologies de l'information et de la communication dans les domaines sanitaire et médico-social ainsi que des modes d'exercice pluridisciplinaire accroissent le besoin d'échange dans l'intérêt d'une meilleure prise en charge des personnes. Les données de santé et les données médico-sociales sont aujourd'hui des données destinées à être partagées, même si elles relèvent de la vie privée de la personne. »⁷⁷⁴.

253. Compte tenu de l'évolution de la relation médicale bilatérale vers un mode de prise en charge multipartite, le législateur a élargi le champ des dépositaires du secret professionnel médical⁷⁷⁵. Ainsi, les professionnels concourant à la prise en charge sanitaire du patient peuvent échanger et partager ses données médicales (**Section 1**). Seulement, cette faculté légale tend à se systématiser en raison de la surspécialisation de l'offre de soins et de leur décloisonnement. La prise en charge d'une pathologie peut requérir l'intervention de professionnels appartenant à des spécialités, des catégories et des secteurs différents. La circulation des données médicales du patient apparaît alors comme une nécessité pour la coordination de son parcours de santé et la continuité de sa prise en charge sanitaire.

254. Si la communication des données médicales du patient est facilitée par le déploiement des dispositifs de santé numérique et par l'instauration du DMP, le patient demeure à leur commande et peut faire obstacle à leur circulation. En vertu du principe de l'autodétermination informationnelle, le patient jouit relativement de la maîtrise et du contrôle des informations qui le concernent. Cela signifie que le patient, en sa qualité de personne concernée, peut partiellement décider de l'usage de ses données médicales. Dans certains cas, le patient peut donc s'opposer à leur communication entre les professionnels intervenant dans son parcours de santé. Pourtant, comme le souligne Maître Jeanne Bossi-Malafosse, la transmission de ses informations médicales apparaît comme une condition essentielle à la dispensation des soins. En conséquence, il semble inéluctable de

⁷⁷⁴ BOSSI-MALAFOSSE (J.), *Le cadre juridique du partage d'informations dans les domaines sanitaire et médico-social : état des lieux et perspectives*, Médecine & Droit, janvier - février 2013, p. 5.

⁷⁷⁵ Article 95 de la loi n°2016-41 du 26 janvier 2016, *op. cit.*

responsabiliser le patient dans l'exercice des droits qu'il détient sur ses données médicales lorsqu'elles sont traitées aux fins de sa prise en charge sanitaire (**Section 2**).

Section 1 : L'échange et le partage des données médicales du patient

255. Le secret professionnel médical est commun aux acteurs qui participent directement à la prise en charge sanitaire d'un même patient. Cependant, l'échange et le partage des données médicales du patient entre ces professionnels ne sont pas libres. En effet, la communication de ces informations médicales correspond à un traitement de données personnelles. Par conséquent, la mise en œuvre de ce traitement est soumise aux règles de droit commun édictées par le RGPD ainsi qu'aux dispositions particulières du code de la santé publique (**Paragraphe 1**). De surcroît, l'échange et le partage des données médicales du patient sont conditionnés par l'exercice de ses droits au consentement et à l'opposition à leur communication (**Paragraphe 2**).

Paragraphe 1 : Les conditions d'échange et de partage des données médicales entre les professionnels concourant à la prise en charge du patient

256. Préalablement à la communication des informations médicales du patient, les professionnels doivent s'assurer qu'ils participent effectivement à sa prise en charge sanitaire ou médico-sociale (**A**). Le cas échéant, les professionnels ne peuvent accéder, dans les limites du périmètre de leurs missions, qu'aux seules informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention, ou au suivi médico-social du patient (**B**). Force est de constater que le traitement des données médicales du patient, consistant en la transmission des informations couvertes par le secret, est scrupuleusement encadré par leur minimisation, la détermination des finalités de leur traitement et la restriction des destinataires autorisés à en connaître.

A) La participation du professionnel à la prise en charge du patient

257. Comme l'indique Sylvie Hennion, « *le développement de la spécialisation des professions médicales ou médico-sociales conduit à devoir faire appel à plusieurs professionnels pour traiter un même patient et à devoir partager l'information médicale,*

sanitaire et sociale relative à ce dernier »⁷⁷⁶. Depuis les années 2000⁷⁷⁷, les prises en charge sont plurielles, pluridisciplinaires, collectives et collaboratives. Dès lors, la circulation de l'information médicale, sanitaire et sociale du patient entre les professionnels apparaît comme une nécessité. Il ne fait aucun doute que « *dans un système de santé où l'offre médicale se spécialise et se fragmente, le partage des données relatives au patient est devenu un enjeu de continuité et de qualité des soins* »⁷⁷⁸. La communication des données médicales d'un patient entre plusieurs professionnels de catégories ou de secteurs différents est devenue un impératif lié à la globalisation des prises en charge sanitaires et sociales. En conséquence, le Premier ministre Jean-Marc Ayrault avait affirmé la nécessité de créer « *une médecine de parcours* » reposant sur la coopération des professionnels⁷⁷⁹ au-delà des clivages sectoriels public et privé, ville et hôpital, et sanitaire, médico-social et social. Cette ambition a été consacrée par l'adoption de la « loi Santé » de 2016⁷⁸⁰ ayant promu la circulation des informations personnelles du patient entre les professionnels du champ sanitaire et ceux des champs médico-social et social, conjointement à la relance du Dossier Médical devenu Partagé. Le décroisement et la coordination des prises en charge sanitaires et sociales ont donc été impulsés par l'autorisation de communiquer des informations relatives à la personne prise en charge entre les professionnels concourant à la continuité de ses soins ou à son suivi médico-social ou social.

258. Désormais, les dispositions de l'article L.1110-4 du code de la santé publique mentionnent que le dossier médical d'un patient peut être partagé entre les professionnels concourant directement à sa prise en charge. Egalement, les informations contenues dans ce dossier peuvent en être extraites afin d'être échangées entre ces mêmes professionnels. Ainsi, la première des conditions de l'accès des professionnels, aux données médicales du patient, réside dans leur participation à sa prise en charge sanitaire, médico-sociale ou sociale. En

⁷⁷⁶ HENNION (S.), *Le partage du secret professionnel à l'ère du numérique*, RDSS, 2020, n°01, p. 130.

⁷⁷⁷ « *Le parcours de soins coordonnés, institué par la loi du 13 août 2004, a pour objectifs de faire bénéficier chaque usager d'un suivi médical coordonné, d'une gestion rigoureuse du dossier médical et d'une prévention personnalisée.* ». Ministère des solidarités et de la santé, *Qu'est-ce que le parcours de soins ?*, Disponible en ligne sur [<https://solidarites-sante.gouv.fr>]. Consulté le 29 décembre 2020.

⁷⁷⁸ Commentaire sous article L.1110-4 du code de la santé publique, ed. Dalloz.

⁷⁷⁹ Discours de Jean-Marc Ayrault, Premier ministre, Stratégie nationale de santé, Grenoble, Vendredi 8 février 2013.

⁷⁸⁰ Article 96 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022, 27 janvier 2016.

effet, Sylvie Hennion affirme que « *la prise en charge constitue la première condition pivot dans les dispositions législatives pour que des professionnels puissent partager des informations à caractère secret* »⁷⁸¹. Les acteurs pouvant obtenir la communication des données médicales du patient peuvent donc appartenir à des catégories professionnelles distinctes dès lors qu'ils concourent effectivement au parcours de santé du patient.

259. Bien que la « loi Santé » de 2016 ait favorisé la circulation des informations médicales entre les professionnels participant à la prise en charge d'un même patient, tous ne peuvent y accéder. Effectivement, seuls les professionnels appartenant aux catégories exhaustivement énumérées à l'article R.1110-2 du code de la santé publique sont susceptibles d'échanger ou de partager les données médicales relatives à la personne qu'ils prennent en charge sur un plan sanitaire, médico-social ou social.

260. En premier lieu, les données médicales du patient peuvent circuler entre l'ensemble des professionnels de santé. Cette catégorie regroupe les médecins, les chirurgiens-dentistes, les sage-femmes, les pharmaciens, les préparateurs en pharmacie, les physiciens médicaux, les aides-soignants, les auxiliaires de puériculture, les ambulanciers, les assistants dentaires, les infirmiers, les masseurs-kinésithérapeutes, les pédicures podologues, les ergothérapeutes, les psychomotriciens, les orthophonistes, les orthoptistes, les manipulateurs d'électroradiologie médicale, les techniciens de laboratoire médical, les audioprothésistes, les opticiens-lunetiers, les prothésistes et orthésistes pour l'appareillage des personnes handicapées ainsi que les diététiciens.

261. En deuxième lieu, les données médicales d'un patient peuvent être communiquées à des *non-professionnels de santé* dont les sous-catégories professionnelles sont énumérées à l'article R.1110-2 du code de la santé publique. Sont ainsi autorisées à échanger ou partager les données de santé du patient les personnes appartenant aux sous-catégories des assistants de service social, des ostéopathes, des chiropracteurs, des psychologues et psychothérapeutes, des aides médico-psychologiques et accompagnants éducatifs et sociaux, des assistants maternels et assistants familiaux, des éducateurs et aides familiaux, des personnels pédagogiques occasionnels des accueils collectifs de mineurs ou permanents des

⁷⁸¹ HENNION (S.), *loc. cit.*

lieux de vie, des particuliers accueillant des personnes âgées ou handicapées, des mandataires judiciaires à la protection des majeurs et délégués aux prestations, des non-professionnels de santé salariés des établissements et services et lieux de vie et d'accueil mentionnés aux articles L.312-1, L.321-1 et L.322-1 du code de l'action sociale et des familles, ou y exerçant à titre libéral en vertu d'une convention, des non-professionnels de santé mettant en œuvre la méthode prévue à l'article L.113-3 du code susvisé pour la prise en charge d'une personne âgée en perte d'autonomie, les non-professionnels de santé membres de l'équipe médico-sociale compétente pour l'instruction des demandes d'allocation personnalisée d'autonomie ou contribuant à cette instruction en vertu d'une convention, les personnels des dispositifs d'appui à la coordination des parcours de santé complexes, ainsi que les étudiants en troisième cycle des études de santé.

262. Sans conteste, la liste des personnes pouvant accéder aux données médicales d'un patient est extrêmement précise, explicitement encadrée et parfaitement circonscrite. Si pour certains auteurs, la liste des catégories de professionnels pouvant accéder aux informations médicales du patient semble extensive, cette énumération nous paraît restrictive dans le cadre d'un parcours sanitaire et social globalisé. En effet, qu'en est-il lorsque le professionnel qui participe directement et effectivement à la prise en charge de la personne concernée n'est pas mentionné au sein de la liste des professionnels pouvant échanger ou partager des informations relatives à la personne concernée ?

En réalité, la première condition à la communication des données médicales du patient réside dans l'inscription du destinataire sur l'inventaire de l'article R.1110-2 du code de la santé publique. L'effectivité d'une prise en charge directe au profit de la personne concernée constitue donc une condition cumulative de seconde position. Par conséquent, il advient l'impossibilité de communiquer des informations médicales à un professionnel ne figurant pas sur ledit inventaire, quand bien même il participerait à la prise en charge sanitaire, médico-sociale ou sociale du patient. A titre d'exemple, les prothésistes dentaires n'appartiennent pas aux catégories visées à l'article R.1110-2 du code de la santé publique. Cela signifie qu'en principe, les chirurgiens-dentistes ne peuvent communiquer des informations médicales nominatives relatives aux patients requérant une prothèse dentaire aux professionnels chargés de les fabriquer. Seulement, comment réaliser une prothèse dentaire sans les empreintes du patient prises par le chirurgien-dentiste ? L'exercice de la profession de prothésiste dentaire repose indispensablement sur les données médicales

transmises par le chirurgien-dentiste. En dépit des usages, il semblerait donc que l'échange d'informations entre ces deux protagonistes ne soit pas juridiquement autorisé, ce dernier ne relevant pas des catégories susmentionnées. Dès lors, l'échange d'informations médicales entre ces deux professionnels constitue-t-il une violation du secret professionnel médical par le chirurgien-dentiste ?

263. La condition de l'appartenance du destinataire de l'information médicale aux catégories listées à l'article R.1110-2 du code de la santé publique s'avère inopportune eu égard aux écueils qu'elle comporte. En effet, toute prise en charge sanitaire et sociale étant singulière, il est hasardeux de prédire dans le marbre les seules catégories de professionnels autorisées à accéder aux informations médicales de la personne concernée, *a fortiori* lorsque des professions du champ de la santé ont été oubliées par le législateur.

Compte tenu de ce qui précède, la condition du concours du professionnel à la prise en charge effective du patient devrait suffire à autoriser la communication de ses données médicales. Toutefois, seul le législateur peut soumettre une catégorie de professionnels à un secret⁷⁸². Il en advient que si les professionnels intervenant à la prise en charge sanitaire ou sociale du patient ne sont pas légalement investis d'un secret professionnel, ceux qui y sont effectivement soumis ne peuvent leur communiquer les données médicales du patient. En ce sens, l'article 9.2 h) du RGPD autorise la communication des données médicales de la personne concernée lorsque ce traitement est nécessaire aux fins de sa « *prise en charge sanitaire ou sociale* » et qu'il est effectué par un professionnel de la santé soumis à une obligation de secret professionnel, ou par une autre personne également soumise à une obligation de secret⁷⁸³. En lieu et place de la liste restrictive de l'article R.1110-2 du code de la santé publique, ne serait-il pas opportun que le législateur vise l'ensemble des professionnels concourant à la prise en charge sanitaire et sociale du patient dans le cadre d'un parcours de santé coordonné ? Ainsi, les professionnels dépositaires d'un même secret pourraient échanger et partager des informations relatives à la personne dont ils concourent effectivement au parcours de santé sans qu'ils ne soient limitativement énumérés par des dispositions réglementaires. Dans cette hypothèse, la communication d'informations entre

⁷⁸² Cf. Paragraphe 555.

⁷⁸³ Article 9.3 du RGPD.

des professionnels n'étant pas inscrits sur cet inventaire réglementaire ne constituerait plus une violation du secret professionnel sanctionnée à l'article 226-13 du code pénal.

264. La communication des données médicales entre les professionnels participant directement à la prise en charge du patient est largement facilitée lorsqu'ils sont membres de la même équipe de soins. Le cas échéant, les « *informations sont réputées confiées par la personne à l'ensemble de l'équipe* »⁷⁸⁴. Cette présomption se révèle indispensable dans la mesure où « *le secret partagé est emblématique du caractère relatif du secret professionnel, sans lequel aucune équipe de soin n'existerait* »⁷⁸⁵. Afin de favoriser ce partage, le législateur a retenu une approche extensive de la notion d'équipe de soins.

Les dispositions de l'article L.1110-12 du code de la santé publique définissent l'équipe de soins comme « *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* ». Aussi, ces professionnels doivent exercer au sein d'une même structure. Il peut s'agir d'un établissement de santé ou médico-social, d'une structure de coopération telle qu'un groupement hospitalier de territoire, ou encore une structure d'exercice partagé ou de coordination sanitaire ou médico-sociale telle qu'une maison ou un centre de santé. S'ils n'exercent pas au sein d'une même structure, les professionnels peuvent être intégrés dans l'équipe de soins s'ils ont été choisis par le patient pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge. Egalement, les professionnels peuvent devenir membre de l'équipe de soins s'ils exercent dans une organisation formalisée comprenant au moins un professionnel de santé. Les membres d'une équipe de soins peuvent ainsi appartenir à différentes catégories professionnelles et être rattachés à des entités juridiques distinctes. Pour chaque patient, la composition d'une équipe de soins est évolutive tout au long de son parcours de santé. En ce sens, Sylvie Hennion explique que le législateur n'a pas limité la définition de l'équipe de soins à son sens purement médical ou paramédical. Effectivement, la notion d'équipe de soins est étendue à tout type

⁷⁸⁴ Article L.1110-4 III du code de la santé publique.

⁷⁸⁵ ZORN-MACREZ (C.), "Chronique martienne" des données de santé numérisées. Brèves observations sur une réglementation surréaliste, RDS, 2010, n° 36, p. 333.

de service ayant pour objet le bien-être sanitaire du patient au sens de la définition de l'OMS⁷⁸⁶. Les dispositions législatives permettent donc le décloisonnement et la coordination des prises en charge globalisées et multisectorielles.

265. De surcroît, la communication des données médicales du patient est particulièrement favorisée par la mise en œuvre du DMP. Au regard de l'intitulé de ce dispositif, l'objectif de ce dossier médical numérique est d'être *partagé*. Les pouvoirs publics ont alors refondé le DMP comme un « *outil d'aide à la coordination des soins* »⁷⁸⁷. En effet, une prise en charge coordonnée suppose la transmission des données médicales du patient entre les professionnels qui y sont impliqués. Jeanne Capodano a remarqué que « *la création du nouveau DMP s'inscrit dans une réforme majeure du secret professionnel opérée par la loi Santé, qui élargit considérablement les possibilités de partage d'informations* »⁷⁸⁸. Tandis que l'émergence du DMP a été concomitante à l'élargissement des contours du *secret médical partagé* aux *non-professionnels de santé*, l'accès à ce dossier numérique a longtemps été réservé aux seuls professionnels de santé. Il aura fallu attendre l'adoption de la loi ASAP⁷⁸⁹ pour que les professionnels appartenant aux champs médico-social et social, inscrits sur l'inventaire de l'article R.1110-2 du code de la santé publique, soient autorisés à accéder à ce dispositif. Désormais, le DMP permet aux professionnels exerçant dans des secteurs et des structures différentes, et appartenant à des catégories professionnelles distinctes, de partager et d'accéder aux informations concernant le patient qu'ils prennent effectivement et directement en charge. En tant qu'outil numérique, le DMP apparaît donc comme un vecteur de circulation de l'information médicale, au-delà des frontières dressées par le secteur de prise en charge, dans le cadre d'un parcours de santé globalisé et coordonné.

B) La minimisation des données médicales échangées ou partagées

266. Lorsqu'il est avéré que les professionnels participent effectivement et directement à la prise en charge sanitaire ou sociale du patient, ces derniers peuvent obtenir la

⁷⁸⁶ HENNION (S.), *loc. cit.*

⁷⁸⁷ Etude d'impact du projet de loi relatif à la santé, 14 octobre 2014, p. 99.

⁷⁸⁸ CAPODANO (J.), *Dossier médical partagé (DMP) et secret professionnel : les nouveaux enjeux*, RDS, 2017, n°76, p. 233.

⁷⁸⁹ Loi n° 2020-1525 du 7 décembre 2020, *loc. cit.*

communication des données médicales de la personne concernée. Cependant, le législateur circonscrit cette communication aux seules informations strictement nécessaires à la coordination ou à la continuité des soins, ou au suivi médico-social et social de la personne prise en charge⁷⁹⁰. La minimisation des données médicales échangées ou partagées constitue donc la seconde condition préalable à leur circulation. Plus précisément, les dispositions de l'article R.1110-1 du code de la santé publique cantonnent la communication des données médicales du patient à une double limite.

267. En premier lieu, les dispositions réglementaires rappellent que seules les « *informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention, ou au suivi médico-social et social* »⁷⁹¹ du patient peuvent être communiquées. Cette condition fait écho à l'article 5.1 c) du RGPD selon lequel les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire à la finalité du traitement. En pratique, ce principe de nécessité constitue une condition subjective difficile à interpréter. Par définition, est nécessaire ce « *dont la présence ou l'action rend seule possible une fin* »⁷⁹². En d'autres termes, est « nécessaire » ce qui est indispensable à une finalité. En théorie, seules les informations indispensables et essentielles à la coordination et à la continuité de la prise en charge sanitaire, médico-sociale et sociale du patient peuvent être échangées ou partagées. Seulement, Sylvie Hennion considère qu'en pratique « *la stricte nécessité s'apprécie toujours en fonction de l'intérêt de la personne prise en charge et en fonction de la nature de cette prise en charge* »⁷⁹³. En effet, les informations à communiquer aux professionnels doivent être déterminées en fonction de la situation propre à chaque patient. Certainement, la Caisse nationale de solidarité pour l'autonomie et l'Agence française de la santé numérique rappellent qu'« *il n'existe pas de liste réglementaire recensant les informations pertinentes car elles varient en fonction de la situation dans laquelle se trouve la personne prise en charge* »⁷⁹⁴. Il appartient donc au professionnel de discerner, pour

⁷⁹⁰ Article L.1110-4 du code de la santé publique.

⁷⁹¹ Article R.1110-1 1° du code de la santé publique.

⁷⁹² Définition du dictionnaire Larousse. Disponible en ligne sur le site [<https://www.larousse.fr>]. Consulté le 10 juin 2020.

⁷⁹³ HENNION (S.), *op. cit.*, p. 134.

⁷⁹⁴ CNSA, ASIP Santé, *Échange et partage des données de santé, Retour d'expérience des bonnes pratiques sur l'échange et le partage des données*, novembre 2018, p. 9. Disponible en ligne sur le site [www.esante.gouv.fr]. Consulté le 03 décembre 2021.

chaque cas, les informations devant être nécessairement échangées ou partagées aux fins de la coordination ou de la continuité de la prise en charge du patient.

Si pour Bruno Py « *il va de soi que les informations sans lien utile avec la démarche médicale doivent rester absolument secrètes* »⁷⁹⁵, cette évidence n'est pas aussi limpide dans le cadre d'une prise en charge sanitaire. La moindre donnée médicale générée à l'occasion d'un acte, d'une consultation ou d'une hospitalisation peut s'avérer nécessaire à la coordination ou à la continuité des soins. Assurément, il peut exister une corrélation entre une information médicale collectée à un moment donné et une pathologie déclarée ultérieurement. Toute information médicale est, par conséquent, potentiellement nécessaire à la coordination et à la continuité du parcours de santé. Opérer un tri dans les informations médicales à transmettre apparaît donc périlleux. La condition de la nécessité de la communication étant particulièrement extensive, le législateur a imposé une deuxième limite à l'échange et au partage des informations médicales.

268. En deuxième lieu, les dispositions réglementaires énoncent que les professionnels participant à la prise en charge du patient peuvent échanger ou partager des informations dans la limite du périmètre de leurs missions. Le respect de cette double limite ne pose pas de difficultés dans l'hypothèse d'un *échange* d'informations médicales. Que l'échange soit réalisé au moyen d'un outil numérique ou d'un support papier, le professionnel dispose du contrôle des éléments communiqués à un destinataire identifié. Partant, le professionnel qui échange des données médicales avec un homologue identifié doit s'assurer que ces informations médicales sont effectivement utiles à la coordination ou à la continuité de la prise en charge médicale et correspondent au périmètre des missions de leur destinataire. Les informations échangées entre professionnels doivent alors être ciblées et cohérentes au regard des compétences et de la mission de chaque intervenant.

269. En revanche, si Lydia Morlet-Haïdara estime que « *cette précision est heureuse en ce qu'elle tend à limiter les abus de partage des données des personnes prises en charge* »⁷⁹⁶, le respect de la double limite instituée à l'article R.1110-1 du code de la santé publique semble

⁷⁹⁵ PY (B.), *Secret professionnel*, Répertoire de droit pénal et de procédure pénale, 2003, actu. 2017, § 161.

⁷⁹⁶ MORLET-HAÏDARA (L.), *Le nouveau cadre légal de l'équipe de soins et du partage des données du patient*, RDSS, 2016, n°06, p. 1104.

davantage épineux en cas de *partage* de données médicales. En effet, le partage consiste en la mise à disposition du dossier médical du patient, numérique ou manuscrit, aux professionnels intervenant à sa prise en charge. En d'autres termes, le partage des données médicales du patient ne repose pas sur l'envoi d'un document d'un expéditeur vers un destinataire. Dès lors, comment s'assurer du respect des conditions érigées par l'article susvisé, *a fortiori* lorsque les données médicales sont partagées au moyen d'un support accessible à une pluralité de professionnels ? Dans cette hypothèse, il revient au professionnel concerné d'auto-limiter son accès. Celui-ci doit veiller à accéder aux seules informations nécessaires à la coordination ou à la continuité de la prise en charge du patient en fonction de ses missions. A titre d'exemple, l'infirmier exerçant dans un service de rhumatologie ne doit pas accéder aux informations collectées par le service de gastro-entérologie lorsque ces informations ne sont ni pertinentes, ni adéquates, ni nécessaires au périmètre de son concours à la prise en charge médicale du patient. A défaut, cet accès illicite serait constitutif d'une violation du secret professionnel médical imputable à celui qui prendrait intentionnellement connaissance de ces données confidentielles non minimisées. A l'occasion du partage d'informations médicales, le respect des conditions détaillées ci-avant repose donc exclusivement sur la bonne foi du professionnel ayant accès au dossier médical du patient. L'appréciation du principe de minimisation des données partagées incombe donc aux professionnels des champs sanitaire, médico-social et social.

270. A l'ère des dossiers médicaux informatisés, le respect de ces conditions pourrait être garanti grâce à la traçabilité des accès de tout professionnel au support numérique. Pour Sylvie Hennion, il est essentiel que l'accès aux fichiers communs soit individualisé en fonction de l'objet précis de la tâche de chaque intervenant⁷⁹⁷. L'auteur s'appuie notamment sur les recommandations du CNOM qui préconisent « *des filtrages informatiques avec différents niveaux de faculté de lecture du dossier mais avec une traçabilité complète des démarches ou actes effectués* »⁷⁹⁸. Toutefois, le paramétrage des accès au dossier médical informatisé, en fonction de la qualité et des missions des professionnels, est propre à chaque établissement de santé ou médico-social. Bien que la sécurité des systèmes d'information

⁷⁹⁷ HENNION (S.), *op. cit.*, p. 135.

⁷⁹⁸ CNOM, *Échange et partage d'information au sein de l'équipe de soins prenant en charge une personne*, Recommandations, février 2017. Disponible en ligne sur le site [www.conseil-national.medecin.fr]. Consulté le 03 décembre 2021.

hospitaliers doit être conforme aux référentiels élaborés par l'Agence du numérique en santé⁷⁹⁹, l'attribution et la gestion des habilitations constituent des actes fonctionnels approuvés discrétionnairement par le responsable de traitement⁸⁰⁰. Elles peuvent donc différer d'une structure de santé à l'autre. En conséquence, la solution proposée par le CNOM peut apparaître hétérogène lorsque les professionnels n'exercent pas au sein du même établissement.

271. Si le paramétrage de l'accès au dossier médical du patient dépend de chaque structure l'ayant constitué, le partage des informations contenues dans le DMP est déterminé universellement par les pouvoirs publics. En effet, les professionnels participant à la coordination des soins du patient « *ont accès aux seules données strictement nécessaires à la prise en charge du titulaire du dossier médical partagé dans le respect des règles de gestion des droits d'accès fixées par un arrêté du ministre chargé de la santé* »⁸⁰¹. La gestion de ces accès intervient automatiquement *via* l'association informatique entre l'authentification du professionnel et l'habilitation qui lui est attribuée. Les professionnels autorisés à accéder au DMP ne peuvent donc pas prendre connaissance de l'intégralité des données médicales qu'il contient. Cette matrice des habilitations permet de garantir la conformité du partage des données médicales au moyen du DMP aux conditions légales et réglementaires relatives à la minimisation des données personnelles. En conséquence, la protection des données médicales confidentielles, originairement couvertes par un secret bilatéral, semble assurée. En outre, tout accès et toute action effectués sur un DMP sont tracés et répertoriés⁸⁰². Ainsi, le titulaire du DMP peut, à tout moment, prendre connaissance des traces d'accès à son dossier et veiller au respect des conditions de partage de ses données médicales. A défaut, « *tout accès en dehors des règles précitées est passible d'une peine d'emprisonnement et d'une amende, conformément au droit pénal* »⁸⁰³.

⁷⁹⁹ Voir : ASIP Santé, *Guide Gestion des habilitations d'accès au SI*, Politique générale de sécurité des systèmes d'information de santé (PGSSI-S), V. 1.0, janvier 2017. Disponible en ligne sur le site [www.esante.gouv.fr]. Consulté le 03 décembre 2021.

⁸⁰⁰ *Ibid.*

⁸⁰¹ Article R.1111-46 alinéa 6 du code de la santé publique.

⁸⁰² Article R.1111-43 du code de la santé publique.

⁸⁰³ Caisse nationale de l'assurance maladie, *Matrice d'habilitations des professionnels de santé*, V.2.5.0, septembre 2021. Disponible en ligne sur le site [https://www.dmp.fr]. Consulté le 11 juin 2020.

272. Alors que les conditions de communication des informations médicales ne posent pas de difficultés dans le cadre de leur échange, les conditions de leur partage devraient être détaillées dans un référentiel applicable, de façon uniforme et homogène, à tout système d'information médical. Dans l'hypothèse où le paramétrage du partage bloquerait l'accès des professionnels à des données pourtant nécessaires à la coordination de la prise en charge du patient, « *les autres communications pourront leur être transmises par la voie des échanges sous la responsabilité du médecin ou du professionnel de santé qui les détient* »⁸⁰⁴. S'il est indispensable de préserver la confidentialité des données médicales et de protéger le droit au respect de la vie privée de la personne concernée, il semble impérieux de faciliter l'accomplissement des missions des professionnels intervenant dans un parcours de santé coordonné et globalisé.

Paragraphe 2 : Les droits du patient sur ses données médicales à l'aune du secret médical

273. Si le législateur autorise la communication des données médicales entre les professionnels participant à la prise en charge sanitaire et sociale du patient, ce dernier en maîtrise l'échange et le partage (A). D'une part, en tant que titulaire du secret médical, le patient peut opposer le caractère confidentiel des informations qui lui sont personnelles. D'autre part, en tant que personne concernée par le traitement de ses données personnelles, le patient jouit, à leur égard, de droits qui lui confèrent une autodétermination informationnelle⁸⁰⁵. Ainsi, le patient peut théoriquement empêcher la transmission de ses données médicales. Néanmoins, la circulation des données médicales du patient constitue une nécessité pour sa prise en charge sanitaire et sociale. C'est pourquoi le législateur l'a,

⁸⁰⁴ CNOM, *Échange et partage d'information au sein de l'équipe de soins prenant en charge une personne*, loc. cit.

⁸⁰⁵ Cf. Paragraphe 32.

dans certains cas, obligée. La maîtrise de la circulation des données médicales par le patient comporte donc des limitations **(B)**.

A) *La maîtrise de la communication des données médicales par le patient*

274. Au cours de la prise en charge du patient, le professionnel de santé peut être amené à communiquer ses données médicales avec des professionnels du champ sanitaire ou social. Préalablement à cette opération de traitement, le patient doit en être informé et les droits qu'il détient sur ses données doivent lui être indiqués. Toutefois, les droits que le patient dispose à l'égard de ses données médicales dépendent de la nature de la communication envisagée. En effet, le patient ne bénéficie pas des mêmes droits selon qu'il s'agisse d'une opération d'échange ou d'une opération de partage et que les professionnels appartiennent, ou non, à la même équipe de soins ou à des catégories professionnelles différentes. La détermination des droits du patient quant à la communication de ses données médicales entre professionnels suppose de distinguer leur échange **(1)** de leur partage **(2)**.

1. *La maîtrise de l'échange des données médicales par le patient*

275. Le traitement consistant en un *échange* de données peut être défini comme la transmission d'une information d'un expéditeur vers un destinataire. En d'autres termes, « *l'échange d'informations se définit comme la « communication d'informations à un ou plusieurs destinataires clairement identifiés par un émetteur connu »* »⁸⁰⁶. C'est ainsi que le législateur admet qu'un professionnel puisse échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge⁸⁰⁷.

276. Préalablement à la mise en œuvre de cet échange, le patient doit en être informé. En effet, l'information relative au traitement des données représente le premier droit de la personne concernée. Toutefois, dans le cadre de la prise en charge sanitaire et sociale du patient, les dispositions normatives n'envisagent que l'information préalable à un échange de données entre professionnels appartenant à des catégories professionnelles différentes. En

⁸⁰⁶ BUCKI (E.), CASANOVAS (G.), LANGARD (S.), *Les règles d'échange et de partage d'informations : aux limites de la démarche empirique*, RDS, 2017, n° 79, p. 659.

⁸⁰⁷ Article L.1110-4 II du code de la santé publique.

effet, l'article R.1110-3 du code de la santé publique précise que le professionnel « *souhaitant échanger des informations relatives à une personne prise en charge [...] avec un professionnel relevant de l'autre catégorie, informe préalablement la personne concernée, d'une part, de la nature des informations devant faire l'objet de l'échange, d'autre part, soit de l'identité du destinataire et de la catégorie dont il relève, soit de sa qualité au sein d'une structure précisément définie* ». La doctrine juridique constate alors qu'« *en cas d'échange mixte (d'une catégorie vers l'autre), une obligation d'information renforcée pèse sur le professionnel concerné* »⁸⁰⁸. Seulement, qu'en est-il de l'information préalable à un échange de données entre professionnels relevant de la même catégorie professionnelle ?

Il apparaît que le législateur l'a passée sous silence. Pourtant, tout responsable de traitement a l'obligation d'informer la personne concernée par le traitement de ses données personnelles. Par conséquent, cette obligation d'information pèse sur le responsable de traitement, peu importe que les données médicales soient échangées entre professionnels appartenant, ou non, à des catégories différentes. Effectivement, l'article 13 du RGPD impose que la personne concernée soit notamment informée des finalités du traitement auquel sont destinées ses données personnelles, de leurs destinataires, ou des catégories de destinataires auxquelles elles seront communiquées. Le RGPD ayant une portée générale, il en résulte que tout patient doit toujours être informé de la nature des données échangées ainsi que de l'identité du professionnel destinataire ou, à défaut, de la catégorie dont il relève. Dès lors, le code de la santé publique ne devrait pas distinguer le périmètre de l'information due à la personne concernée par l'échange de ses données médicales en fonction de la mixité de cet échange. Qu'il soit effectué entre professionnels appartenant à une même catégorie professionnelle, ou entre professionnels relevant de catégories différentes, le patient a le droit de connaître l'identité du professionnel à qui ses données médicales seront transmises. A l'évidence, le droit à l'information du patient quant à l'échange de ses données médicales ne peut être conditionné par la catégorie professionnelle de leur récepteur.

277. De surcroît, la délivrance d'une information relative au traitement des données personnelles de la personne concernée est indispensable à l'exercice des droits qui lui sont reconnus à leur égard. En effet, toute personne concernée ne peut, de façon éclairée, consentir

⁸⁰⁸ BUCKI (E.), CASANOVAS (G.), LANGARD (S.), *loc. cit.*

ou s'opposer à la mise en œuvre d'un traitement qu'à la condition d'en connaître les détails. C'est pourquoi le législateur européen a établi une hiérarchie dans la délivrance des éléments d'information relatifs au traitement des données personnelles. L'article 13 du RGPD prévoit qu'après avoir informé la personne concernée des modalités du traitement, le responsable de traitement doit lui fournir les informations complémentaires relatives à l'exercice de ses droits. En effet, la personne concernée par le traitement de ses données personnelles doit connaître les particularités du traitement pour décider de l'activation de ses prérogatives sur les informations qui la concernent.

278. Dans le cadre d'un échange de données médicales, le patient jouit du droit de s'opposer à cette opération de traitement. En effet, l'article L.1110-4 du code de la santé publique dispose que « *la personne est dûment informée de son droit d'exercer une opposition à l'échange [...] d'informations la concernant. Elle peut exercer ce droit à tout moment.* ». Il appartient donc au professionnel de santé, expéditeur des données médicales, d'informer le patient du droit de s'opposer à cet échange. Le droit à l'opposition du traitement dépend donc de la transparence de l'information délivrée au patient : ce dernier ne peut valablement exercer son droit que s'il a connaissance du contenu des données envoyées à un récepteur identifié. Alors que le patient peut maîtriser l'échange de ses données médicales par le biais de son droit d'opposition, l'effectivité de cette autodétermination dépend exclusivement de la délivrance d'une information effective et préalable à ce traitement. En ce sens, certains auteurs ont souligné que « *le droit d'opposition du patient est assuré par l'information préalable de l'identité des professionnels concernés* »⁸⁰⁹. Certainement, la seule information de l'existence d'un droit d'opposition à l'échange des données médicales ne suffit pas à en assurer l'efficacité.

279. Par ailleurs, il convient de préciser que le patient jouit d'un droit d'opposition et non d'un droit au consentement à l'échange de ses données médicales. Si le professionnel expéditeur a l'obligation d'informer le patient de ce traitement, il n'a pas à recueillir son assentiment. Il en résulte que la base légale de l'échange des données médicales du patient ne repose pas sur le consentement de la personne concernée. En effet, la communication de données ayant pour finalité la coordination et la continuité des soins du patient repose sur

⁸⁰⁹ *Ibid.*

l'accomplissement des missions des professionnels concourant à sa prise en charge sanitaire ou sociale⁸¹⁰. Ainsi, le traitement consistant en l'échange des données médicales répond à une mission d'intérêt public dont le responsable de traitement est investi lorsque le patient est pris en charge en secteur public⁸¹¹, et aux intérêts légitimes poursuivis par le responsable de traitement lorsque le patient est pris en charge en secteur privé⁸¹². Lorsque le traitement est fondé sur l'une de ces deux bases légales, alors « *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* »⁸¹³. Même si l'échange des données de santé entre professionnels ne requiert pas le consentement du patient, le patient peut valablement s'opposer à cet échange à tout moment. Le patient maîtrise donc l'échange de ses données médicales entre les professionnels participant à sa prise en charge.

280. De la même façon, les règles d'échange des données médicales du patient s'appliquent dans le cadre de la télésanté. Conséquemment, le patient bénéficie du droit de s'opposer à l'échange de ses données personnelles entre les téléprofessionnels de santé. En matière de télémedecine, les dispositions de l'ancien article R.6316-2 du code de la santé publique confirmaient que « *les professionnels participant à un acte de télémedecine peuvent, sauf opposition de la personne dûment informée, échanger des informations relatives à cette personne, notamment par le biais des technologies de l'information et de la communication* »⁸¹⁴. Désormais, les dispositions réglementaires organisant les modalités de réalisation des actes de télémedecine ne précisent plus le procédé de circulation de la donnée médicale entre les téléprofessionnels de santé. Dans le cadre d'un acte de télémedecine, les téléprofessionnels de santé peuvent donc échanger comme partager les informations médicales relatives au patient, notamment au moyen de son ENS. Certainement, cette plateforme contient « *des outils permettant des échanges sécurisés avec les acteurs du système de santé [...] et des outils permettant d'accéder à des services de télésanté* »⁸¹⁵.

⁸¹⁰ Délibération n° 2020-081 du 18 juin 2020 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux, *JORF* n°184, 28 juillet 2020, texte n° 94.

⁸¹¹ Article 6.1 e) du RGPD.

⁸¹² Article 6.2 f) du RGPD.

⁸¹³ Article 21.1 du RGPD.

⁸¹⁴ Dans sa version en vigueur du 22 octobre 2010 au 05 juin 2021.

⁸¹⁵ Article L.1111-13-1 II 5° du code de la santé publique.

Néanmoins, lorsque l'acte sanitaire réalisé à distance n'implique pas la participation du patient concerné, et que les acteurs de la télémédecine ne partagent pas un dossier médical auquel ils auraient communément accès⁸¹⁶, l'échange des données médicales demeure privilégié. Le cas échéant, le patient bénéficiaire d'un acte médical réalisé à distance doit toujours être informé de la transmission de ses données médicales entre les téléprofessionnels identifiés. L'autodétermination informationnelle du patient profitant de la télémédecine apparaît ainsi affirmée. Assurément, celui-ci doit connaître l'identité et la catégorie professionnelle du destinataire de ses données médicales et peut toujours s'y opposer. Cependant, l'exercice du droit d'opposition à l'échange de ses données médicales entre les téléprofessionnels de santé participant à l'acte de télésanté ferait obstacle à sa réalisation. De toute évidence, chaque acte de télésanté doit être effectué dans des conditions garantissant « *l'accès des professionnels de santé aux données de santé du patient nécessaires à la réalisation de l'acte ou de l'activité* »⁸¹⁷.

281. Si le patient peut, à tout moment, faire obstacle à l'échange de ses informations médicales, encore faut-il qu'il ait connaissance de cet échange, qu'il ait conscience de ce droit et, le cas échéant, qu'il sache comment l'exercer. Afin de garantir l'autodétermination informationnelle du patient à l'égard de l'échange de ses données médicales, le législateur ne devrait pas délimiter le champ de l'information préalable en considération des catégories auxquelles appartiennent les professionnels participant à sa prise en charge. Par suite, le champ de l'information préalable à l'échange de données médicale devrait toujours être conforme aux dispositions des articles 13 et 14 du RGPD⁸¹⁸, lesquelles apparaissent davantage protectrices des droits de la personne concernée.

2. La maîtrise du partage des données médicales par le patient

282. Le traitement consistant au *partage* des données médicales du patient peut être défini comme la mise à disposition d'informations accessibles au moyen d'un support matérialisé ou dématérialisé. Il s'agit donc d'une mise en commun d'informations entre personnes

⁸¹⁶ Tel que le DMP ou un système d'information hospitalier.

⁸¹⁷ Article R.6316-3 c) du code de la santé publique.

⁸¹⁸ Articles 13 et 14 du RGPD.

fondées à en connaître⁸¹⁹. Comme pour l'*échange* de données médicales, le patient doit être préalablement informé du *partage* de ses informations médicales et des droits subséquents dont il dispose. Toutefois, l'information relative au partage des données médicales du patient et les droits qu'ils lui sont concédés diffèrent selon que les professionnels appartiennent, ou non, à une même équipe de soins.

283. Lorsque les données médicales du patient sont partagées avec un professionnel ne faisant pas partie de l'équipe de soins⁸²⁰, « *l'information préalable de la personne est attestée par la remise à celle-ci, [...] d'un support écrit, qui peut être un écrit sous forme électronique, reprenant* »⁸²¹ les catégories d'informations ayant vocation à être partagées, les catégories de professionnels fondés à en connaître, la nature des supports utilisés pour les partager et les mesures prises pour préserver leur sécurité⁸²². En outre, ce support d'information doit indiquer « *les modalités effectives d'exercice de ses droits [...] ainsi que de ceux qui s'attachent aux traitements opérés sur l'information recueillie, en application de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* »⁸²³. Bien que ces formalités peuvent, en pratique, sembler contraignantes, cette information constitue un droit essentiel de la protection des données à caractère personnel. Dès lors, tout patient concerné par le partage de ses données médicales, au sein ou en dehors de l'équipe de soins, devrait bénéficier de la même information intégrale⁸²⁴.

284. En l'état actuel de la législation, lorsque les données médicales du patient sont partagées entre les membres d'une même équipe de soins, celui-ci est uniquement informé que les éléments immatériels de son corps humain sont réputés confiés à chacun des professionnels qu'elle regroupe⁸²⁵. En effet, le secret professionnel médical est partagé, de façon extensive, entre les professionnels appartenant à une même équipe de soins⁸²⁶. C'est

⁸¹⁹ BUCKI (E.), CASANOVAS (G.), LANGARD (S.), *op. cit.*, p. 659.

⁸²⁰ Cf. Paragraphe 264.

⁸²¹ Article D.1110-3-2 du code de la santé publique.

⁸²² Article D.1110-3-1 1° du code de la santé publique.

⁸²³ Article D.1110-3-2 du code de la santé publique.

⁸²⁴ Analogie à l'information prévue aux articles 13 et 14 du RGPD.

⁸²⁵ Article L.1110-4 III du code de la santé publique.

⁸²⁶ Cf. Paragraphe 264.

ainsi que « *le législateur a prévu une présomption de consentement au partage des données du patient* »⁸²⁷. Dans cette hypothèse, le patient n'a pas à consentir au partage de ses informations médicales. En effet, lorsque plusieurs professionnels concourent à la prise en charge d'un patient, *a fortiori* lorsqu'ils sont membres d'une même équipe de soins, le partage des données médicales doit être facilité. De façon pragmatique, Sylvie Hennion explique que « *la présomption de consentement évite des demandes formelles répétées d'accord du patient* »⁸²⁸. Néanmoins, à l'instar de l'échange des informations médicales, le patient dispose d'un droit d'opposition à leur partage au sein de l'équipe de soins. L'auteur considère que cette présomption de consentement « *limite, de fait, l'expression de la volonté à celle de son opposition aux partages de l'information* »⁸²⁹. Même si la maîtrise du partage des données médicales au sein d'une équipe de soins est limitée à l'opposition du patient, ce dernier peut, s'il le désire, empêcher toute circulation de ses informations entre les professionnels intéressés. En outre, cette opposition ne peut concerner que certaines informations ou viser des professionnels identifiés. Il apparaît que « *le patient a alors le droit d'imposer au professionnel de santé un secret absolu, ou de sélectionner les informations qu'il pourra communiquer* »⁸³⁰. Au demeurant, la mise à disposition de ces informations par le mécanisme du partage tend largement à simplifier et à favoriser la coordination et la continuité des soins tout en préservant la maîtrise des données par le patient concerné. Cette autodétermination informationnelle suppose toutefois que la personne concernée soit effectivement informée de la mise en œuvre de ce traitement, du droit de s'y opposer, des modalités d'exercice de ses droits ainsi que des conséquences inhérentes à une éventuelle opposition sur sa prise en charge sanitaire et sociale.

285. En revanche, lorsque les données médicales du patient sont mises à la disposition de professionnels étrangers à l'équipe de soins, son consentement préalable doit être recueilli par tout moyen⁸³¹. Le consentement au partage des informations médicales en dehors de l'équipe de soins « *est valable tant qu'il n'a pas été retiré par tout moyen, y compris sous*

⁸²⁷ MORLET-HAÏDARA (L.) *Le nouveau cadre légal de l'équipe de soins et du partage des données du patient*, *op. cit.*, p.1103

⁸²⁸ HENNION (S.), *op. cit.* p.131.

⁸²⁹ *Ibid.*

⁸³⁰ SAINT MARTIN (A.), *Le secret médical et le patient (I) le patient (a priori) maître du secret professionnel médical*, *op. cit.*, p. 109.

⁸³¹ Article L.1110-4 III du code de la santé publique.

forme dématérialisée. Il est strictement limité à la durée de la prise en charge de la personne »⁸³². Dans ce contexte, le patient doit alors exprimer sa volonté, de quelque façon que ce soit, au partage de ses données médicales. Autrement dit, le patient doit expressément autoriser leur mise à disposition en dehors de l'équipe de soins. Pourtant, bien qu'ils ne soient pas membres d'une même équipe de soins, les professionnels bénéficiant de l'accès aux données médicales du patient participent nécessairement à sa prise en charge sanitaire ou sociale. Partant, les données médicales ainsi partagées ne peuvent qu'être limitées à cette finalité. De surcroît, tout professionnel ne peut accéder à des données médicales qu'à condition d'être légalement investi du secret professionnel médical. Il en ressort que tout professionnel concourant à la prise en charge sanitaire ou sociale du patient ne peut accéder qu'à des données confidentielles et minimisées dans le respect de l'intimité de sa vie privée. Dès lors, est-il raisonnable d'accorder au patient un tel pouvoir décisionnel ? Le pouvoir de maîtrise accordé au patient sur ses données médicales ne devrait-il pas devenir relatif lorsque le traitement a pour finalité sa prise en charge sanitaire ?

286. Allouer au patient un droit au consentement au partage de ses données médicales revient à lui concéder l'entière maîtrise de ce traitement essentiel à la coordination de ses soins. Assurément, le patient peut autoriser comme refuser la mise en œuvre du traitement de ses données personnelles. En ce sens, Axel Saint Martin considère que « *le patient est libre d'interdire la communication d'informations le concernant, de son dossier médical ou de ses antécédents aux autres professionnels de santé* »⁸³³. Seulement, les données médicales du patient constituent les moyens matériels et intellectuels sur lesquels repose la prise en charge sanitaire de l'intéressé. Par suite, comment les professionnels, devant assurer la continuité et la coordination des soins du patient, peuvent-ils exécuter leur mission s'ils ne disposent pas des moyens nécessaires à son accomplissement ? Le refus du partage des données médicales entre les professionnels concourant aux soins ou au suivi médico-social et social du patient revient à entraver son parcours de santé.

287. Pourtant, le consentement ne constitue pas la base légale de la communication des données médicales du patient par leur partage. Qu'il s'agisse d'un échange ou d'un partage

⁸³² Article D.1110-3-3 du code de la santé publique.

⁸³³ SAINT MARTIN (A.), *Le secret médical et le patient (I) le patient (a priori) maître du secret professionnel médical*, op. cit., p. 110.

d'informations médicales entre professionnels appartenant à des catégories ou des équipes de soins différentes, leur communication dans l'objectif d'assurer la coordination ou la continuité des soins est toujours fondée sur deux bases légales déterminées en fonction du secteur dans lequel le patient est prise en charge. Lorsque le patient est soigné en secteur public, la base légale de l'échange ou du partage de ses données médicales repose sur la mission d'intérêt public dont le responsable de traitement est investi. En revanche, quand le patient est pris en charge en secteur privé, la communication de ses informations médicales entre les professionnels y participant est fondée sur les intérêts légitimes poursuivis par le responsable de leur traitement⁸³⁴.

De surcroît, le législateur européen autorise exceptionnellement le traitement des données médicales du patient par les professionnels concourant à sa prise en charge sanitaire ou sociale sans que l'intéressé n'ait à donner son consentement⁸³⁵. Le droit au consentement, édicté à l'article L.1110-4 III du code de la santé publique, conditionne donc indûment la mise en œuvre du traitement consistant au partage des données médicales du patient entre professionnels n'appartenant pas à la même équipe de soins. En vertu du RGPD, le consentement n'est pas compté parmi les droits de la personne concernée. En effet, le consentement est considéré comme l'une des six bases légales sur laquelle un traitement de données personnelles peut être fondé⁸³⁶ ; et comme l'une des dix exceptions en vertu de laquelle un traitement de données sensibles peut être autorisé⁸³⁷. Le droit au consentement au partage des données médicales institué par le droit national équivaut donc à accorder un droit supplémentaire au patient concerné alors que sa reconnaissance se trouve incompatible avec le cadre juridique relatif à la protection des données personnelles. Que les données médicales du patient soient partagées au sein ou en dehors de l'équipe de soins, celui-ci ne devrait bénéficier que d'un droit d'opposition à ce traitement⁸³⁸, à l'instar de la communication par l'échange des éléments immatériels de son corps humain.

⁸³⁴ Cf. Paragraphe 279.

⁸³⁵ Article 9.2 h) du RGPD.

⁸³⁶ Cf. Paragraphe 19.

⁸³⁷ Cf. Paragraphe 17.

⁸³⁸ Conformément à l'article 21.1 du RGPD.

Le droit d'opposition offre à la personne concernée une maîtrise mesurée du traitement de ses données personnelles. En effet, dans l'éventualité où l'exercice du droit d'opposition à la communication des données médicales fait obstacle à la prise en charge sanitaire du patient, le responsable de traitement peut outrepasser cette opposition 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* »⁸³⁹. Dans cette hypothèse, les motifs impérieux pouvant légitimer le traitement devraient s'apprécier en fonction des conséquences d'une telle opposition pour la santé du patient. Lorsque le patient n'a pas la volonté de refuser les soins, mais que l'opposition à la communication de ses données médicales entraîne des conséquences graves pour sa santé, alors les intérêts vitaux devraient prévaloir sur le droit fondamental à la protection des données à caractère personnel⁸⁴⁰. Toutefois, lorsque l'opposition à la communication des données médicales nécessaires à la prise en charge sanitaire n'entraîne aucune conséquence grave pour la santé du patient, ou lorsque cette opposition s'accompagne d'un refus de soins, le professionnel devrait respecter la volonté du patient. L'exercice de toute opposition au traitement⁸⁴¹ ayant pour finalité la prise en charge médicale, sa coordination ou sa continuité commande donc d'évaluer la nécessaire sauvegarde de la vie du patient par rapport à ses droits et libertés⁸⁴¹. Néanmoins, indépendamment de la gravité des répercussions liées à l'exercice du droit d'opposition sur la prise en charge sanitaire, le patient pourrait être tenu d'en assumer les conséquences dommageables⁸⁴². Si le patient est libre de s'opposer à la communication des éléments immatériels de son corps humain au profit de sa santé, ne lui appartiendrait-il pas le devoir d'auto-limiter cette prérogative⁸⁴³ ?

288. Les droits applicables au partage des données médicales du patient encadrent les modalités de l'accès au DMP, à quelques tempéraments près. Ce dossier numérique, destiné à favoriser la coordination, la qualité et la continuité des soins, permet le partage des données médicales de son titulaire entre les professionnels participant à sa prise en charge sanitaire. A cet effet, le législateur affirme que tout professionnel participant à la prise en charge du

⁸³⁹ Article 21.1 du RGPD.

⁸⁴⁰ Cf. Paragraphe 330.

⁸⁴¹ *Ibid.*

⁸⁴² Cf. Paragraphe 321.

⁸⁴³ *Ibid.*

patient peut accéder à son dossier numérique⁸⁴⁴. Par principe, cet accès est subordonné à l'assentiment du patient⁸⁴⁵. En effet, « *nul ne peut consulter le DMP sans l'autorisation préalable de son titulaire* »⁸⁴⁶. Toutefois, lorsque le professionnel à qui le titulaire du DMP a consenti l'accès est membre d'une équipe de soins, cet accès est « *réputé autorisé à l'ensemble des professionnels [qui en sont] membres* »⁸⁴⁷. Les professionnels relevant du champ médico-social ou social peuvent alors accéder au DMP de la personne qu'ils prennent en charge lorsqu'ils appartiennent à la même équipe de soins que le professionnel autorisé à y accéder⁸⁴⁸. En effet, l'ensemble des membres d'une équipe de soins bénéficient de la présomption de consentement au partage du secret professionnel médical⁸⁴⁹. Partant, le titulaire du DMP jouit d'un droit d'opposition à l'accès des professionnels, membres d'une équipe de soins, disposant de cette présomption. En effet, « *les dispositions sur le secret partagé, auxquelles le législateur ne semble pas avoir entendu déroger pour le DMP, prévoient un droit d'opposition au partage des données, en faveur du titulaire* »⁸⁵⁰. Seulement, quelles sont les modalités d'exercice de ce droit ?

289. Les dispositions législatives et réglementaires relatives au DMP ne mentionnent pas explicitement la possibilité de s'opposer à l'accès des membres d'une équipe de soins. Toutefois, le législateur a prévu, de façon générale, que « *le titulaire peut indiquer dans son dossier médical partagé l'identité des professionnels ou les établissements de santé, les établissement ou services sociaux ou médico-sociaux auxquels il entend interdire l'accès à son dossier* »⁸⁵¹. A cet effet, l'interface du DMP comporte une rubrique « *accès bloqués* » dans laquelle il est indiqué que « *vous pouvez bloquer l'accès à un professionnel de santé en effectuant une recherche de ce professionnel sur la base des critères indiqués ci-dessous, qu'il soit déjà autorisé ou non à accéder à votre DMP. Ce professionnel de santé ne pourra plus accéder à votre DMP, même en situation d'urgence. Vous pouvez mettre fin à tout*

⁸⁴⁴ Article L.1111-17 III du code de la santé publique.

⁸⁴⁵ Article R.1111-46 alinéa 1 du code de la santé publique.

⁸⁴⁶ BOURDAIRE-MIGNOT (C.), 2018 : *l'année du DMP pour tous ?*, RGDM, 2018, n°66, p. 28.

⁸⁴⁷ Article R.1111-46 alinéa 2 du code de la santé publique.

⁸⁴⁸ Depuis l'entrée en vigueur du Décret n°2021-1047 du 4 août 2021 relatif au dossier médical partagé, *JORF* n°182, 7 août 2021.

⁸⁴⁹ Cf. Paragraphe 284.

⁸⁵⁰ BOURDAIRE-MIGNOT (C.), 2018 : *l'année du DMP pour tous ?*, *op. cit.*, p. 35 à p. 36.

⁸⁵¹ Article R.1111-46 alinéa 8 du code de la santé publique.

moment à ce blocage en modifiant la liste des accès bloqués ». Ainsi, l'opposition au partage des données contenues dans le DMP, entre les membres d'une équipe de soins, se matérialise par un blocage numérique actionné par son titulaire.

Si pour Camille Bourdaire-Mignot « *il semble que le titulaire du DMP pourrait parfaitement interdire l'accès de son DMP à l'un des professionnels [...] exerçant au sein de l'équipe de soins qui l'a pris en charge* »⁸⁵², l'effectivité du droit d'opposition apparaît insuffisante. A l'inverse du mécanisme de l'échange de données entre professionnels identifiés, le mécanisme du *partage* des informations médicales entre les membres d'une équipe de soins ne permet pas de distinguer l'intégralité des potentiels accesseurs. En effet, la notion d'équipe de soins, loin d'être immuable, s'adapte en fonction de l'évolution du parcours de santé du patient⁸⁵³. Dès lors, comment le titulaire du DMP pourrait-il « *indiquer [...] l'identité des professionnels [...] auxquels il entend interdire l'accès à son dossier* »⁸⁵⁴ ? Il en résulte que le titulaire du DMP ne peut s'opposer au partage des données médicales qu'il contient avant que les professionnels, bénéficiant d'une présomption de consentement à l'accès, ne s'y soient connectés. Certainement, avant la première connexion du professionnel membre de l'équipe de soins, le titulaire du DMP peut en ignorer l'identité et, par conséquent, son éventuel accès. Néanmoins, suite à un premier accès du professionnel de santé au DMP, une notification est envoyée au titulaire afin de l'en informer⁸⁵⁵. Aussi, le titulaire du DMP « *peut, à tout moment, prendre connaissance des traces d'accès à son dossier* »⁸⁵⁶. Vraisemblablement, ce n'est donc qu'après le premier accès d'un professionnel membre d'une équipe de soins que le titulaire du DMP peut véritablement l'inscrire sur la liste des interdictions.

290. En outre, il convient de s'interroger sur l'étendue du partage de ce dossier numérique aux professionnels membres d'une équipe de soins. Alors que les dispositions de droit commun circonscrivent le partage des informations du patient à la durée de la prise en charge médicale, les accès autorisés au DMP n'ont pas de limitation temporelle. Il appartient donc

⁸⁵² BOURDAIRE-MIGNOT (C.), 2018 : *l'année du DMP pour tous ?*, loc. cit.

⁸⁵³ Cf. Paragraphe 264.

⁸⁵⁴ Article R.1111-46 alinéa 8 du code de la santé publique.

⁸⁵⁵ Article R.1111-46 alinéa 9 du code de la santé publique.

⁸⁵⁶ Article L.1111-19 du code de la santé publique.

au titulaire du DMP de gérer les listes des accès et des interdictions de connexion à son DMP. À tout moment, le titulaire du DMP peut donc interdire un accès antérieurement autorisé et, pareillement, autoriser un accès préalablement interdit. Tant que le titulaire du DMP n'a pas restreint l'accès des membres de l'équipe de soins le prenant en charge, ces derniers bénéficient-ils d'un accès permanent au DMP ? Dans le doute, il appartient au titulaire du DMP de régenter les autorisations octroyées suite à sa prise en charge sanitaire. Pour cela, encore faut-il qu'il ait connaissance de l'identité des professionnels de santé bénéficiaires d'une présomption d'autorisation d'accès.

Par ailleurs, le titulaire du DMP peut s'opposer, par anticipation, à son accès dans l'hypothèse où il serait « *hors d'état d'exprimer sa volonté, en présence d'une situation comportant un risque immédiat pour sa santé* »⁸⁵⁷. De la même façon, le titulaire du DMP peut refuser que « *le médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente [...] qui reçoit un appel concernant une personne [y] accède* »⁸⁵⁸.

291. En revanche, lorsque le professionnel n'appartient pas à une équipe de soins, son accès au DMP doit être préalablement autorisé par son titulaire⁸⁵⁹. Dans ce contexte, le consentement à l'accès au DMP redevient le principe. De cette manière, le professionnel accesseur, participant à la prise en charge médicale du patient, doit adresser une demande de connexion au titulaire du DMP qui peut l'y autoriser. Aussi, un professionnel de santé peut recueillir, « *après avoir informé la personne concernée, son consentement pour qu'un autre professionnel de santé à qui il serait nécessaire de confier une partie de la prestation accède à son dossier médical partagé et l'alimente* »⁸⁶⁰. Des professionnels de santé n'appartenant pas à la même équipe de soins peuvent alors partager les données médicales du patient au moyen du DMP sous réserve de son assentiment. Cette possibilité garantit l'autodétermination du patient au partage de ses informations médicales au moyen de ce dossier numérique. Dans cette hypothèse, le titulaire du DMP conserve son droit au consentement à l'accès des professionnels à son carnet numérique de santé.

⁸⁵⁷ Article L.1111-17 I du code de la santé publique.

⁸⁵⁸ *Ibid.*

⁸⁵⁹ Article R.1111-46 alinéa 3 du code de la santé publique.

⁸⁶⁰ Article R.1111-41 alinéa 3 du code de la santé publique.

292. Néanmoins, le droit au consentement à l'accès au DMP et au partage des informations qu'il contient ne sont-ils pas contraires à sa finalité ? En effet, le DMP a vocation à être partagé avec l'ensemble des professionnels participant à la prise en charge médicale du patient afin d'assurer la continuité et la coordination de ses soins. Ainsi, le DMP constitue un outil de coopération sanitaire, à destination des professionnels, permettant l'accomplissement de leurs missions. Eu égard à cette finalité, l'accès au DMP ne devrait pas reposer sur le consentement de son titulaire. En effet, la connexion au DMP devrait être permise à tout professionnel de santé participant à la prise en charge sanitaire du patient, dans la limite des seules données médicales nécessaires à l'accomplissement de ses missions respectives⁸⁶¹.

L'affermissement du rôle central du DMP comme unique dossier médical appelle à supprimer le droit au consentement au profit d'une généralisation du droit d'opposition au partage des informations qu'il contient. Toutefois, le législateur devrait en simplifier les modalités d'exercice, notamment pour faciliter l'opposition à l'accès des professionnels de santé membres d'une équipe de soins. Ainsi, le titulaire du DMP bénéficierait du contrôle de ses accès grâce à la seule gestion des interdictions. En effet, bloquer l'accès d'un professionnel au DMP revient à s'opposer au partage des éléments immatériels de son corps humain.

293. Outre la gestion des accès au DMP, son titulaire dispose d'un droit au masquage des informations qu'il contient. Le législateur admet que « *certaines informations peuvent être rendues inaccessibles par le titulaire du dossier médical partagé* »⁸⁶². Ainsi, le titulaire du DMP peut circonscrire l'accès des professionnels autorisés à s'y connecter. Par le biais du masquage des données médicales, il peut moduler les informations consultables. Seulement, cette maîtrise accordée au titulaire du DMP ne risque-t-elle pas de mettre sa santé en péril ? La limitation de la communication des données médicales du patient pourrait contrevenir à sa prise en charge sanitaire. C'est pourquoi ce contrôle octroyé au patient concerné comprend certaines restrictions.

⁸⁶¹ Cf. Paragraphe 271.

⁸⁶² Article L.1111-15 alinéa 5 du code de la santé publique.

B) Les restrictions de la maîtrise de la communication des données médicales par le patient

294. La communication des données médicales du patient, entre les différents professionnels concourant à sa prise en charge sanitaire, est nécessaire à la coordination et à la continuité de ses soins. La transmission de ces informations entre professionnels tend effectivement à la préservation de la santé du patient. Eu égard à l'importance de cette communication, le législateur l'a, dans certains cas, exigée. Le cas échéant, le patient se trouve privé de son droit d'opposition au traitement de ses données personnelles. En effet, lorsque la communication des données médicales du patient repose sur une obligation légale pesant sur le professionnel de santé, le patient ne peut faire obstacle à son exécution.

295. Cette communication est notamment imposée pour assurer la continuité de la prise en charge entre la médecine de ville et la médecine hospitalière. Grâce à l'instauration des lettres de liaison, le législateur a systématisé une communication des informations médicales à double sens. Ainsi, le praticien qui adresse un patient à un établissement de santé doit accompagner sa demande d'une lettre de liaison synthétisant les informations médicales nécessaires à sa prise en charge hospitalière⁸⁶³. Ces informations sont incontournables pour orienter et organiser le parcours de santé du patient. En outre, lorsque le médecin adresseur n'a pas la qualité de médecin traitant, l'établissement de santé au sein duquel le patient a été admis doit informer ce dernier de la date, de l'heure et du service d'admission du malade⁸⁶⁴. De surcroît, au cours de l'hospitalisation, le médecin traitant et, s'il est différent, le médecin adresseur sont autorisés à demander l'accès au dossier médical hospitalier du patient⁸⁶⁵. Force est d'observer que les médecins de ville bénéficient du droit d'être informés de l'état de santé du malade hospitalisé et de son évolution.

A son tour, le médecin hospitalier en charge du patient doit adresser, au jour de sa sortie, une lettre de liaison au praticien qui a adressé le patient ainsi qu'à son médecin traitant⁸⁶⁶ et, le cas échéant, à la structure de transfert. Ce document de liaison doit comporter

⁸⁶³ Article L.1112-1 II du code de la santé publique.

⁸⁶⁴ Article R.1112-6 du code de la santé publique.

⁸⁶⁵ Article L.1112-1 II alinéa 2 du code de la santé publique.

⁸⁶⁶ Article L.1112-1 II du code de la santé publique.

les éléments utiles à la continuité des soins. Précisément, il doit contenir le motif d'hospitalisation, la synthèse médicale du séjour, les résultats d'examen, les traitements prescrits à la sortie de l'établissement ainsi que les suites à donner à l'issue de l'hospitalisation⁸⁶⁷. Ces informations s'avèrent indispensables à la continuité des soins du patient et visent « à éviter les ruptures de parcours de soins trop souvent constatées à la suite d'hospitalisation »⁸⁶⁸.

Si les lettres de liaison semblent pouvoir être envoyées par voie postale, le législateur incite les professionnels de santé à les transmettre de façon dématérialisée par messagerie sécurisée⁸⁶⁹. L'objectif est de réduire le délai de communication de la lettre de liaison, *a fortiori* lorsqu'elle fait suite à la sortie hospitalière du patient. En effet, la volonté du législateur est d'« informer obligatoirement le jour même de la sortie le médecin traitant afin qu'il puisse répondre aux questions de son patient et le prendre en charge dans les meilleures conditions possibles dès sa sortie »⁸⁷⁰. Afin d'assurer une transmission rapide des lettres de liaison, le législateur exige qu'elles soient, en complément, versées dans le DMP du patient s'il a été créé. Cette obligation a été affirmée par la loi ASAP⁸⁷¹. Il est désormais prévu que « lorsque les lettres de liaison sont dématérialisées, elles doivent être déposées dans le dossier médical partagé du patient et envoyées par messagerie sécurisée »⁸⁷² aux professionnels de santé susmentionnés. Dans ce contexte, le patient ne peut donc ni s'opposer à la communication de ses informations médicales, ni choisir leur mode de transmission.

296. Compte tenu du caractère obligatoire de ce dispositif, la doctrine juridique estime « qu'un médecin adressant son patient à un hôpital sans rédiger cette lettre [de liaison] pourrait voir sa responsabilité engagée si, en raison de cette carence, la prise en charge

⁸⁶⁷ Article R.1112-1-2 du code de la santé publique.

⁸⁶⁸ VÉLAN (O.), LACLAIS (B.), TOURAINE (J.-L.), GEOFFROY (H.), FERRAND (R.), *Rapport n°2673 fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé, Assemblée nationale, 20 mars 2015.*

⁸⁶⁹ Article L.1112-1 II alinéa 5 du code de la santé publique.

⁸⁷⁰ VÉLAN (O.), LACLAIS (B.), TOURAINE (J.-L.), GEOFFROY (H.), FERRAND (R.), *Rapport n°2673, loc. cit.*

⁸⁷¹ Loi n°2020-1525 du 7 décembre 2020, *loc. cit.*

⁸⁷² Article L.1112-1 II du code de la santé publique.

hospitalière se passait mal »⁸⁷³. Identiquement, « *l'hôpital qui confie un patient soigné à la médecine de ville sans délivrer les informations indispensables à sa prise en charge serait fautif en cas de problème lié à ce défaut d'information* »⁸⁷⁴. Le manquement à l'obligation de communication des lettres de liaison constitue donc une faute pouvant engager la responsabilité du professionnel de santé. Toutefois, si ce manquement était le fait du patient, dans l'hypothèse où il conserverait la maîtrise de la communication de ses données médicales, alors la responsabilité du professionnel de santé saurait être écartée. Le patient qui participe à la réalisation de son propre préjudice doit en assumer les conséquences dommageables⁸⁷⁵.

297. Au-delà du contexte de l'hospitalisation du patient, la communication de ses données médicales à des fins de coordination des soins tend à se généraliser. En effet, le législateur a prescrit l'obligation, pour les professionnels de santé, de transmettre les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins du patient à l'issue de chaque acte ou consultation⁸⁷⁶. Ces éléments médicaux, ne devant initialement qu'être reportés dans le DMP, doivent également être envoyés par messagerie sécurisée au médecin traitant, au médecin prescripteur le cas échéant, et à tout professionnel dont l'intervention dans la prise en charge sanitaire du patient paraît pertinente⁸⁷⁷. Tandis que le patient a le droit de masquer certaines informations colligées dans son DMP, ou de refuser l'accès de certains professionnels de santé, ces mêmes informations seront, malgré tout, transmises à une pluralité de professionnels de santé. Dès lors que le patient est titulaire d'un DMP, il apparaît que ces éléments médicaux doivent systématiquement et obligatoirement être communiqués par le professionnel de santé prodiguant l'acte sanitaire, nonobstant la maîtrise et les droits dont il dispose sur les données médicales colligées dans son DMP. L'emploi de l'impératif par le législateur conforte le fondement juridique de ce traitement. Ainsi, l'envoi de ces éléments par messagerie sécurisée semble reposer sur une obligation légale incombant à tout professionnel de santé, à laquelle le patient titulaire d'un DMP ne peut s'opposer. Il résulte

⁸⁷³ MARKUS (J.-P.), CRISTOL (D.), PEIGNE (J.), AUTIER (E.), Commentaire sous l'article L.1111-2 du code de la santé publique, 35^e ed, Dalloz, 2021.

⁸⁷⁴ *Ibid.*

⁸⁷⁵ Cf. Paragraphe 321.

⁸⁷⁶ Article L.1111-15 alinéa 1 du code de la santé publique.

⁸⁷⁷ *Ibid.*

de ces dispositions que la maîtrise de la communication des données médicales par le patient est profondément affectée. Véritablement, les hypothèses où le patient peut encore s'opposer à l'échange ou au partage de ses informations médicales semblent considérablement réduites.

298. Tandis que le législateur peut imposer au professionnel de santé de communiquer les informations médicales qu'il a générées au terme de la consultation ou de l'hospitalisation, il n'exige pas la transmission des informations médicales nécessaires à la réalisation d'un acte de télémedecine. A titre d'exemple, la téléexpertise⁸⁷⁸ ou la téléassistance médicale⁸⁷⁹ permettent de mettre en rapport un professionnel médical avec un professionnel de santé grâce à l'usage des technologies de l'information et de la communication. Alors que le patient ne participe pas directement à ces deux actes de télémedecine, leur effectuation requiert néanmoins la transmission de ses données médicales entre les professionnels de santé y participant. Autrement dit, la réalisation d'un acte de téléexpertise ou de téléassistance médicale repose exclusivement sur la fourniture préalable des données médicales du patient par le télémedecin requérant. Dès lors, les informations médicales du patient devraient être transmises en amont de cette pratique médicale. Cependant, les téléprofessionnels de santé ne peuvent échanger les informations médicales relatives au patient tant qu'il ne s'y est pas opposé, ni les partager sans qu'il n'y ait consenti. Seulement, les actes de télémedecine étant réalisés à distance, la circulation des données médicales du patient est indispensable à cette finalité. Leur communication constitue même une condition *sine qua non* à l'accomplissement des actes de téléexpertise et de téléassistance médicale. Assurément, le téléprofessionnel de santé requis doit accéder aux données médicales du patient pour rendre un avis expert ou pour assister son confrère dans la réalisation d'un acte. C'est pourquoi le législateur a souhaité que chaque acte de télémedecine soit « *réalisé dans des conditions garantissant [...] l'accès des professionnels de santé aux données médicales du patient nécessaires à la réalisation de l'acte* »⁸⁸⁰.

⁸⁷⁸ L'article R.6316-1 2° du code de la santé publique définit la téléexpertise comme l'acte médical « *qui a pour objet de permettre à un professionnel de santé de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux en raison de leurs formations ou de leurs compétences particulières, sur la base des informations de santé liées à la prise en charge d'un patient* ».

⁸⁷⁹ L'article R.6316-1 4° du code de la santé publique définit la téléassistance médicale comme l'acte médical « *qui a pour objet de permettre à un professionnel médical d'assister à distance un autre professionnel de santé au cours de la réalisation d'un acte* ».

⁸⁸⁰ Article R.6316-3 c) du code de la santé publique.

Vraisemblablement, cette volonté législative n'a été assortie d'aucune garantie juridique. Cette promesse faite aux télémedecins représente même une ineptie. Alors que le patient doit donner son consentement à la réalisation de l'acte de télémédecine, le législateur admet implicitement qu'il puisse refuser le traitement des éléments immatériels de son corps humain. Le cas échéant, comment « garantir » l'accès des professionnels de santé aux données médicales du patient ? Dans cette hypothèse, la communication des informations médicales du patient, nonobstant son refus, constituerait une violation du secret professionnel médical, une atteinte à la vie privée de la personne concernée et un manquement à la protection de ses données personnelles.

En l'état actuel de la législation, le refus du patient à la transmission de ses informations médicales entre les télémedecins devrait entraîner la résiliation du contrat de soins ou la cessation de la relation statutaire qui les lie. En effet, cet obstacle rend l'exercice des actes de téléexpertise et de téléassistance médicale impossible. Cette conséquence juridique apparaît discordante à l'heure du développement massif de la santé numérique. De surcroît, l'antinomie juridique démontrée ci-avant doit impérieusement être solutionnée. Certainement, ce paradoxe normatif ne peut subsister dans l'ordre juridique national. Le consentement du patient, à la réalisation de l'acte de télémédecine, devrait obliger les téléprofessionnels de santé à transmettre ses informations médicales. De cette façon, la base légale du traitement consistant en la communication des données du patient reposerait sur l'obligation légale incombant aux téléprofessionnels de santé. Dès lors, le patient ayant consenti à la réalisation de l'acte de télémédecine ne pourrait plus s'opposer ou consentir à la nécessaire circulation de ses informations médicales. Au demeurant, le patient qui refuserait l'échange ou le partage de ses données médicales entre les téléprofessionnels de santé resterait libre de renoncer à la réalisation de l'acte de télémédecine. Indéniablement, la circulation des données médicales du patient représente l'essence de la télémédecine. Si la normalisation de la restriction de la maîtrise de la communication de ces éléments immatériels par le patient est critiquable, cette restriction serait néanmoins légitimée dans le cadre de cet acte médical pratiqué à distance.

299. Enfin, la maîtrise des données communiquées au moyen du DMP par son titulaire connaît également des restrictions légales. En effet, le titulaire du DMP ou, le cas échéant, la personne chargée à son égard d'une mesure de protection juridique avec représentation, ne peut interdire tous les accès à son DMP, ni masquer toutes les informations médicales qu'il

contient. D'abord, les données médicales contenues dans le DMP demeurent toujours accessibles au professionnel qui les a déposées⁸⁸¹. Ensuite, le médecin traitant dispose d'un droit d'accès au Dossier Médical Partagé de son patient sans que ce dernier ne puisse l'interdire⁸⁸². De surcroît, le médecin traitant accède à l'ensemble des informations contenues dans ce dossier, y compris celles masquées par son titulaire⁸⁸³. Cette double restriction au profit du médecin traitant « *permet d'éviter de transférer totalement au patient la charge de la responsabilité liée au contenu du dossier* »⁸⁸⁴. En effet, Camille Bourdaire-Mignot constate que « *le patient n'a donc pas la maîtrise du contenu du dossier qui reste toujours accessible à un professionnel de santé au moins : le médecin traitant* »⁸⁸⁵. Après, dans les situations d'urgence médicale, le titulaire du DMP est présumé consentir à l'accès des professionnels de santé prodiguant les soins nécessaires à sa survie⁸⁸⁶, et du médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente⁸⁸⁷. Dès lors, il appartient au titulaire du DMP de s'opposer expressément à sa consultation dans de telles situations. Finalement, l'accès au DMP semble *de facto* autorisé aux médecins de la protection maternelle et infantile sans que les représentants légaux du mineur ne puissent s'y opposer⁸⁸⁸.

300. Alors que le patient ne maîtrise pas intégralement la communication de ses données médicales entre les professionnels intervenant à sa prise en charge sanitaire ou médico-sociale, le patient ne peut, à l'inverse, imposer la communication des éléments immatériels de son corps humain en dehors des conditions légales et réglementaires exposées ci-avant. En effet, le consentement du patient à la révélation de ses informations médicales ne saurait délier le professionnel de son obligation de secret⁸⁸⁹. Le caractère absolu du secret

⁸⁸¹ Article R.1111-49 du code de la santé publique.

⁸⁸² *Ibid.*

⁸⁸³ Article L.1111-16 alinéa 2 du code de la santé publique.

⁸⁸⁴ BOURDAIRE-MIGNOT (C.), 2018 : *l'année du DMP pour tous ?*, *op. cit.*, p. 30.

⁸⁸⁵ *Ibid.*

⁸⁸⁶ Article L.1111-17 I du code de la santé publique.

⁸⁸⁷ Article L.1111-17 I alinéa 2 du code de la santé publique.

⁸⁸⁸ Article L.1111-18 alinéa 3 du code de la santé publique.

⁸⁸⁹ Crim., 22 décembre 1966, n°66-92.897, Bull. crim, n° 305 ; D., 1967, 122 ; JCP, 1967, jur. II. 15126, note R. Savatier ; RSC, 1967, 453, obs. Levasseur ; Crim. 8 avr. 1998, n° 97-83.656.

professionnel médical⁸⁹⁰ s'oppose donc à toute divulgation des données médicales du patient, quand bien même cette communication serait expressément demandée par celui-ci. Il en ressort que le droit à la portabilité des données personnelles consacré par le RGPD⁸⁹¹, permettant de les transférer numériquement d'un organisme vers un autre, serait contraire au secret professionnel médical. Par surcroît, « *le droit à la portabilité ne s'applique pas aux données personnelles traitées sur une autre base légale que le consentement ou l'exécution d'un contrat* »⁸⁹². La constitution d'un dossier médical et la formalisation des données médicales du patient en son sein constitue une obligation légale pour tout professionnel et établissement de santé⁸⁹³. Par conséquent, le droit à la portabilité des données médicales consignées dans les dossiers médicaux du patient est définitivement inapplicable. Dans l'hypothèse où le patient désire transmettre son dossier médical informatisé à un tiers, il lui appartient d'en demander la communication dans un format numérique puis de le transférer, directement et personnellement, au responsable de traitement de son choix.

301. La restriction des droits du patient à l'égard de la communication de ses données médicales est toujours justifiée par la protection de sa santé. Il apparaît que la transmission de ces informations s'avère indispensable à la coordination de son parcours de santé. Dès lors, le patient, acteur de sa santé et maître de ses données personnelles, ne devrait entraver sa prise en charge médicale. A l'inverse, celui-ci aurait le devoir d'y collaborer.

⁸⁹⁰ Cass. crim., 19 décembre 1885, *Watelet*, Bull. crim., 1885, n° 363 ; D., 1885, p. 345 ; S., 1886, p. 86 ; DP, 1886, p. 347.

⁸⁹¹ Article 20 du RGPD.

⁸⁹² CNIL, *Le droit à la portabilité en questions*, 22 mai 2017. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 17 mars 2021.

⁸⁹³ Cf. Paragraphes 104 et 109.

Section 2 : L'inéluctable responsabilisation de la personne concernée par le traitement de ses données médicales

« L'autonomie de la volonté est le principe unique de toutes les lois morales et des devoirs qui y sont conformes ; au contraire toute hétéronomie du libre choix, non seulement n'est la base d'aucune obligation, mais elle est plutôt opposée au principe de l'obligation et à la moralité de la volonté. »⁸⁹⁴.

302. Le patient est titulaire de droits qui lui octroient une autonomie dans la gestion de sa santé comme dans la gestion de ses données médicales personnelles. En vertu de cette autonomisation, le patient est libre d'opérer des choix au moyen du libre exercice de ses droits. Ainsi, les patients bénéficient d'une capacité d'action et de décision pouvant orienter et impacter leur parcours de santé.

Seulement, l'exercice des droits que le patient détient sur ses données médicales peut contrarier sa prise en charge sanitaire. Ordinairement, toute personne concernée peut, de la façon la plus absolue qui soit, s'opposer au traitement de ses données personnelles, en demander la rectification, l'effacement, la limitation, la portabilité ou, plus simplement encore, refuser de livrer les informations qui la concernent. Toutefois, ces droits ne sont pas toujours compatibles avec un traitement de données ayant pour finalité la prise en charge médicale de l'individu. En effet, la portée de l'exercice des droits conférés par le RGPD peut s'avérer préjudiciable pour la prise en charge sanitaire du patient. Certainement, la dispensation d'un acte de prévention, de diagnostic ou de soins est fondée sur l'analyse de ses données médicales. Il est donc indispensable que le patient favorise le traitement des éléments immatériels de son corps humain dès lors qu'il apparait nécessaire à l'objectif poursuivi : sa prise en charge sanitaire (**Paragraphe 1**). Ainsi, le consentement aux soins impliquerait corrélativement une renonciation à la plénitude des droits sur ses données médicales personnelles (**Paragraphe 2**).

⁸⁹⁴ KANT (E.), *Critique de la raison pratique*, Théorème IV, Première partie, Trad. par François Picavet, PUF, 1965, p. 33.

Paragraphe 1 : Le devoir du patient de renseigner ses données médicales

303. En tant qu'acteur de sa santé et commanditaire de l'usage de ses données personnelles, le patient a le devoir de collaborer à sa prise en charge médicale. A ce titre, le patient doit informer le professionnel de santé en lui livrant les données médicales indispensables à la dispensation de l'acte sanitaire (**A**). Ce devoir d'information est facilité par les outils numériques de santé mis à la disposition du patient. En particulier, la collaboration du patient à la prise en charge sanitaire peut être honorée grâce à la documentation du DMP par son titulaire (**B**). A défaut, le professionnel de santé ne peut être tenu pour responsable du dommage causé par l'ignorance d'une information que le patient lui a volontairement dissimulée. Le patient autonome assume donc les conséquences dommageables de ses actes.

A) L'instauration prétorienne d'un devoir légal d'information à la charge du patient

304. La prise en charge sanitaire d'un patient repose sur l'analyse de ses données médicales par les professionnels qui y participent directement. La prise en charge médicale implique donc un traitement de données personnelles auquel le patient ne peut s'opposer. Bien au contraire, le patient devrait livrer, aux professionnels de santé, les données nécessaires à la dispensation des actes médicaux. Si la prise en charge médicale s'appuie sur les données cliniques produites par les praticiens lors de l'examen clinique, elle se fonde également sur les données collectées auprès du patient à l'occasion de l'interrogatoire médical⁸⁹⁵. En effet, le patient est le seul détenteur d'informations souvent déterminantes pour l'orientation de son parcours de soins, pour l'établissement du diagnostic, ou encore, pour l'administration d'une thérapeutique. Partant, ces informations médicales personnelles doivent impérativement être portées à la connaissance des professionnels de santé.

305. C'est ainsi que par une décision du 20 janvier 2011⁸⁹⁶, les juges du Quai de l'Horloge ont retenu un devoir de collaboration, de transparence et d'information réciproque à la charge du patient. En l'espèce, une femme séropositive au virus de l'immunodéficience humaine

⁸⁹⁵ Cf. Paragraphe 50.

⁸⁹⁶ Civ. 1^{ère}, 20 janvier 2011, n°09-68.042.

(VIH) a donné naissance à un enfant contaminé *in utero*. Il résulte des faits que la mère se savait malade, était suivie depuis des années pour cette infection et avait parfaitement connaissance des risques de transmission du virus à son enfant. Néanmoins, cette dernière n'en a jamais informé son gynécologue et a même déclaré n'avoir aucun antécédent médical. En conséquence, le fœtus n'a pas pu recevoir le traitement permettant de prévenir cette transmission. La protagoniste a alors recherché la responsabilité de l'établissement de santé dans lequel exerçait le gynécologue afin de réparer la perte de chance de diagnostiquer et de traiter plus tôt l'affection dont souffre son enfant. Les juges de première instance et d'appel l'ont déboutée de sa demande. Cette dernière a donc formé un pourvoi en cassation. Les juges de cassation ont alors décidé que, bien informée des risques, la patiente avait dissimulé son état de santé au gynécologue alors qu'à la date de naissance de l'enfant, le dépistage systématique du VIH n'était pas obligatoire. Les juges en ont déduit que le gynécologue l'ayant prise en charge n'avait commis aucun manquement fautif susceptible d'engager la responsabilité de l'établissement. Autrement dit, le dommage résultant d'une dissimulation par le patient d'informations relatives à sa santé n'est pas imputable au médecin.

Eu égard à cette décision, la doctrine juridique reconnaît unanimement un devoir de collaboration à la charge du patient. Selon Anne Laude, « *le patient est [...] tenu à une obligation de collaborer, de révéler tous les symptômes de l'affection qu'il présente ainsi que l'ensemble des informations pertinentes pour élaborer le diagnostic* »⁸⁹⁷. En outre, Coralie Leuzzi-Louchart considère que « *le patient est lui-même débiteur, si ce n'est d'une obligation d'information, à tout le moins d'un devoir d'information envers le praticien qui le prend en charge, surtout lorsque cette information est déterminante pour la bonne réussite des soins et des interventions pratiquées* »⁸⁹⁸. Globalement, Paul Véron y perçoit « *un devoir général de collaboration à l'égard du praticien, qui implique notamment de ne pas dissimuler les informations utiles à sa prise en charge* »⁸⁹⁹. Pour ce dernier auteur, « *cette décision pourrait rejoindre le mouvement [...] de reconnaissance de devoirs mis à la charge du patient* »⁹⁰⁰.

⁸⁹⁷ LAUDE (A.), *Le patient entre responsabilité et responsabilisation*, Les Tribunes de la santé, 2013, n°41, p. 82.

⁸⁹⁸ LEUZZI-LOUCHARTE (C.), *Les devoirs du patient : l'échange réciproque d'information*, RGDM, 2013, n° 49, p. 137.

⁸⁹⁹ VERON (P.), *Dissimulation par la patiente de son état de santé et exclusion de la responsabilité du praticien : vers un devoir de collaboration du patient ?*, RDS, 2012, n°49, p. 603.

⁹⁰⁰ *Ibid.*

Préalablement à cette reconnaissance prétorienne, Bernard Hoerni et Michel Bénézech estimaient déjà que « *les devoirs des malades [...] sont [...] tout à fait réels, assez nombreux et relativement contraignants* »⁹⁰¹. Bien qu'ils ne soient pas explicitement consacrés par le législateur, « *ils n'en sont pas moins importants. Ils s'imposent comme condition de soins de qualité* »⁹⁰². En 2004, ces deux médecins ont alors dégagé et catégorisé l'ensemble des devoirs incombant au patient. Il ressort de leurs travaux que « *le premier devoir du malade est de renseigner convenablement le médecin pour lui permettre de formuler diagnostic et traitement correspondants* »⁹⁰³. C'est donc dans la lignée de cette doctrine médicale que le juge civil a instauré un devoir d'information à la charge du patient. Compte tenu de ce qui précède, le patient a effectivement le devoir de renseigner ses données médicales de façon loyale, honnête et transparente, aux fins de collaborer à sa prise en charge sanitaire.

306. Le déploiement de la télésanté justifie davantage l'instauration d'un devoir de collaboration du patient. La téléconsultation, qu'elle soit dispensée dans le cadre de la télé médecine ou du télésoin, repose exclusivement sur la transmission des données médicales du patient au moyen des technologies de l'information et de la communication. Le plus souvent, la téléconsultation est effectuée par vidéotransmission ou par téléphone et ne permet pas la production de données cliniques par le professionnel de santé. Le cas échéant, la consultation à distance repose uniquement⁹⁰⁴ sur les données collectées par le téléconsultant sur la base des informations fournies par le patient. Dans le cadre de la téléconsultation, l'anamnèse occupe – conséquemment – une place fondamentale. Maryse Deguergue alerte que « *la technologie utilisée peut, plus facilement que la rencontre physique, permettre au patient de cacher un certain nombre d'informations nécessaires au médecin pour accomplir son acte médical, son diagnostic par exemple* »⁹⁰⁵. Dès lors, « *il faut souligner l'importance du comportement du patient lors d'une téléconsultation* »⁹⁰⁶. C'est pourquoi la collaboration

⁹⁰¹ HOERNI (B.) & BENEZECH (M.), *Les devoirs des patients*, La Presse Médicale, vol. 33, 2004, n°2, p. 80.

⁹⁰² *Ibid.*

⁹⁰³ HOERNI (B.) & BENEZECH (M.), *op. cit.*, p. 81.

⁹⁰⁴ Hormis lorsque le patient consulte dans une cabine de télé médecine ou lorsqu'un professionnel de santé est présent auprès du patient afin de réaliser des gestes à la place du téléconsultant.

⁹⁰⁵ DEGUERGUE (M.), *Télé médecine et responsabilités*, *op. cit.*, p. 33.

⁹⁰⁶ *Ibid.*

du patient, traduite par le devoir de renseigner ses données médicales, doit être renforcée. Si l'exercice de la télésanté est conditionné par la mise en œuvre du traitement des données médicales du patient, il appartient au patient de les fournir au professionnel téléconsultant. Assurément, les données médicales du patient constituent l'unique attirail permettant l'effectuation de la téléconsultation.

307. Toutefois, il ne faut pas négliger que le patient est un profane et que tout individu ne dispose pas des mêmes capacités cognitives. Partant, « *le professionnel de soins doit être particulièrement vigilant sur les informations que lui livre son patient* »⁹⁰⁷. Au-delà, il appartient au professionnel de santé de conduire un interrogatoire « *pointu, précis et complet* »⁹⁰⁸ et de collecter, auprès du patient, les informations nécessaires à la dispensation des actes de prévention, de diagnostic ou de soins. A cet effet, le professionnel de santé doit maîtriser et orienter l'entretien médical en posant au patient les questions adéquates à l'établissement d'un bon diagnostic⁹⁰⁹. Tandis que le juge a retenu un devoir de collaboration à la charge du patient, il a corrélativement retenu l'obligation, pour le médecin, de se renseigner avec précision sur l'état de santé du malade⁹¹⁰. Dès lors, il ne peut être reproché au patient de ne pas avoir « *délivré des informations dont il pouvait légitimement ignorer l'intérêt, l'importance ou la pertinence* »⁹¹¹. Si on peut attendre du patient qu'il décrive les symptômes ressentis et qu'il indique ses antécédents médicaux et familiaux, ses traitements en cours et ses allergies, c'est parce que le professionnel de santé l'aura consciencieusement interrogé. En définitive, le devoir de collaboration du patient comprend un devoir de transparence dans les réponses apportées aux questions posées.

308. L'instauration de ce devoir apparaît nécessaire dans la mesure où le patient contrôle, *ab initio*, ses données médicales. Cela signifie que le patient est libre de dissimuler ses informations médicales ou de renseigner des données inexactes. Force est d'observer que

⁹⁰⁷ CORGAS-BERNARD (C.), *Responsabilité civile médicale et nouvelles pratiques numériques : L'exemple de la télémédecine*, LPA, 2014, n°164, p. 27.

⁹⁰⁸ *Ibid.*

⁹⁰⁹ CORGAS-BERNARD (C.), *loc. cit.* ; LEUZZI-LOUCHART (C.), *Les devoirs du patient : l'échange réciproque d'information*, *op. cit.*, p. 141.

⁹¹⁰ Civ. 1^{ère}, 5 mars 2015, n°14-13.292, Bull. civ., I, n° 52 ; D., 2015, n° 11, p. 623 ; JCP G, 2015, n° 19, p. 927, note Bacache ; Gaz. Pal., 2015, n° 183, p. 18, comm. M. Mekki ; Gaz. Pal., 2015, n° 78, p. 26, note C. Berlaud.

⁹¹¹ LEUZZI-LOUCHART (C.), *Les devoirs du patient : l'échange réciproque d'information*, *loc. cit.*

cette exigence fait écho au devoir d'exactitude que le patient aurait à l'égard de ses données personnelles⁹¹². Cette absence d'information pourrait avoir des répercussions dramatiques sur la santé du patient. Par exemple, l'absorption de certains médicaments est incompatible avec certaines pathologies ou peut interagir avec la prise d'autres traitements. Le cas échéant, les réactions chimiques et biologiques conduisent parfois au décès du malade. Par conséquent, « *cette liberté de dire ou de ne pas dire s'accompagne, malgré tout, d'une forme de responsabilité puisqu'il est constamment admis en droit que la responsabilité naît de la liberté* »⁹¹³. Dès lors, le patient qui prend la liberté de ne pas révéler des informations fondamentales sur son état de santé est-il responsable des conséquences dommageables engendrées par son comportement ? Autrement dit, le patient est-il juridiquement responsable d'un manquement au devoir d'information ayant nuit à sa prise en charge médicale et lui ayant causé un préjudice ? La responsabilité médicale est empreinte des règles de droit commun de la responsabilité civile. Ainsi, « *de même que le contractant ne saurait se prévaloir de sa propre turpitude, le patient ne saurait reprocher au médecin les conséquences dommageables de son propre comportement déloyal* »⁹¹⁴. Cela signifie que le patient qui dissimule des informations déterminantes sur son état de santé doit en assumer les conséquences dommageables⁹¹⁵. En d'autres termes, le professionnel de santé n'a pas à répondre des conséquences dommageables induites par le comportement du patient, lequel lui est opposable devant le juge.

La faute de la victime constitue une cause d'exonération de responsabilité civile⁹¹⁶. En conséquence, « *le comportement du patient est parfois invoqué en matière de responsabilité civile au titre du partage de responsabilité, voire pour exonérer le professionnel de santé de sa responsabilité* »⁹¹⁷. Le professionnel ou l'établissement de santé doit alors démontrer que la faute de la victime présente les caractères de la force majeure

⁹¹² Cf. Paragraphe 130.

⁹¹³ *Ibid.*

⁹¹⁴ VERON (P.), *Dissimulation par la patiente de son état de santé et exclusion de la responsabilité du praticien : vers un devoir de collaboration du patient ?*, *op. cit.*, p. 603.

⁹¹⁵ CAA Nantes, 1^{ère} ch., 21 décembre 1995, n°94NT00321.

⁹¹⁶ Civ. 1^{ère}, 17 janvier 2008, n°06-20107, Bull. civ., I, n° 14 ; D., 2008, n° 18, p. 1256, note A. Dumery ; Revue Responsabilité civile et Assurances, 2008, n° 03, Mars 2008, comm. 110, C. Radé ; LPA, 2008, n°69, p. 10, note C. Youego.

⁹¹⁷ LAUDE (A.), *Le patient entre responsabilité et responsabilisation*, *op. cit.*, p. 83.

d'une part, et qu'elle a concouru à la réalisation ou à l'étendue du dommage d'autre part. Pour cela, le comportement du malade doit être fautif et doit avoir contribué au préjudice subi. Une fois prouvée, la faute de la victime peut engendrer trois conséquences. Tout d'abord, lorsque la faute est l'unique cause du dommage, elle devient totalement exonératoire : la responsabilité de l'auteur présumé ne peut donc être engagée. Ensuite, lorsque la faute a participé à causer le dommage, elle n'est que partiellement exonératoire : la responsabilité sera partagée entre l'auteur et la victime. Cela aura pour effet de réduire l'indemnisation allouée à la victime. Finalement, lorsque la victime a causé une faute, mais que cette dernière n'a aucun rôle causal dans la réalisation du dommage, elle reste sans effet sur la responsabilité originnaire de son auteur. Il en advient que « *le comportement du patient peut être une cause exonératoire de la responsabilité de l'établissement ou du professionnel de santé, ou influencer sur le montant de la réparation allouée au patient, fait ainsi application du principe de la réparation intégrale du préjudice conduisant à ce que le responsable répare le dommage qu'il a lui-même causé, et non pas celui que le patient s'est causé à lui-même* »⁹¹⁸. Le manquement du patient à son devoir d'information est donc sanctionné par une diminution de la réparation du préjudice auquel il a participé. Effectivement, « *la rétention à laquelle il [le patient] procède peut notamment justifier une mise hors de cause du médecin dont la responsabilité est recherchée, si l'erreur ou la faute qui lui est reprochée a été causée par cette absence d'information* »⁹¹⁹.

309. Néanmoins, pour être exonératoire, l'absence d'information par le patient devrait être volontaire. Partant, le patient devrait avoir adopté un comportement déloyal en se soustrayant à l'interrogatoire du professionnel de santé. Ainsi, le patient correctement questionné ne devrait pas dissimuler les informations médicales qui lui sont demandées. Également, l'absence d'information par le patient ne devrait pas résulter d'un manquement du professionnel de santé à son devoir de renseignement. En effet, « *le médecin qui ne procéderait pas à un interrogatoire consciencieux et structuré de son patient, commettrait une faute de nature à engager sa responsabilité* »⁹²⁰.

⁹¹⁸ LAUDE (A.), *Le patient entre responsabilité et responsabilisation*, op. cit., p. 84.

⁹¹⁹ LAUDE (A.), *Le patient entre responsabilité et responsabilisation*, op. cit., p. 82.

⁹²⁰ LEUZZI-LOUCHART (C.), *Les devoirs du patient : l'échange réciproque d'information*, op. cit., p. 138.

310. Depuis près de vingt ans, le patient acteur jouit d'une autonomie dans la gestion de sa santé et est devenu un collaborateur privilégié du professionnel de santé. En contrepartie, les droits octroyés au patient sont contrebalancés par des devoirs dont il a la responsabilité⁹²¹. En conséquence, si le patient bénéficie de la maîtrise *in extenso* de ses données médicales, il doit l'exercer de façon responsable, en tenant compte du devoir de collaboration à sa prise en charge médicale. En effet, le patient, devenu acteur de sa santé, doit activement contribuer au bon déroulement de sa prise en charge sanitaire, notamment en communiquant les informations personnelles sur lesquelles sera fondée toute décision médicale. Ainsi, le patient qui consent à ses soins prend la responsabilité de délivrer ses données médicales au professionnel de santé. Force est d'observer que « *l'initiative de l'empowerment peut donc découler à la fois du patient et de sa capacité à être acteur de sa santé mais également de la façon dont il va participer et échanger avec son médecin* »⁹²². La pondération de l'autodétermination informationnelle du patient sur ses données médicales résulte donc de l'avènement de la démocratie sanitaire⁹²³.

B) L'instauration d'un devoir moral de documentation du DMP par son titulaire

311. Le patient investi d'un devoir de collaboration à sa prise en charge médicale, peut, de bonne foi, oublier de mentionner des informations importantes concernant sa santé. Assurément, l'enchaînement des questions de l'interrogatoire médical additionné au stress ressenti lors de la consultation médicale peuvent perturber son attention et sa mémoire. Afin de prévenir une éventuelle omission dommageable, il apparaît opportun que les informations médicales du patient soient renseignées au sein de son DMP. Cette documentation serait notamment utile pour les situations où le patient se trouve hors d'état d'informer le professionnel de santé. Ce dernier pourrait ainsi prendre en compte l'ensemble des données médicales qu'il aurait ordinairement recueillies à l'occasion de l'interrogatoire.

Les informations correspondant au champ du devoir de collaboration incombant au patient devraient être inscrites dans son DMP. Avant la consultation, le professionnel de santé

⁹²¹ Article L.1111-1 du code de la santé publique.

⁹²² CASES (A.-S.), *L'e-santé : l'empowerment du patient connecté*, Journal de Gestion et d'Économie Médicales, vol. 35, 2017, n° 4-5, p. 142.

⁹²³ Concept faisant suite à la loi n° 2002-303 du 4 mars 2002, *loc. cit.*

pourrait prendre connaissance des données relatives aux antécédents médicaux et familiaux, aux thérapeutiques et aux allergies *via* ce carnet numérique de santé afin de concentrer son entretien sur l'anamnèse. Ce gain de temps, permis par l'usage des outils numériques, promeut l'humanisation de la relation médicale⁹²⁴. En effet, l'allègement des tâches administratives permet d'optimiser la pratique médicale et de placer le patient au cœur de la relation sanitaire. Comme le souligne le Conseil national du numérique (CNNum), « *la technicisation de la santé incite [...] à réaffirmer la place de la relation interpersonnelle et du lien social au fondement de la pratique de la médecine et du soin* »⁹²⁵. Si le DMP renferme l'historique médical de son titulaire, le professionnel de santé peut davantage se focaliser sur l'analyse des symptômes conduisant à la consultation médicale ainsi que sur l'examen clinique du malade. Le DMP constitue donc un vecteur de diffusion des données médicales du patient au profit de sa prise en charge sanitaire. En conséquence, le devoir empirique de collaborer à la prise en charge médicale induirait, pour le patient, la responsabilité de documenter son DMP.

312. Conformément à l'ambition inscrite dans la « stratégie nationale e-santé 2020 », le DMP constitue un instrument de démocratie sanitaire. En effet, cette technologie numérique permet au patient de s'impliquer dans sa prise en charge médicale et favorise son autonomie⁹²⁶. Cette volonté a été corroborée par la stratégie nationale de santé pour la période 2018-2022 avec la création de l'ENS auquel le DMP est intégré. Johanne Saison-Demars explique que « *ce nouvel espace est donc conçu comme un outil privilégié et personnalisé d'interactions entre les usagers et le système de santé. Il s'agit de faire de l'usager, malade ou non, un acteur de son parcours de santé en lui permettant de co-construire ce parcours en interaction avec les professionnels et les établissements de santé qui le prennent en charge.* »⁹²⁷. Ces dispositifs de santé numérique favorisent donc la communication des

⁹²⁴ LEQUILLERIER (C.), *L'impact de l'intelligence artificielle sur la relation de soin*, Journal de Droit de la Santé et de l'Assurance Maladie, 2017, n° 17, p. 17 à p. 18.

⁹²⁵ FAUVEL (V.), THIEULIN (B.), PA (S.), HARTMANN (C.), BERTHET (C.), BONNET (Y.), *La santé, bien commun de la société numérique*, Rapport remis par le CNNum à la Ministre Affaires sociales, de la Santé et des Droits des femmes, octobre 2015, p. 12. Disponible en ligne sur le site [www.cnnumerique.fr]. Consulté le 03 décembre 2021.

⁹²⁶ Ministère des Affaires sociales et de la Santé, *Stratégie nationale e-santé 2020, Le numérique au service de la modernisation et de l'efficacité du système de santé*, 4 juillet 2016, p.3 et p.5.

⁹²⁷ SAISON-DEMARS (J.), *Une nouvelle réforme en faveur de l'unité du système de santé*, AJDA, 2019, n°42, p. 2488.

informations médicales entre le patient et les professionnels impliqués dans sa prise en charge sanitaire. Ainsi, le devoir de collaboration du patient est amplifié par le développement de ces outils et son exercice en est facilité. Toutefois, si l'instauration d'« *un tel outil participe pleinement de l'autodétermination informationnelle des individus en proposant à ces derniers un véritable tableau de bord de leur vie numérique en santé* »⁹²⁸, le patient devrait demeurer libre de renseigner ses informations médicales dans son dossier numérique partagé. Pourtant, en tant qu'acteur occupant le rôle principal de sa prise en charge médicale, le patient n'aurait-il pas la charge d'alimenter son DMP ?

313. Selon le CNNum, « *la transformation numérique donne un nouvel écho à l'idée de responsabilisation de chacun en tant que vecteur d'augmentation du pouvoir d'agir* »⁹²⁹. Dès lors, le patient qui prend la liberté de ne pas documenter son DMP manque-t-il à son devoir de collaboration ? Autrement dit, l'absence de documentation du DMP en constitue-t-elle un manquement fautif ? Au préalable, il convient d'abord de noter que le DMP est accessible depuis l'ENS. Dans l'hypothèse où le patient jouit effectivement de ce carnet numérique de santé, son alimentation suppose une connexion à l'Internet. Seulement, Thibault Douville dénonce que « *l'accès à Internet est rattaché au droit au logement et à la lutte contre la pauvreté* »⁹³⁰. Or, il existe une corrélation entre les exclusions sociale, économique et administrative et l'exclusion numérique⁹³¹. En 2019, « *15% de la population [française] n'a pas utilisé Internet dans l'année écoulée* »⁹³², « *53% des 75 ans ou plus n'ont pas accès à Internet, comme 34 % des personnes sans diplôme ou titulaires d'un certificat d'études primaires et 16 % des plus modestes* »⁹³³. Par surcroît, « *38% des usagers d'Internet manquent de compétences numériques et 2 % n'en ont aucune* »⁹³⁴. Eu égard à l'illectronisme⁹³⁵, il paraît inconcevable d'édicter un devoir d'alimentation du DMP que

⁹²⁸ FAUVEL (V.), THIEULIN (B.), PA (S.), HARTMANN (C.), BERTHET (C.), BONNET (Y.), *op. cit.*, p. 54.

⁹²⁹ FAUVEL (V.), THIEULIN (B.), PA (S.), HARTMANN (C.), BERTHET (C.), BONNET (Y.), *op. cit.*, p. 7.

⁹³⁰ DOUVILLE (T.), HERVOCHON (C.), NOËL (E.), PAQUIER (Y.), *op. cit.*, p. 112.

⁹³¹ *Ibid.*

⁹³² LEGLEYE (S.), ROLLAND (A.), *Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base*, INSEE Première, n°1780, 30 octobre 2019.

⁹³³ *Ibid.*

⁹³⁴ *Ibid.*

⁹³⁵ Ce terme signifie l'illectronisme numérique.

l'intégralité des bénéficiaires ne serait en mesure d'honorer. L'absence de documentation du DMP ne peut donc être regardée comme une faute imputable à son titulaire. En effet, la documentation du DMP devrait être considérée comme une contribution volontaire au devoir prétorien de collaboration à la prise en charge médicale. En d'autres termes, cette documentation vise à enrichir l'information orale expliquée au professionnel de santé au cours de l'entretien individuel. La documentation du DMP constitue donc un devoir moral non sanctionnable, « dont l'exécution ne peut être poursuivie en justice, ne chargeant l'obligé que d'un devoir de conscience »⁹³⁶. Par suite, l'utilisateur des outils numériques dans le domaine de la santé devrait consciemment favoriser le renseignement son DMP.

314. Si le patient ne peut être juridiquement contraint d'alimenter son DMP, est-il juridiquement responsable des données médicales qu'il y a inscrites ? Les données médicales éditées par le titulaire du DMP ont vocation à être portées à la connaissance des professionnels concourant à sa prise en charge sanitaire. En conséquence, ces informations peuvent appuyer des décisions médicales. Seulement, qu'en est-il lorsque la donnée médicale consignée par le patient est erronée ?

Il convient de rappeler que le titulaire du DMP bénéficie de la pleine maîtrise des données personnelles dont il est l'auteur. En effet, il peut librement les rectifier ou les supprimer en se connectant à son dossier numérique. Néanmoins, les conditions générales d'utilisation du DMP spécifient que « les utilisateurs du service sont seuls responsables [...] des informations et documents qu'ils seraient susceptibles d'y ajouter les concernant »⁹³⁷. A l'instar de l'article L.1111-1 du code de la santé publique⁹³⁸, cela signifie que les prérogatives octroyées au titulaire du DMP s'accompagnent de responsabilités. S'il est concevable que le patient soit responsable de la gestion et de la mise à jour des informations dont il est l'auteur, il semble délicat de lui faire porter l'entière responsabilité de la véracité des informations médicales renseignées, nonobstant le devoir d'exactitude qui lui incomberait⁹³⁹. En tant que profane du domaine médical, il n'est pas rationnel d'attendre du patient la technicité, la

⁹³⁶ GUINCHARD (S.), DEBARD (T.), *op. cit.*, p. 368.

⁹³⁷ Article 6.2 des conditions générales d'utilisation du service DMP pour les bénéficiaires de l'assurance maladie.

⁹³⁸ « Les droits reconnus aux usagers s'accompagnent des responsabilités de nature à garantir la pérennité du système de santé et des principes sur lesquels il repose. ».

⁹³⁹ Cf. Paragraphes 130 et 178.

rigueur et la précision d'un professionnel. A titre d'exemple, le patient atteint d'une bicuspidie valvulaire aortique souffre d'un rétrécissement aortique éventuellement accompagné d'une insuffisance aortique et d'un anévrisme aortique ou d'une coarctation aortique. Tandis que cette distinction est insaisissable pour un individu non-initié, elle revêt une importance pour la prévention et le suivi du patient. Alors que la précision de cet antécédent médical apparaît capitale pour la prise en charge médicale du patient, la cristallisation de cette information dans son DMP peut lui sembler complexe et source d'erreur. Par ailleurs, si la documentation d'une allergie aux pénicillines s'avère primordiale, la mention de cette information peut sembler simple pour certains et difficile pour d'autres. Au-delà de la qualité de profane du patient, il convient donc de prendre ses capacités cognitives en considération.

315. Pourtant, le patient semble devoir assumer les conséquences dommageables engendrées par l'imprécision des informations qu'il a documentées. En droit civil français, le juge apprécie traditionnellement la faute *in abstracto*, par référence au comportement qu'une personne prudente et avisée aurait eu si elle avait été placée dans la même situation⁹⁴⁰. La faute est donc appréciée de façon objective, en comparaison avec un comportement standard, sans tenir compte des caractéristiques individuelles. Pour Philippe Brun, les infériorités individuelles doivent être écartées de l'appréciation *in abstracto* de la faute⁹⁴¹. Ce dernier considère que « *l'auteur du fait dommageable ne saurait en effet pouvoir se retrancher derrière son caractère particulièrement irritable, sa grande maladresse ou ses facultés intellectuelles limitées* »⁹⁴². Néanmoins, il n'empêche que « *le principe de l'appréciation in abstracto n'est nullement exclusif d'une « spécialisation des modèles »* »⁹⁴³. Cela signifie que le comportement du patient pourrait être objectivement comparé à celui d'un patient moyennement prudent et avisé. Si cette appréciation est concevable pour la comparaison de standards objectifs (le professionnel, le consommateur, le sportif, ...), cette approche apparaît inapplicable en matière de documentation du DMP. En effet, l'appréciation *in abstracto* du comportement du patient nécessiterait de le standardiser. Cependant, le statut du patient n'est pas systématiquement associé à une maladie. De plus, toutes les maladies ne

⁹⁴⁰ GUINCHARD (S.), DEBARD (T.), *op. cit.*, p. 555.

⁹⁴¹ BRUN (P.), *Responsabilité du fait personnel*, RDT civ., mai 2015, actu. octobre 2020, § 66.

⁹⁴² *Ibid.*

⁹⁴³ BRUN (Philippe), *op. cit.*, § 97.

présentent pas la même gravité ni la même complexité. Il appert que les patients ne souffrent donc pas du même degré de vulnérabilité. Dès lors, il semblerait cavalier de normaliser le comportement du patient sans tenir compte de ses particularités. Compte tenu de ce qui précède, l'appréciation de la faute *in concreto* ne devrait-elle pas prévaloir ?

Originellement utilisée pour apprécier le caractère intentionnel de la faute, cette appréciation subjective permet d'analyser un comportement « *à la lumière du comportement concret de l'individu, en tenant compte de ses aptitudes ou particularités* »⁹⁴⁴. Ce mode d'appréciation de la faute permettrait de considérer les caractéristiques propres au patient eu égard à ses capacités cognitives et numériques, à la nature de sa pathologie et aux données médicales qu'il pourrait raisonnablement documenter dans son DMP. Il appartiendrait donc au juge d'apprécier – concrètement – l'existence d'une faute pour chacun des cas soumis à son jugement. De la sorte, l'inscription d'une information médicale erronée dans le DMP pourrait être jugée fautive comme non fautive.

316. Ainsi, lorsque le professionnel de santé fonde sa décision médicale sur une information défectueuse, sa responsabilité peut être écartée à condition que l'erreur commise par le patient soit fautive. Toutefois, il ne faut pas méconnaître l'obligation, pour le professionnel de santé, de se renseigner avec précision sur l'état de santé du patient⁹⁴⁵. Le fait de consulter le DMP du patient ne suffirait donc pas à satisfaire cette obligation de renseignement. En effet, cette obligation impliquerait également, pour le professionnel de santé, d'analyser les données médicales documentées par le patient dans son DMP. Autrement dit, l'obligation de renseignement du professionnel de santé suppose qu'il contrôle l'exactitude des informations médicales contenues dans le DMP du patient avant de les considérer et de les traiter. Que les informations médicales soient fournies par le patient à l'occasion de l'anamnèse ou à travers son DMP, il incombe toujours au professionnel de santé de les examiner. A défaut, le professionnel de santé commettrait un manquement fautif. Effectivement, « *l'obligation d'information qui pèse sur le patient ne dispense pas pour autant le médecin de vérifier la véracité et la cohérence des allégations de son patient. Faute de quoi, il verrait à nouveau sa responsabilité engagée* »⁹⁴⁶. En d'autres termes, le

⁹⁴⁴ GUINCHARD (S.), DEBARD (T.), *op. cit.*, p. 560.

⁹⁴⁵ Cf. Paragraphe 307.

⁹⁴⁶ LEUZZI-LOUCHART (C.), *Les devoirs du patient : l'échange réciproque d'information*, *op. cit.* p. 137.

manquement fautif commis par le professionnel de santé exonère l'erreur fautive du patient. Le cas échéant, le professionnel de santé ne peut invoquer l'erreur de la victime et redevient pleinement responsable du dommage causé au patient.

Il apparaît que la responsabilité du patient à l'égard des informations documentées dans son DMP est considérablement atténuée. Au demeurant, la responsabilité du titulaire du DMP peut épisodiquement être engagée dans l'hypothèse d'une dissimulation intentionnelle d'informations au moment de leur vérification par le professionnel de santé. Il paraît utile de rappeler que les informations documentées dans le DMP par son titulaire sont complémentaires à celles renseignées lors de l'entretien individuel. L'exercice de ce devoir moral permet de renforcer l'information due au professionnel de santé et de palier d'éventuelles omissions ou inattentions. Partant, la consultation du DMP et la vérification des informations qu'il contient devraient être effectuées au cours de la consultation médicale. De cette façon, le professionnel de santé pourrait parachever l'interrogatoire médical et exécuter son obligation de renseignement auprès du patient.

317. Cependant, le devoir moral de documentation du DMP, exercé au nom de la collaboration à la prise en charge médicale, n'a de sens que lorsque son titulaire autorise les professionnels de santé à y accéder. Corrélativement, l'obligation de renseignement incombant au professionnel de santé ne peut être exécutée au moyen du DMP, après vérification des informations documentées, que s'il est autorisé à y accéder. Conséquemment, le patient aurait-il le devoir de permettre le partage de ses données médicales ?

Paragraphe 2 : La renonciation du patient concerné à la plénitude de ses droits

« Les technologies de l'internet et les espaces numériques qu'elles ont engendrés n'invitent pas seulement les juristes à l'exploration et à la conquêtes d'une nouvelle terra incognita ; ils transforment de l'intérieur, voire dérèglent, les conditions d'exercice des droits fondamentaux et les mécanismes traditionnels de leur conciliation. »⁹⁴⁷.

318. Le devoir de collaboration à la prise en charge médicale suppose que le patient ne s'oppose pas aux traitements de données nécessaires à la dispensation des soins auxquels il a consentis (**A**). Assurément, l'exercice des droits du patient sur ses données personnelles ne doit pas entraver la prestation de services délivrée par le professionnel de santé. Néanmoins, les restrictions des droits du patient sur ses données médicales ne constituent-elles pas une atteinte à son droit à l'autodétermination informationnelle (**B**) ?

A) Le devoir de non-opposition à la communication des données médicales entre professionnels

319. Par principe, le patient maîtrise la communication de ses données médicales entre les professionnels concourant à sa prise en charge sanitaire. Hormis les cas exhaustifs où le législateur l'exige⁹⁴⁸, le patient dispose du droit de faire obstacle à la circulation de ses informations médicales. Le cas échéant, les professionnels ne peuvent échanger ou partager les données médicales essentielles à la dispensation des actes de prévention, de diagnostic et de soins, ou nécessaires au suivi médico-social et social de la personne concernée. Il en résulte que l'opposition à la communication des données médicales va à l'encontre du devoir de collaboration à la prise en charge sanitaire. Assurément, le patient qui s'oppose à la communication de ses données médicales compromet la continuité et la coordination de ses soins. Mais alors, pourquoi le patient qui consent librement à être soigné entraverait-il la réalisation des services de soins de santé ? A l'évidence, l'obstacle à la communication de

⁹⁴⁷ CE, *Le numérique et les droits fondamentaux*, Les rapports du Conseil d'Etat, Avant-propos de Jean-Marc Sauvé, 2014, p. 5.

⁹⁴⁸ Cf. Paragraphes 295 à 299.

ses informations médicales est contraire à la volonté d'être pris en charge, *a fortiori* à l'heure où les parcours de santé sont globalisés.

Cette contradiction s'explique-t-elle par la méfiance de la personne concernée à l'égard du traitement de ses données sensibles ? Pourtant, les conditions de l'échange et du partage des informations médicales du patient sont rigoureusement encadrées par le législateur. En effet, les professionnels participant à sa prise en charge ne peuvent transmettre que les seules informations strictement nécessaires à la coordination ou à la continuité de ses soins et limitées au périmètre des missions respectives aux intervenants⁹⁴⁹. Autrement dit, la communication des données médicales du patient doit toujours être indispensable à sa prise en charge sanitaire ou sociale et intervient systématiquement dans l'intérêt de sa santé ainsi que dans le respect du secret professionnel médical.

320. Finalement, l'entrave du patient à la communication de ses données médicales ne correspondrait-elle pas à la crainte de la divulgation du secret professionnel médical ? En effet, la circulation des données médicales du patient entre les professionnels concourant à sa prise en charge sanitaire revient à diffuser des informations confidentielles. Les données médicales d'un individu correspondent à des informations portant sur l'intimité de sa vie privée et touchant à sa dignité ainsi qu'à son humanité. Ces éléments immatériels de son corps humain sont générés à l'occasion d'un examen clinique, médical ou paramédical, prodigué dans le cadre d'un colloque singulier. Autrement dit, ces données authentiques sont recueillies et produites dans un cadre de confiance légalement sanctuarisé.

Afin de préserver la confiance de la relation sanitaire, les données médicales confiées au professionnel de santé sont, par nature, confidentielles. En effet, le professionnel intervenant dans le système de santé est dépositaire du secret concernant les informations médicales dont le patient est titulaire⁹⁵⁰. Toutefois, « *spécialisation et travail en équipe conduisent, sinon à remettre en cause, du moins à revisiter le colloque singulier qui fait parfois place à un colloque pluriel* »⁹⁵¹. En conséquence, l'élargissement des contours du secret professionnel médical et l'extension de ses dépositaires semblent remettre en cause les

⁹⁴⁹ Article R.1110-1 du code de la santé publique.

⁹⁵⁰ Cf. Paragraphe 193.

⁹⁵¹ VIALLA (F.), *Le secret partagé*, RDS, 2016, n°2, p. 53.

préceptes du colloque singulier, sacerdoce de la relation médicale. Depuis, les données médicales du patient peuvent être communiquées à des professionnels avec lesquels le patient n'a lié aucune relation, ni instauré aucune confiance. Dès lors, comment appréhender l'adage selon lequel « *il n'y a pas de médecine sans confiance, de confiance sans confidence et de confidence sans secret* »⁹⁵² ?

321. Alors que les données médicales du patient sont communiquées à des professionnels soumis à une obligation légale de secret professionnel, il n'empêche que cette diffusion d'informations confidentielles peut être vécue comme une trahison de la confiance accordée à un professionnel de santé déterminé. Il semble alors légitime que le patient soit « *maître des informations médicales le concernant : il peut choisir qui pourra avoir accès à ses informations médicales et peut imposer au professionnel de santé un secret absolu quant à celles-ci* »⁹⁵³. Le secret professionnel médical, en tant que « *base irremplaçable et indispensable du lien entre le médecin et le malade* »⁹⁵⁴ et « *clé de voute de la relation et de l'efficacité médicales* »⁹⁵⁵, doit absolument être préservé. En revanche, il n'en demeure pas moins que la communication des informations médicales nécessaires à l'exercice de l'art médical, autorisée par le législateur, doit être permise par le patient.

Le patient aurait alors le devoir de ne pas s'opposer à la communication de ses données médicales entre les professionnels participant à sa prise en charge sanitaire. En d'autres termes, le devoir de collaboration du patient à sa prise en charge médicale commande une renonciation de son droit d'opposition à l'échange et au partage de ses informations intimes entre les professionnels y étant impliqués. Axel Saint Martin alerte que « *l'exercice de cette prérogative sera toujours, en pratique, limitée par les sanctions qui peuvent être attachées à son exercice* »⁹⁵⁶. Si le patient reste libre de la maîtrise du secret médical à travers la limitation de la communication de ses données médicales, il doit cependant en assumer les

⁹⁵² PORTES (L.), *loc. cit.*

⁹⁵³ SAINT MARTIN (A.), *Le secret médical et le patient (I) le patient (a priori) maître du secret professionnel médical, op. cit.*, p. 111.

⁹⁵⁴ KAHN (Axel), *Le secret médical : d'Hippocrate à internet*, Recueil Dalloz, 2009, n°39, p.2626.

⁹⁵⁵ *Ibid.*

⁹⁵⁶ SAINT MARTIN (A.), *Le secret médical et le patient (I) le patient (a priori) maître du secret professionnel médical, loc. cit.*

éventuelles conséquences dommageables. En conséquence, le manquement à ce devoir serait, à nouveau, considéré comme fautif.

322. L'opportunité de l'instauration d'un devoir de non-opposition est parfaitement illustrée à travers la téléexpertise médicale. Nous avons démontré que le patient ayant consenti à l'acte de téléexpertise pouvait néanmoins contester la circulation de ses données médicales entre le médecin requérant et le téléexpert requis⁹⁵⁷. Le patient a donc le droit d'opposer le secret médical aux téléprofessionnels de santé nonobstant leur soumission à ce secret professionnel. Seulement, le téléexpert requis ne peut rendre son avis que sur la base des informations médicales envoyées par le médecin requérant *via* une messagerie sécurisée de santé. En effet, l'avis du téléexpert requis dépend de la bonne transmission des données médicales du patient. Par conséquent, « *le médecin requérant est [...] responsable de la pertinence et de la qualité des informations livrées à son confrère* »⁹⁵⁸. Cependant, lorsque le téléexpert requis estime manquer d'informations nécessaires à l'effectuation de son acte, celui-ci doit solliciter un complément d'informations auprès du médecin requérant⁹⁵⁹. A défaut d'informations qualitatives suffisantes, le téléexpert requis devrait refuser de rendre un avis, faute de quoi sa responsabilité pourrait être engagée.

L'analyse des données médicales échangées à l'occasion de la téléexpertise représente un enjeu important en matière de responsabilité médicale. Ainsi, lorsque l'avis du téléexpert est erroné en raison d'un défaut de transmission des informations nécessaires à l'acte de téléexpertise, la responsabilité du médecin requérant pourrait également être retenue. Dès lors, médecin requérant et médecin requis partageraient la responsabilité du dommage subi par le patient. En somme, les deux protagonistes auraient la responsabilité de veiller à la pertinence des informations médicales échangées dans le cadre de la téléexpertise médicale. Toutefois, qu'en est-il lorsque le patient s'est opposé à la transmission, en tout ou partie, de ses données médicales ?

Dans le contexte de la téléexpertise médicale, l'exercice du droit d'opposition à l'échange des données apparaît contraire au devoir de collaboration du patient. En effet,

⁹⁵⁷ Cf. Paragraphe 298.

⁹⁵⁸ CORGAS-BERNARD (C.), *op. cit.*, p. 27.

⁹⁵⁹ FERRAUD-CIANDET (N.), *Droit de la télésanté et de la télémedecine*, Heures de France, p. 127.

l'exercice de ce droit par le patient empêcherait la bonne réalisation de l'acte de télémedecine. Ainsi, l'opposition du patient à la transmission des données nécessaires à la téléexpertise peut être à l'origine d'un dommage consécutif à la réalisation de cet acte médical. Le cas échéant, le manquement du patient au devoir de non-opposition pourrait exonérer, totalement ou partiellement, la responsabilité des téléprofessionnels de santé.

323. Néanmoins, dans l'hypothèse où le patient entraverait la communication de ses données médicales, le médecin requérant ne devrait-il pas renoncer à l'acte de téléexpertise médicale ? Lorsque le médecin doute de son diagnostic, il lui incombe l'exigence déontologique⁹⁶⁰ et prétorienne⁹⁶¹ de faire appel à l'aide de tiers compétents et de concours appropriés. Le patient ne peut alors contrarier l'obligation, pour le médecin, de recourir à l'avis d'un professionnel de santé compétent. En revanche, le patient peut-il s'opposer à la transmission des données médicales utiles à cette fin ? Le recours à un tiers compétent étant fondé sur une obligation déontologique incombant au médecin requérant, le fondement juridique de cette opération de traitement repose sur une *obligation légale* à laquelle le responsable de traitement est soumis⁹⁶². Par conséquent, la personne concernée par le traitement de ses données médicales ne devrait pouvoir s'y opposer. Compte tenu de cette injonction normative, le patient ne peut faire obstacle à la transmission des informations nécessaires à l'obtention d'une aide médicale appropriée. Dans ces conditions, le patient serait-il obligé de consentir à l'acte de téléexpertise ?

La téléexpertise constitue un acte médical relevant de la télémedecine. A ce titre, aucun acte de téléexpertise médicale ne peut être pratiqué sans le consentement libre et éclairé du patient⁹⁶³. Le patient peut donc refuser le recours à la téléexpertise sans préjudice, pour le médecin, de recourir à une aide appropriée. En effet, la téléexpertise médicale constitue simplement un moyen, pour le médecin, de satisfaire à cette obligation. Ainsi, le recours à un professionnel de santé compétent doit être qualifié d'acte de *téléexpertise médicale* uniquement lorsque cet avis est sollicité à distance, par le biais des technologies de

⁹⁶⁰ Articles R.4127-32 et R.4127-33 du code de la santé publique.

⁹⁶¹ Civ. 1^{ère}, 27 novembre 2008, n°07-15.963, Bull. civ., I ; D., 2008, n° 44, p. 3085 ; Gaz. Pal., 2009, n° 71, p. 47, note V. Vuailat ; D., 2009, n° 19, p. 1302, obs. J. Penneau ; LPA, 2009, n° 178, p. 7, note F. Dekeuwer-Defossez.

⁹⁶² Cf. Paragraphe 109.

⁹⁶³ Article R.6316-2 du code de la santé publique.

l'information et de la communication⁹⁶⁴. Dans ce cas, la dispensation de cet acte doit s'inscrire dans les limites des règles relatives à la télémedecine. Par suite, le patient conserve le droit d'objecter l'acte de téléexpertise ainsi que le droit de refuser la transmission de ses données médicales. Si le médecin a l'obligation de recourir à un tiers lorsqu'il doute d'un diagnostic, aucun texte normatif ne l'oblige à recourir à la téléexpertise médicale. En pratique, le Conseil national de l'Ordre des médecins considère que l'obligation de recourir à un tiers compétent « implique que le médecin choisisse soigneusement, et en vertu de leurs seules compétences, les confrères auxquels il présentera ou adressera son patient, avec l'accord de celui-ci »⁹⁶⁵. Lorsque le patient conteste la communication des éléments immatériels de son corps humain dans le cadre de la téléexpertise médicale, le médecin peut remplir son obligation en l'adressant chez un confrère libéral ou hospitalier⁹⁶⁶. Dans ce contexte, les informations médicales du patient seront échangées par les professionnels de santé à travers les lettres de liaison, et seront, le cas échéant, accessibles sur le DMP du patient concerné⁹⁶⁷. Dans cette hypothèse, le patient aurait le devoir de permettre les accès à son DMP ainsi qu'aux informations qu'il contient.

324. L'interdiction de l'accès au DMP, opposée aux professionnels participant à la prise en charge sanitaire du patient, tend à contrarier la coordination et la continuité de ses soins. En effet, cette interdiction empêche le partage simultané de ses données médicales entre l'ensemble des acteurs intervenant dans son parcours de santé. A l'inverse, le titulaire du DMP ne devrait-il pas favoriser la communication des éléments immatériels de son corps humain aux professionnels dépositaires du secret professionnel médical ?

Afin de restreindre l'exercice de ce droit d'interdiction, la proposition de loi instaurant le DMP prévoyait initialement que « *le remboursement des soins par l'assurance maladie dépend[rait] de l'autorisation donnée par le patient au médecin d'accéder au dossier*

⁹⁶⁴ Arrêté du 28 avril 2016 portant cahier des charges des expérimentations relatives à la prise en charge par téléconsultation ou téléexpertise mises en œuvre sur le fondement de l'article 36 de la loi n° 2013-1203 de financement de la sécurité sociale pour 2014, *JORF* n°105, 5 mai 2016, texte n° 20.

⁹⁶⁵ Commentaire de l'article 33 du code de déontologie médicale. Disponible en ligne sur le site [www.conseil-national.medecin.fr]. Consulté le 13 novembre 2020.

⁹⁶⁶ Commentaire de l'article 32 du code de déontologie médicale. Disponible en ligne sur le site [www.conseil-national.medecin.fr]. Consulté le 13 novembre 2020.

⁹⁶⁷ Cf. Paragraphe 297.

médical »⁹⁶⁸. Bien que cette disposition n'ait pas été retenue par le législateur, « *il n'en demeure pas moins qu'elle marque la volonté de contraindre le bénéficiaire du secret médical à renoncer à celui-ci* »⁹⁶⁹. Seulement, l'accès du professionnel au DMP du patient intervient dans les limites de sa prise en charge sanitaire et, subséquent, du secret professionnel médical. La renonciation à la modulation des accès au DMP n'emporte donc aucune renonciation au secret. Assurément, l'ensemble des données médicales formalisées dans le DMP du patient sont limitativement accessibles aux professionnels en considération du périmètre de leur mission. Le professionnel qui accéderait à une donnée médicale qui ne serait pas strictement nécessaire à la prise en charge du titulaire de ce dossier digitalisé commettrait une violation du secret professionnel et porterait atteinte à la vie privée de l'intéressé. Dans le respect de la confidentialité de ces données intimes, des mesures contraignantes pourraient donc inciter le patient à collaborer activement à sa prise en charge sanitaire. Eventuellement, il devrait faciliter la circulation sécurisée de ses données médicales, *via* ce carnet numérique de santé, dans l'objectif de promouvoir la prévention, la coordination, la qualité et la continuité de ses soins.

325. Egalement, le titulaire du DMP devrait limiter le masquage des informations médicales qui y sont colligées. En pratique, « *ce masquage est à la seule initiative du patient qui pourrait, pour des motifs d'ordre personnel, dissimuler une information dont il ignore le caractère essentiel au plan médical* »⁹⁷⁰. Eu égard à l'instauration empirique d'un devoir de renseignement à la charge du patient, le titulaire du DMP devrait donc autoriser l'accès à l'ensemble des données médicales utiles à la coordination de son parcours de santé. A défaut, le patient devrait assumer les conséquences dommageables causées par la dissimulation volontaire des données médicales essentielles à sa prise en charge sanitaire. En ce sens, les dispositions de l'article L.1111-15 du code de la santé publique affirment que « *la responsabilité du professionnel de santé ne peut être engagée en cas de litige portant sur l'ignorance d'une information qui lui était masquée dans le dossier médical partagé et dont il ne pouvait légitimement avoir connaissance par ailleurs* »⁹⁷¹.

⁹⁶⁸ SAINT MARTIN (A.), *Le secret médical et le patient (II)*, RDS, 2010, n° 36, p. 327.

⁹⁶⁹ *Ibid.*

⁹⁷⁰ BOURDAIRE-MIGNOT (C.), *2018 : l'année du DMP pour tous ?*, *op. cit.*, p. 29.

⁹⁷¹ Article L.1111-15 alinéa 1 du code de la santé publique.

326. En conséquence, Sylvie Hennion remarque que l'interdiction de l'accès au DMP et le masquage des informations qu'il contient mettraient « *en cause tout le système numérique ou d'échange entre professionnels et, en réalité, le patient aura le choix entre se faire soigner et accepter le partage d'information ou refuser le soin* »⁹⁷². Dans le contexte d'une prise en charge sanitaire, il existe indéniablement un conflit entre le droit à la santé, la portée des droits du patient sur ses données médicales, et son devoir de collaboration à son parcours de santé.

B) La remise en cause de l'autodétermination du patient concerné par le traitement de ses données médicales

327. L'instauration de devoirs à la charge du patient porte-t-elle atteinte au principe de l'autodétermination informationnelle dont bénéficie tout individu ? En pratique, les droits du patient sur ses données médicales font l'objet de restrictions. En effet, le patient ne peut librement modifier ses informations médicales⁹⁷³, ni véritablement s'opposer à leur circulation entre les professionnels participant à sa prise en charge⁹⁷⁴. A l'inverse, le patient aurait davantage le devoir de les renseigner et d'en permettre la communication. Partant, cette prescription semble contraire au droit, pour l'individu, de maîtriser les informations le concernant. Pourtant, cette limitation ne doit pas être regardée comme une atteinte au droit fondamental à la protection des données personnelles.

Véritablement, toute personne bénéficiant d'une prise en charge sanitaire dispose des qualités de *patient* et de *personne concernée*. Ces deux statuts sont créateurs de droits fondamentaux qu'il convient d'articuler selon un principe de proportionnalité, et de contrebalancer par la responsabilisation de leur titulaire. Autrement dit, l'autodétermination informationnelle du patient se trouve limitée en raison de la collision des droits fondamentaux à la santé et à la protection des données personnelles d'une part **(1)**, et de l'instauration de devoirs en contrepartie du renforcement de ces droits d'autre part **(2)**.

⁹⁷² HENNION (S.), *Le partage du secret professionnel à l'ère du numérique*, op. cit., p. 132.

⁹⁷³ Cf. Section 2 du Chapitre 2 du Titre 1 de la Première partie de la présente thèse.

⁹⁷⁴ Cf. Chapitre 2 du Titre 2 de la Première partie de la présente thèse.

1. La collision entre le droit fondamental à la santé et le droit fondamental à la protection des données personnelles

328. En premier lieu, il s'agit de résoudre le conflit entre les droits fondamentaux du *patient* et les droits fondamentaux de la *personne concernée*. La résolution de ce conflit ne relève pas de l'évidence dans la mesure où, dans le cadre de la prise en charge sanitaire, ces deux catégories de droits appartiennent à une seule et unique personne physique.

329. D'abord, l'individu qui consulte un professionnel de santé dispose du statut de *patient* et bénéficie, à ce titre, de droits particuliers.

D'une façon générale, toute personne jouit du droit à la protection de la santé⁹⁷⁵. A l'échelle de l'Union européenne, ce droit fondamental trouve sa source à l'article 35 de la Charte des droits fondamentaux de l'Union européenne⁹⁷⁶, à laquelle le Traité de Lisbonne⁹⁷⁷ a conféré une valeur juridique contraignante. Etant ancré dans l'ordre juridique de l'Union européenne, son respect s'impose aux institutions, aux organes et aux organismes de l'Union ainsi qu'aux États membres⁹⁷⁸. En droit interne, ce droit fondamental dispose d'une valeur constitutionnelle. D'une part, le droit à la protection de la santé est consacré dans le Préambule de la Constitution du 27 octobre 1946⁹⁷⁹, lequel est intégré dans le « bloc de constitutionnalité »⁹⁸⁰. D'autre part, il a été reconnu comme l'un des principes fondamentaux

⁹⁷⁵ CASAUX-LABRUNEE (L.), *Le droit à la santé*, In CABRILLAC (R.), *Libertés et droits fondamentaux 2021*, Dalloz, 27^e ed., 2021, p. 942 à p. 943.

⁹⁷⁶ L'article 35 de la CDFUE dispose : « *Toute personne a le droit d'accéder à la prévention en matière de santé et de bénéficier de soins médicaux dans les conditions établies par les législations et pratiques nationales. Un niveau élevé de protection de la santé humaine est assuré dans la définition et la mise en œuvre de toutes les politiques et actions de l'Union* ».

⁹⁷⁷ Traité de Lisbonne modifiant le traité sur l'Union européenne, le traité instituant la Communauté européenne et certains actes connexes, signé à Lisbonne le 13 décembre 2007.

⁹⁷⁸ Article 51 de la CDFUE.

⁹⁷⁹ L'alinéa 11 du Préambule de la Constitution du 27 octobre 1946 dispose : « *Elle [la République] garantit à tous, notamment à l'enfant, à la mère et aux vieux travailleurs, la protection de la santé, la sécurité matérielle, le repos et les loisirs. Tout être humain qui, en raison de son âge, de son état physique ou mental, de la situation économique, se trouve dans l'incapacité de travailler a le droit d'obtenir de la collectivité des moyens convenables d'existence.* ».

⁹⁸⁰ Le Conseil constitutionnel contrôle de la constitutionnalité interne et externe des lois conformément au bloc de constitutionnalité, à savoir la Constitution du 4 octobre 1958 ainsi que les textes et les principes intégrés dans son Préambule : la Déclaration des droits de l'homme et du citoyen de 1789, le Préambule de la Constitution de 1946, la Charte de l'environnement de 2004, les principes fondamentaux reconnus par les lois de la République et les principes particulièrement nécessaires à notre temps.

reconnus par les lois de la République⁹⁸¹. En outre, le Conseil constitutionnel a qualifié ce droit fondamental « *d'objectif à valeur constitutionnelle* »⁹⁸², dont la mise en œuvre appartient au législateur compte tenu d'une obligation de moyens. Si la Constitution garantit le droit à la protection de la santé, le législateur en garantit l'effectivité. Certainement, il ne fait aucun doute qu'« *un « droit à » sans effet est un droit en sommeil, affirmé mais lettre morte* »⁹⁸³. Laurence Gay explique que « *le texte fondamental proclame un droit mais ce droit n'existera éventuellement que dans le cadre de la loi* »⁹⁸⁴. Pour parvenir à cet objectif constitutionnel, le législateur a donc inscrit ce droit à l'article L.1110-1 du code de la santé publique. Il est ainsi affirmé que « *le droit fondamental à la protection de la santé doit être mis en œuvre par tous moyens disponibles au bénéfice de toute personne* ». Il convient de noter que cet article est codifié dans le chapitre préliminaire dédié aux « *droits de la personne* », lequel est inséré au sein du titre consacré aux « *droits des personnes malades et des usagers du système de santé* ».

D'une façon plus particulière, le droit fondamental à la protection de la santé est principalement concrétisé par les droits des malades depuis la loi du 4 mars 2002⁹⁸⁵. Dès lors, le patient peut décider de bénéficier de soins de qualité, qui lui seront délivrés sans discrimination, dans le respect de sa dignité et dans la confidentialité. Ainsi, le droit fondamental à la santé est notamment activé par l'exercice des droits subjectifs octroyés au patient. Le patient est alors devenu un acteur aux commandes de sa santé. La protection du droit fondamental à la santé apparaît donc renforcée par l'instauration de normes de concrétisation. Au demeurant, la matérialisation de ce droit, à travers la prise en charge médicale d'un individu, implique le traitement de ses données médicales personnelles.

330. Ensuite, l'individu qui consulte un professionnel de santé jouit du statut de *personne concernée*. En effet, la mise en œuvre du droit à la santé entraîne subséquentement la mise en

⁹⁸¹ Cons. Const., Décision n° 74-54 DC, 15 janvier 1975 : D., 1975, p. 529, note Hamon.

⁹⁸² Cons. Const., Décision n° 93-325 DC, 13 août 1993 : D., 1994, n° 13, p. 111, obs. D. Maillard Desgrées du Loû ; Dr. soc., 1994, n° 01, p. 69, étude J.-J. Dupeyroux et X. Prétot ; RFDA, 1993, n° 05, p. 871, note B. Genevois ; Rev. crit. DIP, 1994, n° 01, p. 01, ét. D. Turpin ; Cons. Const., Décision n° 90-283 DC, 8 janvier 1991 : RDSS, 1991, n°02, p. 204, J.-S. Cayla ; AJDA, 1991, n° 05, p. 382, comm. P. Wachsmann.

⁹⁸³ CASAUX-LABRUNEE (L.), *op. cit.*, p. 930.

⁹⁸⁴ GAY (L.), *La notion de « droits-créances » à l'épreuve du contrôle de constitutionnalité*, Cahiers du conseil constitutionnel, juin 2004, n° 16.

⁹⁸⁵ Loi n° 2002-303 du 4 mars 2002, *loc. cit.*

œuvre d'un traitement de données personnelles, indispensable à la réalisation de cet objectif. Autrement dit, la mise en œuvre du traitement des données médicales du patient découle de l'activation de son droit fondamental à la santé. Assurément, le professionnel de santé a l'obligation technique de collecter et d'analyser les données médicales du patient qu'il prend en charge. Le traitement des données médicales du patient constitue donc une condition *sine qua non* de la concrétisation du droit fondamental à la santé par sa prise en charge sanitaire. En conséquence, le patient, en sa qualité de personne concernée, bénéficie du droit à la protection de ses données personnelles.

La Charte des droits fondamentaux de l'Union européenne a érigé le droit à la protection des données personnelles au rang des droits fondamentaux. Son article 8 dispose que « *toute personne a droit à la protection des données à caractère personnel la concernant* ». Concrètement, « *cette disposition fondamentale est traduite par des textes européens de droit dérivé récents* »⁹⁸⁶. En effet, le droit à la protection des données est singulièrement garanti par le RGPD et plus précisément par les droits de la personne concernée qu'il est venu renforcer. « *Outre le droit à l'information, le droit d'accès et de rectification, le droit d'opposition ou encore le droit de ne pas faire l'objet d'une décision algorithmique, le RGPD a surtout reconnu de nouvelles prérogatives : le droit à l'oubli ou droit à l'effacement et le droit à la portabilité* »⁹⁸⁷. Vraisemblablement, ces droits subjectifs, que la personne concernée détient sur ses données personnelles, concrétisent le concept fondamental de l'autodétermination informationnelle dégagé par la Cour constitutionnelle fédérale d'Allemagne⁹⁸⁸. En effet, « *la consécration d'un principe d'autodétermination informationnelle vise à dépasser une conception abstraite de la protection des données à caractère personnel des individus pour la recentrer sur la liberté de l'individu, en lui donnant les moyens d'être aux commandes de sa vie numérique* »⁹⁸⁹. Autrement dit, le principe de l'autodétermination informationnelle « *donne sens à tous ces droits, qui tendent à le garantir*

⁹⁸⁶ BENSAMOUN (A.), *Droits fondamentaux et internet*, In CABRILLAC (R.), *Libertés et droits fondamentaux 2021*, op. cit., p. 322.

⁹⁸⁷ *Ibid.*

⁹⁸⁸ Cour constitutionnelle fédérale allemande, 15 décembre 1983, « *la constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel* ».

⁹⁸⁹ FAUVEL (V.), THIEULIN (B.), PA (S.), HARTMANN (C.), BERTHET (C.), BONNET (Y.), op. cit., p. 49.

*et doivent être interprétés et mis en œuvre à la lumière de cette finalité »*⁹⁹⁰. Le principe de l'autodétermination informationnelle est donc intrinsèquement lié au droit fondamental à la protection des données personnelles dont l'effectivité est notamment assurée grâce aux droits conférés par le RGPD.

En droit interne, le principe de l'autodétermination informationnelle « *a été implicitement consacrée dans la loi pour une République numérique du 7 octobre 2016, modifiant ici la loi Informatique et libertés »*⁹⁹¹. Désormais, le premier article de la loi Informatique et Libertés modifiée atteste que les personnes concernées disposent des droits « *de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant »* conformément aux dispositions du RGPD. En effet, la protection des « *libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel »*⁹⁹², est garantie par ce règlement européen qui se trouve directement applicable dans l'ordre juridique interne aux Etats membres de l'Union européenne. Dès lors, la personne concernée est censée détenir les commandes de sa vie numérique et joue le rôle principal dans le traitement de ses données personnelles.

331. Compte tenu de ce qui précède, le patient qui exerce son droit fondamental à la santé bénéficie conséquemment du droit fondamental à la protection de ses données médicales. En théorie, le patient serait donc libre de décider et de contrôler leur usage dans le cadre de sa prise en charge sanitaire. Dans la mesure où « *le droit à l'autodétermination informationnelle permet [...] d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté »*⁹⁹³, le patient devrait jouir de l'entière des droits consacrés par le RGPD. Seulement, l'exercice des droits du patient sur ses données médicales peut entraver sa prise en charge sanitaire et ainsi porter atteinte à l'exercice de son droit fondamental à la santé. Pourtant, l'activation du droit à la protection des données personnelles fait suite à l'activation du droit à la santé. Logiquement, la mise en œuvre du droit à la protection des données ne devrait donc pas faire obstacle à la réalisation du droit à la santé. Dès lors, la limitation des droits du

⁹⁹⁰ CE, *Étude annuelle 2014 : le numérique et les droits fondamentaux*, Documentation française, 2014, p. 267 et s. Disponible en ligne sur le site [www.conseil-etat.fr]. Consulté le 03 décembre 2021.

⁹⁹¹ BENSAMOUN (A.), *op. cit.*, p. 323.

⁹⁹² Article 1.2 du RGPD.

⁹⁹³ MARTIAL-BRAZ (N.), *Le renforcement des droits de la personne concernée*, Dalloz IP/IT, 2017, n°05, p.253.

patient sur ses données personnelles apparaît comme une nécessité imparable, sans laquelle les professionnels de santé, débiteurs du droit à la santé, ne sauraient le concrétiser. Néanmoins, est-il admissible de prioriser un droit fondamental sur un autre ? Effectivement, « *le fait que le droit de la protection des données personnelles constitue une garantie fondamentale au profit de l'individu pose également la question de savoir si l'individu peut y renoncer* »⁹⁹⁴.

332. Il apparaît que l'exercice des droits du patient sur ses données médicales tend à écorner son droit fondamental à la santé. De la même façon, l'exercice effectif du droit à la santé tend à limiter l'exercice des droits que le patient détient sur ses données médicales. Ces limitations proviennent intrinsèquement de l'exercice de ces deux catégories de droits allouées au patient. Ainsi, il existe un conflit entre les intérêts d'une même personne physique. Assurément, le patient ne peut exercer cumulativement les droits qui lui sont conférés par le RGPD et par le code de la santé publique sans limiter la portée de ses droits fondamentaux. Seulement, le droit à la santé et le droit à la protection des données bénéficient de la même valeur normative. Si « *déterminer la valeur d'un principe [...] c'est mesurer dans l'ordre juridique sa force* »⁹⁹⁵, aucune primauté d'un droit fondamental sur un autre n'est envisageable. En effet, Christophe Caron affirme que « *si l'ensemble des prérogatives répond à la qualification de droit fondamental, elles bénéficient toutes d'une grande valeur. Il devient alors impossible d'établir une quelconque hiérarchie entre eux* »⁹⁹⁶. Il convient donc d'articuler les libertés et les droits fondamentaux reconnus par la Charte des droits fondamentaux de l'Union européenne à la lumière du principe de proportionnalité envisagé en son article 52⁹⁹⁷. Certainement, « *la proportionnalité impose un jeu de balance pour décider le conflit de principes inconciliables entre eux* »⁹⁹⁸. Alors, la résolution de ce conflit

⁹⁹⁴ DANIS-FATOME (A.), *Ordre public et protection des données à caractère personnel*, AJ contrat, 2019, n°8 et n°9, p.366.

⁹⁹⁵ CASAUX-LABRUNEE (L.), *op. cit.*, p. 921.

⁹⁹⁶ CARON (C.), *Utilisation de la « balance des intérêts » pour résoudre les conflits de droits fondamentaux*, Recueil Dalloz, 2004, n°23, p. 1633.

⁹⁹⁷ Selon l'article 52 alinéa 1 de la CDFUE, « *Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.* ». En l'espèce, nous transposons ce principe afin de résoudre le conflit entre les droits fondamentaux appartenant à une même personne physique.

⁹⁹⁸ PAMBOUKIS (H.), *Acte public étranger*, Répertoire de droit international, septembre 2019, § 89.

implique de trouver un équilibre par la mise en balance des intérêts du patient, tout en préservant le contenu essentiel du droit dont la portée se trouvera limitée.

333. D'une part, le droit à la santé tend à la protection de la vie humaine consacrée par l'article 2 de la Convention européenne des droits de l'homme. En effet, la Cour européenne des droits de l'homme a considéré que les autorités d'un Etat qui refuseraient l'accès d'une personne aux soins médicaux – qu'elles se sont engagées à délivrer à l'ensemble d'une population – porteraient atteinte au droit au respect de la vie⁹⁹⁹. D'autre part, le droit à la protection des données personnelles vise à protéger l'intimité de la vie privée des individus. Néanmoins, le quatrième considérant du RGPD précise 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* »¹⁰⁰⁰. Dans le contexte d'une prise en charge sanitaire, le droit à la protection des données médicales doit donc être concilié avec le droit à la santé. Compte tenu de ce qui précède, la limitation des droits du patient sur ses données médicales personnelles apparaît proportionnellement légitimé par la protection de sa vie, objectif par le droit fondamental à la santé. Dès lors, la limitation des droits du patient sur ses données médicales constitue la solution la plus protectrice de l'intérêt le plus légitime¹⁰⁰¹.

334. De surcroît, la limitation des droits de la personne concernée ne porte pas atteinte à la substance du droit à la protection des données. En premier lieu, le traitement des données médicales concernant le patient est exceptionnellement autorisé aux fins de sa prise en charge sanitaire¹⁰⁰². Cette dérogation est accordée « *si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel [...] ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret* »¹⁰⁰³. La confidentialité des données médicales et le respect de l'intimité de la vie privée demeurent

⁹⁹⁹ CEDH, Gr. ch., 10 mai 2001, n° 25781/94.

¹⁰⁰⁰ Considérant 4 du RGPD.

¹⁰⁰¹ Civ. 1^{ère}, 30 septembre 2015, n° 14-16.273, Bull. civ., I, n° 228 ; LEFP, 2015, n° 10, p. 2, note T. Douville ; Gaz. Pal., 2015, n° 288, p. 24, note C. Berlaud ; JCP G, 2015, n° 51, comm. 1385, P. Ducoulombier ; CCE, 2015, n° 11, comm. 92, obs. A. Lepage ; D., 2016, n° 05, p. 277, obs. E. Dreyer ; RTD civ., 2016, n° 02, p. 449, obs. N. Cayrol.

¹⁰⁰² Article 9.2 h) du RGPD.

¹⁰⁰³ Article 9.3 du RGPD.

ainsi préservés. En second lieu, l'usage des données médicales aux fins de la prise en charge sanitaire du patient doit impérativement être effectué conformément au droit à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel. Il en résulte que la limitation de l'autodétermination informationnelle du patient ne méconnaît pas le contenu du droit fondamental à la protection des données personnelles. Autrement dit, la restriction de l'exercice des droits de la personne concernée ne porte pas atteinte à la vie privée du patient.

Au demeurant, toute limitation aux droits et obligations octroyés à la personne concernée par le RGPD ne peut intervenir que par la voie de mesures législatives prises par le droit de l'Union ou le droit d'un Etat membre¹⁰⁰⁴. Cette limitation des droits de la personne concernée doit respecter l'essence de ses libertés et de ses droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique pour, notamment, garantir sa protection¹⁰⁰⁵. Par une décision du 12 août 2004, le Conseil constitutionnel a admis qu'il appartenait « *au législateur de concilier, d'une part, le droit au respect de la vie privée et, d'autre part, les exigences de valeur constitutionnelle qui s'attachent tant à la protection de la santé, qui implique la coordination des soins et la prévention des prescriptions inutiles ou dangereuses* »¹⁰⁰⁶. Dans l'espoir de dénouer le conflit entre les droits fondamentaux à la santé et à la protection des données personnelles, il appartient donc au législateur de justifier que la concrétisation du droit fondamental à la santé implique, pour le patient, de renoncer à certains des droits – non absolus – qui lui sont concédés par le RGPD. Au surplus, le patient aurait même la responsabilité d'y renoncer en faveur du devoir de collaboration à sa prise en charge sanitaire.

¹⁰⁰⁴ Article 23 du RGPD.

¹⁰⁰⁵ *Ibid.*

¹⁰⁰⁶ Cons. Const., 12 août 2004, n° 2004-504 DC, *Loi relative à l'assurance maladie*, cons. 5 : JCP A, 2004, n° 37, act. 1565.

2. *L'instauration de devoirs en contrepartie des droits fondamentaux*

335. Le droit fondamental à la protection de la santé, dont l'objectivation emporte un traitement de données médicales, est catégorisé parmi les droits-créances¹⁰⁰⁷. Cela signifie que ce droit fondamental ne peut se réaliser qu'« *indirectement à travers l'accomplissement par le débiteur d'une prestation* »¹⁰⁰⁸. En effet, l'effectivité du droit à la protection de la santé requiert l'intervention de l'Etat, des professionnels de santé et du principal intéressé : le patient. Lise Casaux-Labrunée remarque que « *les droits- créances supposent [...] dans bien des cas, la participation active des bénéficiaires à la mise en œuvre de leurs droits* »¹⁰⁰⁹. Autrement dit, « *le « droit à la santé » est aussi un droit-créance sur soi-même* »¹⁰¹⁰. Il est certain que ce droit fondamental « *ne peut entièrement reposer sur autrui dès lors qu'il a pour objet l'individu lui-même* »¹⁰¹¹. L'effectivité du droit à la protection de la santé dépend donc, en partie, de l'individu. Notamment, « *toute personne qui intervient dans le système de santé est tenue de respecter ce droit, y compris l'usager, qui doit adopter un comportement vertueux dans la gestion de son « capital santé » afin d'assurer la pérennité du système de santé* »¹⁰¹². Partant, le patient doit activement participer à la satisfaction du droit à la santé qu'il désire exercer. La mise en œuvre du droit à la santé par le patient implique alors le devoir de participer à son efficience. Dès lors, pèse sur le patient le devoir de mettre ses données médicales à la disposition des professionnels concourant à sa prise en charge sanitaire.

La personne soignée, en ses qualités de patient et de personne concernée, est titulaire de droits fondamentaux doublement renforcés. En effet, elle dispose d'une autodétermination sur son corps et d'une relative autodétermination informationnelle sur ses données médicales. Le patient est alors libre d'effectuer des choix relatifs à sa santé et à l'usage des éléments immatériels de son corps humain. En conséquence, le patient serait à la fois acteur de sa santé et acteur du traitement de ses données médicales. Par définition, est un acteur la « *personne*

¹⁰⁰⁷ Voir : GAY (L.), *La notion de « droits-créances » à l'épreuve du contrôle de constitutionnalité*, loc. cit.

¹⁰⁰⁸ CASAUX-LABRUNEE (L.), *op. cit.*, p. 926.

¹⁰⁰⁹ *Ibid.*

¹⁰¹⁰ CASAUX-LABRUNEE (L.), *op. cit.*, p. 928.

¹⁰¹¹ *Ibid.*

¹⁰¹² MEMETEAU (G.), GIRER (M.), *Cours de droit médical*, 5^e ed., LEH, 2016, p. 685.

qui joue un rôle effectif dans une affaire ou dans un événement »¹⁰¹³. Au moyen de l'exercice de ses droits, le patient peut donc jouer un rôle dans sa prise en charge sanitaire. Assurément, le patient qui jouit de la maîtrise de sa santé et du contrôle de ses données a le pouvoir de contribuer à sa prise en charge sanitaire ou, à l'inverse, d'y faire obstacle. Dès lors, l'effectivité du droit à la santé dépend des actions de son titulaire. La limitation de l'autodétermination informationnelle du patient apparaît alors justifiée par l'objectivation de son droit-créance à la santé et par son devoir de contribution aux soins. Certainement, l'exercice des droits du patient sur les éléments immatériels de son corps humain ne doit pas empêcher les actes sanitaires qui lui sont prodigués. Compte tenu de ce qui précède, l'instauration d'un devoir de collaboration à la prise en charge médicale résulte de la nature du droit fondamental à la santé.

336. Par ailleurs, le devoir de collaboration à la prise en charge médicale peut être simplement observé comme le corollaire du renforcement des droits du patient et de la personne concernée. Certainement, *« si l'activité juridique fait ainsi apparaître des prérogatives au bénéfice des individus, elle suscite aussi, nécessairement, des charges »*¹⁰¹⁴. En d'autres termes, si les droits ont laissé place aux devoirs, c'est parce que ces devoirs sont la contrepartie de ces droits. En effet, toute personne jouissant d'une capacité d'action, permise par l'exercice de ses droits, doit s'accommoder de contreparties. C'est ainsi que les sociétés contemporaines ont défini *« des devoirs en contrepoint des droits et libertés qu'elles peuvent consentir à garantir »*¹⁰¹⁵. D'abord, le Préambule de la Charte des droits fondamentaux de l'Union européenne annonce que *« la jouissance de ces droits [fondamentaux] entraîne des responsabilités et des devoirs »*¹⁰¹⁶. En conséquence, les droits à la santé et à la protection des données sont, *de facto*, assortis de contreparties. Plus exactement, le législateur français a affirmé que *« les droits reconnus aux usagers [du système de santé] s'accompagnent des responsabilités de nature à garantir la pérennité du*

¹⁰¹³ Définition des Dictionnaires français Larousse. Disponible en ligne sur le site [www.larousse.fr]. Consulté le 03 décembre 2020.

¹⁰¹⁴ AUBERT (J.-L.), SAVAUX (É.), *Introduction au droit et thèmes fondamentaux du droit civil*, 18^e ed., Sirey, août 2020, p. 254.

¹⁰¹⁵ HENNETTE-VAUCHEZ (S.), ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, 4^e ed., Dalloz, p. 26.

¹⁰¹⁶ Préambule de la Charte des droits fondamentaux de l'Union Européenne.

*« système de santé et des principes sur lesquels il repose »*¹⁰¹⁷. Lors d'une session sénatoriale relative au projet de loi relatif aux droits des malades, Etienne Caniard avait allégué que la consécration de droits pour le patient « *nécessite automatiquement une prise de responsabilité et donc des devoirs* »¹⁰¹⁸. La notion de responsabilité envisagée à l'article L.1111-1 du code de la santé publique se concrétiserait donc par l'institution de devoirs à la charge du patient.

337. Dans un sens commun, le devoir moral consiste en une « *obligation dont l'exécution ne peut être poursuivie en justice, ne chargeant l'obligé que d'un devoir de conscience* »¹⁰¹⁹. Alors que le devoir juridique est « *une norme comportementale générale, d'ordre moral et social, qui s'impose à tous [...]. Le respect d'un devoir juridique peut être obtenu par le bénéficiaire à l'aide d'une action en justice* »¹⁰²⁰. La seule différence entre un devoir moral et un devoir juridique réside dans la capacité, pour autrui, de s'en prévaloir devant le juge. Cette différenciation renvoie à la distinction entre l'obligation morale et l'obligation juridique. En effet, l'obligation morale correspond à un pur devoir de conscience auquel la personne n'est pas tenue et auquel personne ne peut l'obliger. A l'inverse, l'obligation juridique est « *celle dont l'exécution est systématiquement sanctionnée par le droit, au besoin par la contrainte étatique, et dont le créancier peut donc toujours obtenir l'exécution forcée, en justice* »¹⁰²¹. Le devoir moral correspond donc à l'obligation morale et le devoir juridique à l'obligation juridique. Alors, le devoir de collaboration à la prise en charge médicale constitue-t-il un devoir moral ou une obligation juridique pour le patient ?

338. Najib Hage-Chahine établit la distinction entre le devoir et l'obligation sur l'existence d'un lien de droit entre deux sujets déterminés : le créancier et le débiteur¹⁰²². Sans qu'il soit nécessaire de détailler les débats doctrinaux relatifs à la nature de la relation médicale, il est

¹⁰¹⁷ Article L.1111-1 du code de la santé publique

¹⁰¹⁸ GIRAUD (F.), DERIOT (G.), LORRAIN (J-L.), *Rapport n°174 fait au nom de la commission des affaires sociales sur le projet de loi relatif aux droits des malades et à la qualité du système de santé*, Sénat, 16 janvier 2002, p. 678.

¹⁰¹⁹ *Ibid.*

¹⁰²⁰ GUINCHARD (S.), DEBARD (T.), *op. cit.*, p. 368.

¹⁰²¹ BUFFELAN-LANORE (Y.), LARRIBAU-TERNEYRE (V.), *Droit civil. Les obligations*, Sirey, 17^e ed., octobre 2020, p. 56.

¹⁰²² Voir : HAGE-CHAHINE (N.), *La distinction de l'obligation et du devoir en droit privé*, Yves LEQUETTE (dir.), Thèse de doctorat, Droit, Université Paris II, avril 2014.

possible d'affirmer que le lien de droit entre le patient et le professionnel de santé repose sur le contrat de soins. En ce sens, David Jacotot certifie que « *la formule de l'illustre arrêt Mercier, rendu le 20 mai 1936, selon laquelle « il se forme entre le médecin et son client un véritable (nous soulignons) contrat » reste solidement ancrée dans notre Droit* »¹⁰²³. En effet, la relation médicale repose sur un accord de volontés (soigner et être soigné) destiné à créer des obligations¹⁰²⁴. En conséquence, le professionnel de santé a l'obligation principale de prodiguer des soins attentifs, consciencieux et fondés tant sur les données acquises de la science que sur l'analyse des données médicales du patient. Dans l'exécution de cette obligation, les parties doivent faire preuve de bonne foi. Prescrite à l'article 1104 du code civil, « *l'exigence de bonne foi est inscrite parmi les principes généraux gouvernant la formation et l'exécution du contrat* »¹⁰²⁵. Le principe de bonne foi comprend une obligation de loyauté, une obligation de collaboration et une obligation de coopération des cocontractants. Ainsi, l'obligation de loyauté implique « *de la part du créancier, l'absence de manœuvres qui rendraient plus difficile l'exécution de la prestation de l'autre partie* »¹⁰²⁶. Par suite, le patient ne doit pas volontairement dissimuler les informations médicales utiles à l'exécution de ce contrat. De surcroît, l'obligation de coopération implique l'obligation, pour chaque partie, de donner à son cocontractant les informations qu'il a à connaître au sujet de l'exécution du contrat¹⁰²⁷. Le patient doit donc livrer ses informations médicales aux professionnels participant à sa prise en charge sanitaire. En vertu du principe de bonne foi, le devoir de collaboration du patient à la prise en charge médicale constituerait une obligation de collaboration à l'exécution du contrat de soins et à la concrétisation de son droit fondamental à la santé. En conséquence, ce devoir saurait être qualifié d'obligation juridique de moyens.

339. En tant que contrepartie au renforcement de ses droits, le patient aurait le devoir – juridique – de collaborer à la concrétisation de son droit à la santé, lequel emporte une limitation de son autodétermination informationnelle. Prescrire des devoirs juridiques pour

¹⁰²³ JACOTOT (D.), *D'une relation bipartite à une relation multipartite. Essai sur le contrat médical*, In, LEONHARD (J.), PY (B.), VIALLA (F.), *Mélanges en l'honneur de Gérard Mémeteau. Droit médical et éthique médicale : regards contemporains*, LEH Édition, 2015, p. 506.

¹⁰²⁴ Article 1101 du code civil.

¹⁰²⁵ BUFFELAN-LANORE (Y.), LARRIBAU-TERNEYRE (V.), *op. cit.*, p. 296.

¹⁰²⁶ TRANCHANT (L.), ÉGEA (V.), *Droit des obligations*, Dalloz, 25^e ed., septembre 2020, p. 75.

¹⁰²⁷ *Ibid.*

le patient ne revient pas à affaiblir ses prérogatives mais, au contraire, à le considérer comme un acteur à responsabiliser. Certainement, l'absence de bonne foi d'une partie à un contrat devrait l'empêcher de se prévaloir de certains de ses droits tels que le droit à la réparation intégrale du préjudice auquel elle a participé¹⁰²⁸.

En conclusion, la restriction de l'autodétermination informationnelle du patient est consécutive à la mise en œuvre de ses droits fondamentaux. C'est parce que le patient peut effectivement maîtriser et contrôler l'usage de ses données médicales qu'il a le devoir de ne pas entraver sa prise en charge médicale. C'est parce que les droits conférés par le RGPD existent concrètement que leur exercice, dans le cadre d'une prise en charge sanitaire, nécessite une limitation. Dès lors, il n'y aurait pas de véritable atteinte aux droits de la personne concernée sur ses données médicales à caractère personnel.

¹⁰²⁸ Cf. Paragraphe 308.

Conclusion du chapitre

340. Pour honorer la prise en charge sanitaire d'un patient, le soignant doit indispensablement traiter et analyser ses données médicales. Si le professionnel de santé produit des données médicales à l'occasion de l'examen clinique du malade, ce dernier doit également appuyer son raisonnement sur des informations médicales préexistantes. Le contexte médical, l'histoire de la maladie et l'historique de la santé du patient sont des données essentielles à la décision médicale. En effet, la donnée médicale constitue le fondement de toute décision concernant la santé du patient. Il apparaît donc essentiel que le professionnel de santé puisse accéder à un nombre suffisant de données médicales relatives au patient. Ces éléments immatériels lui sont fournis par le patient à l'occasion de l'anamnèse, ainsi que par ses homologues à l'occasion de consultations antérieures.

341. Par ailleurs, le patient détient des droits sur ses données médicales personnelles et leur exercice peut être préjudiciable pour l'efficacité de sa prise en charge sanitaire. En effet, le patient peut bloquer la communication de ses données médicales entre les intervenants à sa prise en charge sanitaire et sociale, dissimuler des informations le concernant ou interdire l'accès à son DMP. En somme, par la simple maîtrise de ses données médicales, le patient peut nuire à sa prise en charge sanitaire et porter atteinte à son droit fondamental à la santé. Toutefois, en tant que débiteur d'un droit de créance sur lui-même¹⁰²⁹, le patient a le devoir de participer à la mise en œuvre de son droit à la santé et, conséquemment, de collaborer à sa prise en charge sanitaire. Ainsi, le patient devrait s'abstenir d'exercer les droits qu'il détient sur ses données médicales au profit de son parcours de santé. En l'espèce, la mise en œuvre d'un traitement de données médicales résulte de l'activation du droit à la santé. Dès lors, en tant que personne concernée, le patient devrait exercer les droits qui lui sont concédés de façon favorable pour sa santé. Assurément, les volontés du professionnel de santé et du patient convergent vers deux objectifs commun : le rétablissement et la guérison.

¹⁰²⁹ Cf. Paragraphe 335.

Conclusion du titre

342. L'intérêt de la formalisation et de la conservation des données médicales du patient dans un dossier *ad hoc* réside dans l'accessibilité de l'information médicale. D'une part, l'accessibilité des données médicales du patient constitue un véritable enjeu pour l'efficacité de sa prise en charge sanitaire. Face à une offre médicale fragmentée, pluridisciplinaire et décloisonnée, la circulation des données médicales du patient entre les intervenants à sa prise en charge sanitaire garantit la coordination et la continuité de son parcours de soins. A cette fin, les professionnels peuvent échanger des documents médicaux, partager des dossiers médicaux et se connecter au dossier médical partagé du patient. D'autre part, l'accessibilité des données médicales constitue un vecteur d'information pour le patient. Le droit d'accès du patient aux données formalisées dans ses dossiers médicaux accroît la transparence dans la relation médicale, achève le paternalisme médical et entérine son autonomisation.

Si la formalisation des données médicales du patient constitue le prérequis à leur communication, l'accès aux informations médicales est toujours soumis au contrôle du patient. Certainement, le patient demeure le maître du secret médical. En conséquence, l'ouverture, la réutilisation et l'exploitation des données médicales du patient semble dépendre de la volonté de la personne concernée. Pourtant, l'exploitation des données cliniques des patients constitue un enjeu pour la recherche et l'innovation en santé.

Conclusion de la première partie

343. La personne qui bénéficie d'une prise en charge sanitaire cumule deux statuts distincts, emportant l'application de régimes juridiques particuliers : le *patient* et la *personne concernée*. Cependant l'articulation des droits conférés à la personne concernée avec les obligations inhérentes à toute prise en charge sanitaire pose de réelles difficultés. En effet, l'exercice des droits renforcés par le RGPD peut empêcher l'accomplissement de la prise en charge sanitaire du patient. Pourtant, la mise en œuvre de ce traitement est subséquente et indispensable à la réalisation de cette finalité. De surcroît, le traitement des données médicales est effectué dans l'intérêt du patient : il en est l'ultime bénéficiaire. Il n'en demeure pas moins que l'exercice de l'entièreté des droits qu'il détient sur ses données médicales mettrait en péril sa santé. Dès lors, eu égard à la primauté de la sauvegarde de la vie humaine¹⁰³⁰, il apparaît justifié que, par devoir, le patient s'abstienne d'exercer la plénitude des droits qui lui sont octroyés par le RGPD. Compte tenu de ce qu'il précède, il convient indispensablement d'harmoniser le corpus normatif applicable à la protection des données personnelles traitées aux fins de la prise en charge sanitaire du patient.

344. S'il est admissible que les droits du patient sur ses données médicales soient restreints lorsque le traitement est effectué dans son propre intérêt, qu'en est-il lorsque ces données, générées à l'occasion de sa prise en charge sanitaire, sont réutilisées pour une finalité dont l'intérêt bénéficie à la collectivité ? Dans cette hypothèse, les droits de la personne concernée retrouvent-ils leur pleine effectivité

¹⁰³⁰ Cf. Paragraphe 333.

DEUXIEME PARTIE :

**LE TRAITEMENT DES DONNEES MEDICALES DU
PATIENT AU BENEFICE DE LA COLLECTIVITE**

345. Les données médicales constituent des informations recueillies ou produites à l'occasion de la prise en charge sanitaire du patient afin de cristalliser son état de santé¹⁰³¹. Elles fixent ainsi ses conditions psychiques, physiques et biologiques. Dans un premier temps, ces informations confidentielles représentent l'outil nécessaire à la dispensation des actes de prévention, de diagnostic ou de soins au bénéfice du patient. Dans un second temps, ces mêmes données médicales constituent la ressource essentielle aux recherches rétrospectives et à l'innovation dans le domaine de la santé, ainsi qu'à la mise en œuvre de la santé publique. A cet égard, elles font l'objet d'une utilisation secondaire par des exploitants provenant de divers horizons. Il peut notamment s'agir d'un professionnel de santé analysant la gestion d'une pathologie au sein d'un service médical, d'un industriel du secteur pharmaceutique, d'un auto-entrepreneur concevant un dispositif d'aide au diagnostic médical, d'un médecin junior préparant sa thèse d'exercice de la médecine, ou encore des services de l'Etat et des biostatisticiens en matière d'épidémiologie et de lutte contre les menaces sanitaires¹⁰³².

¹⁰³¹ Cf. Paragraphes 50 à 53.

¹⁰³² Voir : DOUVILLE (T.), *Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs...)*, JDSAM, 2018, n° 20, p. 12.

La détermination des droits et des devoirs du patient, lorsque ses données médicales sont ainsi réutilisées au bénéfice de la collectivité (**Titre 2**), présuppose de définir le statut juridique de cet élément immatériel et d'étudier les droits que les tiers exploitants détiennent conséquemment à son égard (**Titre 1**). Autrement dit, la définition du statut de la donnée médicale constitue un enjeu fondamental tant pour jalonner les contours de ses possibles exploitations au bénéfice de la collectivité, que pour identifier l'ampleur de l'autodétermination informationnelle du patient concerné. Vous l'aurez compris, dans cette deuxième partie, nous nous attacherons à examiner les seuls traitements nécessaires « *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* »¹⁰³³.

¹⁰³³ Article 9.2 i) du RGPD.

TITRE 1 :

LA DETERMINATION DU STATUT JURIDIQUE ET DU REGIME APPLICABLES A LA DONNEE MEDICALE

346. Dans le domaine de la santé, l'ensemble des réutilisateurs de la donnée médicale ont pour exigence commune de poursuivre un motif d'intérêt public¹⁰³⁴. La réutilisation de la donnée médicale à des fins étrangères à la prise en charge sanitaire du patient doit donc bénéficier à la collectivité. Au demeurant, l'intérêt public du traitement ne se révèle pas incompatible avec tout intérêt commercial¹⁰³⁵. En effet, la recherche dans le domaine de la santé peut, à titre d'exemple, engendrer une innovation incorporelle en faveur de l'amélioration de la qualité des soins, qui sera ensuite commercialisée aux établissements et aux professionnels de santé. Par ailleurs, le traitement des données médicales à des fins de santé publique favorise l'anticipation et la gestion des risques sanitaires de grande échelle, ce qui conduit notamment à la réduction des dépenses de l'Assurance maladie et à la persistance de l'économie nationale. La donnée médicale présente donc des utilités économiques qui lui confèrent de la valeur et en font un objet de convoitise¹⁰³⁶. Les producteurs des données médicales, leurs réutilisateurs et les patients concernés pourraient alors être tentés d'en faire un commerce afin d'en tirer des bénéfices.

Cependant, la donnée médicale ne constitue pas une matière première ordinaire. Assurément, cette information, profondément intime, émane directement de la personne humaine¹⁰³⁷. C'est pourquoi elle lui est singulièrement affectée par le mécanisme des droits de la personnalité. Afin de conjurer toute marchandisation du corps humain du patient¹⁰³⁸, il conviendrait d'affirmer l'extrapatrimonialité de la donnée médicale en lui édifiant un statut juridique spécifique (**Chapitre 1**). De cette façon, elle ne pourrait jamais être appréciée

¹⁰³⁴ Article 66.I de la loi Informatique et Libertés modifiée.

¹⁰³⁵ Health Data Hub, *Qu'est-ce que l'intérêt public ?* Disponible en ligne sur le site [www.health-data-hub.fr]. Consulté le 13 septembre 2021.

¹⁰³⁶ Cf. Paragraphe 381.

¹⁰³⁷ Cf. Paragraphes 50 à 53.

¹⁰³⁸ Cf. Paragraphes 362 et 371.

pécuniairement, ni réservée dans aucun patrimoine. La relative autodétermination informationnelle du patient et sa dignité humaine seraient alors définitivement préservées.

347. En revanche, l'extrapatrimonialité de la donnée médicale ne proscrit pas la valorisation économique des résultats de son traitement (**Chapitre 2**). Certainement, les conclusions des recherches rétrospectives dans le domaine de la santé peuvent constituer des biens incorporels, certes créés à partir de la donnée médicale du patient, mais manifestement distincts de celle-ci. La donnée médicale extrapatrimoniale serait une source de richesse à travers son exploitation, tandis que le patient se verrait épargné de toute instrumentalisation des attributs immatériels de son corps humain.

Chapitre 1 : L'extrapatrimonialité de la donnée médicale

« La « *summa divisio* » des personnes et des choses a pris les traits, dans le code civil, d'une distinction entre les personnes et les biens, comme si le destin de toutes choses était d'être offertes à la propriété. »¹⁰³⁹.

348. Bien que la loi Informatique et Libertés modifiée consacre une section dédiée aux « *traitements de données caractère personnel dans le domaine de la santé* »¹⁰⁴⁰, ces dispositions ne visent qu'à encadrer les conditions dans lesquelles ces informations confidentielles peuvent être utilisées lorsque leur traitement poursuit un motif d'intérêt public dans le domaine de la santé¹⁰⁴¹. La loi nationale ne confère aucun statut juridique qui serait spécifique à la donnée médicale. Pourtant, la détermination de ce statut est fondamentale pour discerner son régime juridique et, ainsi, délimiter les prérogatives que la personne concernée, mais également les tiers, peuvent exercer sur celles-ci (**Section 1**). Cette circonscription apparaît particulièrement nécessaire au regard de la multiplication des usages de la donnée médicale, de la révélation de ses utilités économiques et de l'accroissement de sa valeur marchande¹⁰⁴². L'analyse purement économique du droit conduirait donc à qualifier cette émanation du corps humain de *bien*. Toutefois, face à la cupidité manifestée à l'égard de cet objet et à l'avidité de se l'approprier, il semble indispensable d'en consacrer l'extrapatrimonialité (**Section 2**). Certainement, la donnée médicale, en tant qu'élément immatériel du corps humain du patient, est intimement liée à la personne de laquelle elle émane. A ce titre, elle mériterait d'être juridiquement protégée grâce à sa sacralisation.

¹⁰³⁹ LOISEAU (G.), *Pour un droit des choses*, Recueil Dalloz, 2006, n°44, p. 3015.

¹⁰⁴⁰ Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

¹⁰⁴¹ Cf. Paragraphe 23.

¹⁰⁴² Voir : GHANTY (A.) et al., *Protection des données personnelles*, Francis Lefebvre, 2019.

Section 1 : Tentative de qualification de la donnée médicale

349. Tandis que le RGPD distingue différentes natures de données personnelles telles que celles concernant la santé, des sous-catégories de données de santé peuvent être, en pratique, identifiées. C'est ainsi que les données médicales, générées à l'occasion de la prise en charge sanitaire du patient, constituent une espèce particulière d'informations formalisant un état biologique, physique ou psychique. Si nous avons eu l'occasion de définir la notion de donnée médicale personnelle¹⁰⁴³, il convient désormais de s'interroger sur son statut. En effet, ni le statut de la donnée à caractère personnel, ni le statut de la donnée médicale ne font l'objet d'une consécration juridique (**Paragraphe 1**). Pourtant, la spécificité de la donnée médicale, convergeant entre les choses et les personnes, mérite que l'on s'interroge sur son statut, indépendamment de son usage, lorsqu'elle est détachée du patient qui en est la source. Même lorsqu'elle est anonymisée, la donnée médicale comporte des risques pour les droits et libertés du patient. Il conviendrait donc de lui allouer un régime protecteur à l'instar des éléments et des produits du corps humain détachés de leur hôte (**Paragraphe 2**).

Paragraphe 1 : Le statut de la donnée médicale à caractère personnel

350. Compte tenu du lien étroit entre la donnée médicale personnelle et le corps humain du patient, nous assistons à l'apparition empirique d'un élément immatériel du corps humain : la chose anthropomorphique à caractère personnel (**A**). Ce nouveau statut, obtenu par la pratique médicale, requiert d'être accompagné d'un régime juridique hybride respectueux des aspects physiques et moraux qu'elle abrite (**B**).

A) L'émergence d'une chose anthropomorphique personnelle

351. La donnée médicale personnelle a pour particularité de formaliser tant les attributs de la personnalité du patient que les attributs de son corps humain. En effet, « *les informations de santé sont au carrefour de ces deux types d'informations, participant tant du dévoilement physiologique de la personne que de la révélation d'éléments de son état civil ou de sa vie*

¹⁰⁴³ Cf. Paragraphe 15.

privée »¹⁰⁴⁴. Compte tenu de ses caractères indéniablement humains, la chose anthropomorphique personnelle consiste, à la fois, en une allégorie représentant l'individualité du patient (1), et en une réification de son corps humain (2).

1. La personnalisation de la donnée personnelle

352. Le droit français est structuré par la *summa divisio*. D'abord, le droit est divisé en branches et en sous-branches. Ensuite, chacune de ces sous-branches est organisée en catégories juridiques. C'est ainsi que le droit civil, sous-branche du droit privé, distingue la catégorie des choses de la catégorie des personnes. Tout élément existant, qu'il soit animé ou inanimé, corporel ou incorporel, naturel, matériel, animal ou humain relève nécessairement de l'une ou de l'autre de ces deux catégories. En vertu de ce raisonnement, la donnée médicale à caractère personnel ne pourrait être qualifiée que de chose ou de personne. En effet, « *cette summa divisio permet de ranger toutes les réalités matérielles et de leur appliquer tel ou tel régime juridique : soit l'on n'est personne et sujet de droit, soit chose et objet de droit* »¹⁰⁴⁵.

La classification d'un élément dans une catégorie est effectuée par défaut. En effet, seuls les êtres humains nés vivants et viables sont qualifiés de *personne* jusqu'à leur mort, leur absence ou leur disparition. Par déduction, tout élément qui ne répond pas à ces deux conditions cumulatives tombe dans la catégorie des choses. La *summa divisio* du droit civil repose donc sur une logique binaire. Seulement, la qualification d'un objet ou d'un sujet de droit peut dépasser la rigidité de ce mode de classification. A l'occasion d'une tentative de qualification de l'intelligence artificielle, Samir Merabet a déploré que « *certaines choses dotées de vie se voient refuser la personnalité juridique tandis que d'autres qui en sont pourtant dépourvues sont qualifiées de sujets de droit* »¹⁰⁴⁶. Cette incohérence révèle les limites de la *summa divisio* : le droit civil ne nous offre que deux alternatives déterminées par défaut. Par conséquent, la donnée médicale à caractère personnel doit-elle fatalement être

¹⁰⁴⁴ MALLET-POUJOL (N.), *Droit à et droit sur l'information de santé*, In *Le droit des données de santé*, op. cit., p. 80.

¹⁰⁴⁵ PAUVERT (B.), *Le droit des éléments et produits du corps – ou les enjeux d'une réification silencieuse –* In NICOLAS (G.), *Les éléments et produits du corps humain*, CDSA, février 2011, n°12, p. 12.

¹⁰⁴⁶ MERABET (S.), *Vers un droit de l'intelligence artificielle*, Thèse de doctorat, Droit, Université Aix-Marseille, Dalloz, 2020, p. 127.

qualifiée de chose ? La classification, selon la *summa divisio*, se cantonne à faire correspondre un élément réellement existant à une catégorie juridique fictive et, parfois, inadaptée. Pourtant, l'opération de qualification juridique constitue le préalable indispensable à la détermination du régime de droit applicable à l'élément existant, en l'occurrence, la donnée médicale personnelle. Compte tenu des enjeux inhérents à cette qualification, la « *dialectique héritée du droit romain et qui oppose les objets de droit au sujet de droit est-elle encore satisfaisante pour rendre compte des réalités contemporaines* »¹⁰⁴⁷ ? Face aux difficultés de qualification des données à caractère personnel, Cécile Deschanel s'interroge : « *devons-nous les protéger au même titre que le sont les personnes parce que nous considérons qu'elles sont si liées à elles qu'elles se confondent ? Faut-il admettre que l'atteinte portée à une donnée personnelle constitue, en réalité, une atteinte à la personne elle-même dans ce qui fait sa singularité* »¹⁰⁴⁸ ? S'il est certain que la donnée médicale personnelle ne peut être qualifiée de personne, celle-ci est étroitement liée au sujet de droit dont elle est issue : le patient. Compte tenu de cette réalité, est-il loisible de catégoriser, par défaut, la donnée médicale personnelle parmi les choses ? En solution, Samir Merabet a observé que « *des propositions doctrinales ont été formulées en vue de permettre à des objets juridiques de profiter de certains attributs des sujets de droit sans que l'octroi de la personnalité juridique ne soit nécessaire* »¹⁰⁴⁹. Il convient alors d'étudier les éventuels statuts juridiques applicables à la donnée médicale personnelle au-delà du carcan de la *summa divisio* du droit civil.

353. La donnée à caractère personnel, qu'elle soit neutre ou sensible, est directement ou indirectement rattachée à une personne physique. En d'autres termes, la donnée est personnelle dans la mesure où elle contient nécessairement des éléments d'identification directe ou indirecte de la personne concernée. En effet, le caractère personnel de la donnée permet de relier l'information à la personne qu'elle concerne et aux attributs de sa personnalité. En conséquence, « *la donnée [personnelle] est indéfectiblement liée à son objet car, sans lui, elle n'existerait pas ; elle en constitue en quelque sorte les accessoires.* »¹⁰⁵⁰.

¹⁰⁴⁷ Civ. 1^{ère}, 8 octobre 1980, note Alain Couret, D. 1981, p. 361.

¹⁰⁴⁸ DESCHANEL (C.), *L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité ?*, RLDI, 2019, n°156, p. 38.

¹⁰⁴⁹ MERABET (S.), *op. cit.*, p. 146.

¹⁰⁵⁰ BOURGEOIS (M.), THIBIERGE (L.), *Droit de la donnée : plaidoyer pour un régime général*, La semaine juridique Entreprise et Affaires, 2020, n°20, p. 42.

C'est ainsi que Matthieu Bourgeois et Louis Thibierge considèrent que la théorie de l'accessoire est applicable à la donnée personnelle, « *faisant ainsi suivre à la donnée le même régime que celui applicable à son objet* »¹⁰⁵¹. La donnée à caractère personnel pourrait alors être assimilée aux attributs de la personnalité, à l'instar des informations affectées à la personne concernée dont elle formalise l'objet. Si pour ces deux auteurs, les données personnelles sont une « excroissance » de la personne physique, Danièle Bourcier et Primavera De Filippi les observent comme une « extension » de la personnalité des individus¹⁰⁵².

A l'occasion d'un colloque portant sur les biens numériques, il a été affirmé que « *les données personnelles sont des éléments de personnalité de chacun ; elles émanent des individus, révèlent leur identité et participent de leurs comportements* »¹⁰⁵³. Les données personnelles peuvent dévoiler des attributs corporels et objectifs, tels qu'une identité ou un état de santé, ainsi que des attributs incorporels et subjectifs, comme un caractère, une préférence ou une opinion propre à un être humain. En tout état de cause, les données personnelles marquent l'individualité de la personne « *qui la rend irréductible à toute autre* »¹⁰⁵⁴. Les données personnelles constituent donc des excroissances de l'être et de l'âme de la personne humaine dont l'assemblage compose la personnalité. La personnalité de la personne physique ne doit donc pas se confondre avec la personnalité juridique. En effet, « *la personnalité dont il est ici question est une donnée de fait, à la différence de la personnalité juridique qui est une construction du droit* »¹⁰⁵⁵. En 1999, la Commission européenne considérait déjà que « *les données personnelles de santé sont partie intégrante de la personnalité de l'individu qu'elles concernent* »¹⁰⁵⁶. En vertu de cette approche humaniste

¹⁰⁵¹ *Ibid.*

¹⁰⁵² BOURCIER (D.), DE FILIPPI (P.), *Vers un droit collectif sur les données de santé*, RDSS, 2018, n°03, p. 444.

¹⁰⁵³ ROCHFELD (J.), *Contre l'hypothèse de la qualification des données personnelles comme des biens*, In NETTER (E.), CHAIGNEAU (A.), *Les biens numériques*, PUF, 2015, p. 231.

¹⁰⁵⁴ LEPAGE (A.), *Droits de la personnalité*, Répertoire de droit civil, Dalloz, septembre 2009, actu. janvier 2021, § 17.

¹⁰⁵⁵ *Ibid.*

¹⁰⁵⁶ Commission européenne, *Avis n° 13 du 30 juillet 1999 : Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*, Journal International de Bioéthique, vol. 12, 2001, n° 3, p. 114.

approuvée par la doctrine juridique, et affirmée par Pierre Catala¹⁰⁵⁷, il en ressort que la donnée personnelle incarne l'être humain dont elle émane. D'une certaine manière, elle en est la personnification¹⁰⁵⁸.

En ce sens, Cécile Deschanel affirme que, « *ce prolongement de la personne dans ses accessoires, que ce soit les données personnelles, les éléments et produits du corps humain ou encore les attributs de la personnalité, ne se justifie que par le désir de voir s'appliquer l'adage *accessorium sequitur principale*.* »¹⁰⁵⁹. Tandis que les données à caractère personnel sont globalement assimilées à des attributs de la personnalité, le statut spécifique aux informations relatives à la santé de l'individu mérite d'être précisé. En application de la théorie de l'accessoire, le régime applicable à la donnée médicale personnelle doit être déterminé en fonction du statut applicable à son objet principal : le corps humain du patient.

2. *La réification de la condition physiologique du patient*

354. Sous un versant biologique, une donnée correspond à « *la traduction, dans une forme compréhensible par un être vivant, d'une réalité* »¹⁰⁶⁰. Matthieu Bourgeois et Louis Thibierge spécifient que « *cette proposition ajoute à la donnée brute (le réel) sa représentation sous une forme (ici biologique) qui permet à l'organisme vivant de la recevoir et de lui donner une signification. Ce sont là les deux caractéristiques essentielles [...] de la donnée : l'état du réel et sa perceptibilité par un agent. Autrement dit : une représentation du réel qui peut circuler* »¹⁰⁶¹. Partant de cette dimension biologique, les informations relatives à la santé d'une personne, converties en données médicales, traduisent une condition clinique et biologique provenant directement du corps humain du patient. Ces données cliniques constituent la retranscription de la physiologie propre à un individu. En d'autres termes, elles tendent à formaliser, en une information concrète, une condition physique intrinsèque et naturelle de la personne humaine. Si la donnée personnelle est un prolongement

¹⁰⁵⁷ Dans son ouvrage *Le droit à l'épreuve du numérique, Jus ex Machina*, Paris, PUF, 1998, Pierre Catala écrivait « *quand l'objet des données est un sujet de droit, l'information est un attribut de la personnalité* ».

¹⁰⁵⁸ La personnification consiste à attribuer des caractéristiques humaines à un objet inanimé ou à une réalité abstraite.

¹⁰⁵⁹ DESCHANEL (C.), *op. cit.*, § 7.

¹⁰⁶⁰ BOURGEOIS (M.), THIBIERGE (L.), *op. cit.*, p. 43.

¹⁰⁶¹ BOURGEOIS (M.), THIBIERGE (L.), *op. cit.*, p. 41.

de la personnalité, la donnée médicale correspond davantage à un prolongement corporel de la personne concernée¹⁰⁶². Elle constitue donc un élément immatériel du corps humain dans la mesure où elle formalise les attributs du corps humain de la personne concernée.

Pour dire les choses autrement, la donnée médicale personnelle réifie le corps humain du patient en ce qu'elle fixe une réalité qui n'existe, avant qu'elle ne soit formalisée, qu'à l'intérieur de son hôte. Cette fixation de la condition physiologique du patient dans une donnée médicale conduit à édifier un objet immatériel relatif au corps et à l'âme¹⁰⁶³ du patient. Seulement, cet objet ne peut être ni franchement qualifié de chose, ni véritablement qualifié de personne. Certainement, la donnée médicale se situe à la confluence des choses, de la personnalité et des attributs de l'être humain. Pourtant, « *la summa divisio entre les choses et les personnes, directement issue du principe de dignité, est garantie à la fois par la protection juridique de la vie et par celle du corps humain* »¹⁰⁶⁴. Si la donnée médicale correspond à un élément immatériel du corps humain du patient, son respect devrait alors être assuré au moyen du principe de dignité.

355. La donnée médicale, ayant pour objet le corps humain inviolable et sacré du patient, mérite alors une qualification accompagnée d'un régime qui lui seraient particuliers. Tout comme Antoine Leca suggérerait d'instaurer un nouveau statut juridique propre au corps humain et à ses éléments dans le but d'affermir leur humanité et d'édifier un régime protecteur¹⁰⁶⁵, il apparaît nécessaire de créer un statut singulier à la donnée médicale en raison de sa nature spéciale : celui d'une chose anthropomorphique. Dans le silence de la loi, cet objet de réification du corps humain nécessite manifestement une protection spécifique, notamment contre toutes appropriation et marchandisation.

¹⁰⁶² Voir : MALLET-POUJOL (N.), *Droit à et droit sur l'information de santé*, RGDM, 2004, n°04, p. 81 à p. 85.

¹⁰⁶³ Dans l'hypothèse où l'information médicale porte sur la psychologie du patient.

¹⁰⁶⁴ SAINT PAU (J.-C.), *op. cit.*, p. 139.

¹⁰⁶⁵ Voir : LECA (A.), *Corpus id est persona ? Réflexions à propos de la situation juridique du corps humain*, In THOLOZAN (Olivier), *De jure corporis ou la réification du corps humain*, CDSA, 2004, n°02, p. 37 à p. 79.

B) La création d'un régime hybride d'ordre public

« *S'il est interdit de commercialiser certaines parties du corps humain, est-il acceptable de commercialiser les données qui représentent des informations émanant du corps humain ?* »¹⁰⁶⁶.

356. En tant que chose anthropomorphique, l'objet de la donnée médicale personnelle porte tant sur les attributs de la personnalité du patient que sur les attributs de son corps humain. Ces attributs étant protégés par les droits de la personnalité, la donnée médicale personnelle profite conséquemment de leur protection. Les droits de la personnalité sont définis comme un ensemble de « *droits inhérents à la personne humaine qui appartiennent de droit à toute personne physique (innés et inaliénables) pour la protection de ses intérêts primordiaux* »¹⁰⁶⁷. Ces droits sont des attributs inséparables de la personnalité de tout individu, et dotés d'une opposabilité absolue¹⁰⁶⁸. Plus précisément, Agathe Lepage explique que la personnalité et les caractères singuliers des personnes, en tant qu'êtres humains constitués de chair et de sang, s'expriment à travers différents attributs corporels et incorporels qui sont protégés par les droits de la personnalité¹⁰⁶⁹. Autrement dit, il existe deux familles de droits de la personnalité : ceux protégeant le respect de l'intégrité morale et ceux protégeant le respect de l'intégrité physique.

En premier lieu, la donnée médicale personnelle, relative à l'état de santé du patient, entre dans la sphère de l'intimité de sa vie privée. A ce titre, elle est protégée par le droit au respect de la vie privée notamment consacré à l'article 9 du code civil. En second lieu, la donnée médicale personnelle est protégée par le droit à la protection des données à caractère personnel, lequel relève des droits de la personnalité. En effet, « *la loi relative à l'informatique, aux fichiers et aux libertés, ainsi que le Règlement général à la protection des données protègent à travers la donnée, la personne concernée par le traitement, son individualité, son intégrité morale, c'est-à-dire sa vie privée* »¹⁰⁷⁰. C'est ainsi que la

¹⁰⁶⁶ BOURCIER (D.), DE FILIPPI (P.), *op. cit.*, p. 448.

¹⁰⁶⁷ CORNU (G.), *Vocabulaire juridique*, 13^e ed, PUF, 2020.

¹⁰⁶⁸ GUINCHARD (S.), DEBARD (T.), *op. cit.*, p. 411.

¹⁰⁶⁹ LEPAGE (A.), *Droits de la personnalité*, RDT civ., septembre 2009, actu. janvier 2021, § 17.

¹⁰⁷⁰ BRASSELET (R.), *La circulation de la donnée à caractère personnel relative à la santé*, Bruno PY (dir.), Thèse de doctorat, Droit, Université de Lorraine, décembre 2018, p. 97.

protection des données personnelles est observée comme une composante du droit au respect de la vie privée¹⁰⁷¹. La protection de la donnée médicale personnelle par cette famille des droits de la personnalité ne couvre donc que la protection de l'intégrité morale du patient. Ce dernier est alors maître des informations médicales le concernant et bénéficie du droit de les réserver dans la stricte sphère de sa vie privée.

357. Néanmoins, cette chose anthropomorphique consiste également en un élément immatériel du corps humain du patient. Alors que « *la doctrine fait souvent reposer les droits de la personnalité sur une summa divisio entre [...] le respect de l'intégrité physique et le respect de l'intégrité morale* »¹⁰⁷², la chose anthropomorphique devrait également faire l'objet d'une protection par le droit au respect du corps humain. En effet, « *le point commun entre la dignité et les droits de la personnalité réside dans l'irréductible individualité de l'être humain* »¹⁰⁷³, dont la donnée médicale personnelle représente la parfaite illustration. Le droit au respect du corps, de ses éléments et de ses produits appartient aux droits de la personnalité et devrait s'appliquer à la chose anthropomorphique personnelle.

358. Si la donnée médicale s'entend comme toute information médicale recueillie ou produite par les professionnels intervenant dans le système de santé à l'occasion de la prise en charge sanitaire du patient, nul ne devrait pouvoir participer à une production de données médicales en dehors d'une nécessité médicale pour lui-même ou dans l'intérêt thérapeutique d'autrui¹⁰⁷⁴. Dès lors, toute donnée médicale ne devrait être produite que dans le cadre d'une relation médicale ou d'une recherche impliquant la personne humaine à laquelle le patient a consenti¹⁰⁷⁵. Ainsi, les données médicales doivent être collectées ou produites dans le respect de l'intégrité du corps humain du patient¹⁰⁷⁶ et conformément à l'expression de sa volonté¹⁰⁷⁷. Ainsi, aucun acte médical ou soignant ne pourrait être prodigué dans l'unique objectif de générer des éléments immatériels du corps humain du patient en dehors de ces deux finalités.

¹⁰⁷¹ Cf. Paragraphe 333.

¹⁰⁷² LEPAGE (A.), *Droits de la personnalité*, op. cit., § 24.

¹⁰⁷³ LEPAGE (A.), *Droits de la personnalité*, op. cit., § 19.

¹⁰⁷⁴ Article 16-3 du code civil.

¹⁰⁷⁵ Hormis lorsque le patient est hors d'état de donner son consentement ou lorsque celui-ci est décédé.

¹⁰⁷⁶ Article 16-3 du code civil.

¹⁰⁷⁷ Article L.1111-4 du code de la santé publique.

Assurément, aucune personne ne peut valablement consentir à une atteinte à son intégrité physique à l'exception des cas prévus par la loi¹⁰⁷⁸. « *Hors de ces cas particuliers, l'ordre public commande en effet que la vie et le corps de la personne soient protégés, indépendamment de sa volonté, des atteintes qui peuvent lui être portées par autrui.* »¹⁰⁷⁹. Il en résulte que la personne concernée ne devrait jamais pouvoir consentir à une production de données médicales indépendamment de sa prise en charge sanitaire ou de sa participation à une recherche médicale prospective. De cette façon, le corps humain ne pourrait jamais être considéré comme un simple outil de production de données médicales conduisant à l'asservissement des individus¹⁰⁸⁰. Toutefois, lorsque cette donnée est produite par le professionnel de santé et intégrée dans un dossier *ad hoc*, le patient en devient le titulaire. Cela signifie qu'il peut la divulguer, voire même en concéder l'usage à des tiers à la prise en charge médicale¹⁰⁸¹.

359. Il apparaît que la chose anthropomorphique personnelle mérite un respect identique à celui dû aux éléments et aux produits du corps humain. Certainement, la donnée médicale personnelle correspond à une réification du corps humain du patient. Christophe Willmann explique qu'un courant doctrinal rattache la dignité humaine à la représentation de l'homme recouvrant « *ce qui abaisse ou avilit l'être humain en tendant à la réification de son corps ou en portant atteinte aux droits essentiels de sa personne* »¹⁰⁸². En ce sens, Dominique Viriot-Barrial explicite que la lutte contre l'atteinte à la dignité résultant de la réification de la personne dans son corps se manifeste par une protection corporelle, par une protection extracorporelle mais encore par une protection éthique¹⁰⁸³. C'est ainsi que les données médicales personnelles, à travers les principes d'intégrité du corps humain et de dignité humaine, doivent être notamment protégées contre toute patrimonialité, contre toute

¹⁰⁷⁸ Voir : CEDH, 19 février 1997, n° 21627/93.

¹⁰⁷⁹ LEPAGE (A.), *Droits de la personnalité*, *op. cit.*, § 26.

¹⁰⁸⁰ Par la décision n° 94-343/344 DC du 27 juillet 1994, le Conseil Constitutionnel a considéré qu'il ressortait que la sauvegarde de la dignité de la personne humaine contre toute forme d'asservissement et de dégradation est un principe à valeur constitutionnelle.

¹⁰⁸¹ Cf. paragraphes 280 et 558.

¹⁰⁸² WILLMANN (C.), *Conditions de travail et d'hébergement contraires à la dignité humaine*, Répertoire de droit pénal et de procédure pénale, octobre 2003, actu. mars 2014, § 84.

¹⁰⁸³ VIRIOT-BARRIAL (D.), *Dignité de la personne humaine*, Répertoire de droit pénal et de procédure pénale, juin 2014, actu. septembre 2020, § 17.

exploitation économique, contre toute inégalité ou contre toute discrimination¹⁰⁸⁴. Assurément, « *la dignité, comme unité du corps et de la personne, implique de ne pas désocialiser, exclure, discriminer, maltraiter par le corps. [...] La dignité, comme unité corps-personne, convoque aussi la non-exclusion en raison du corps [...]. La dignité se confond alors avec l'égalité première, celle de tous les humains.* »¹⁰⁸⁵. Cette protection permettrait de préserver la dignité de la personne humaine en cas d'usage de la donnée médicale. A l'instar des restes des personnes décédées et des cendres de celles dont le corps a donné lieu à crémation, les données médicales personnelles devraient être traitées avec respect, dignité et décence¹⁰⁸⁶. Mais surtout, il conviendrait d'allouer à cette chose anthropomorphique une protection hybride calquée sur les régimes applicables aux aspects moraux et corporels des droits de la personnalité tels qu'institués aux articles 9, 16 et suivants du code civil.

360. Tandis que la donnée médicale personnelle est d'ores et déjà protégée, dans ses aspects moraux, par les droits de la personnalité, le régime applicable aux éléments et aux produits du corps humain lui serait également transposable. Il apparaît donc nécessaire d'abandonner la *summa divisio* entre l'incorporel et le corporel afin de combiner les régimes visant à protéger l'intégrité morale et l'intégrité physique des individus pour les appliquer à la chose anthropomorphique personnelle. En conséquence, il convient d'articuler le régime général des droits de la personnalité avec les particularités inhérentes au droit au respect des éléments et des produits du corps humain. Finalement, de cette jointure, il pourrait émerger un ultime droit de la personnalité, accompagné d'un régime juridique autonome, en dépit de la surcroissance des nouveaux droits de la personnalité¹⁰⁸⁷. Il convient alors de déterminer les contours du régime juridique qui serait applicable à la donnée médicale personnelle.

361. Alors que la donnée médicale personnelle est ici observée comme une chose anthropomorphique, celle-ci bénéficie du régime des droits de la personnalité, appartenant à la catégorie des droits extrapatrimoniaux. Le droit au respect de la vie privée, le droit à la

¹⁰⁸⁴ *Ibid.*

¹⁰⁸⁵ BIOY (X.), *Le corps humain et la dignité*, Cahiers de la recherche sur les droits fondamentaux, 2017, n°15, p. 14.

¹⁰⁸⁶ Voir : article 16-1-1 du code civil.

¹⁰⁸⁷ Voir : HASSLER (T.), *La crise d'identité des droits de la personnalité*, LPA, n°244, 7 décembre 2004, p. 3.

protection des données personnelles et le droit au respect du corps humain, de ses éléments et de ses produits ont donc pour traits communs leur indisponibilité, leur intransmissibilité et leur imprescriptibilité. En vertu de ces trois caractéristiques, « *le régime juridique d'un droit de la personnalité est incompatible avec celui d'un droit patrimonial* »¹⁰⁸⁸. En conséquence, les attributs de la personnalité et du corps humain du patient – et donc ses données médicales à caractère personnel – sont placés hors du marché. Cela signifie qu'ils ne peuvent faire l'objet d'un acte juridique à titre onéreux. Grégoire Loiseau explique que les « choses » hors du marché sont soustraites aux rapports marchands et, en particulier, de la vente¹⁰⁸⁹. De la même façon que « *les conventions ayant pour effet de conférer une valeur patrimoniale au corps humain, à ses éléments ou à ses produits sont nulles* »¹⁰⁹⁰, « *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* »¹⁰⁹¹. Bien que le législateur n'ait pas précisé le régime juridique applicable aux données de santé, et moins encore aux données médicales, il a pris le soin de les exclure du marché. A l'inverse, cette interdiction signifie-t-elle que les données médicales personnelles peuvent faire l'objet d'un acte juridique à titre gratuit ?

362. En raison de son extrapatrimonialité combinée à son attachement à la personne physique de laquelle elle émane, la donnée médicale personnelle est indisponible. Le principe d'indisponibilité prohibe tout acte de disposition portant sur l'objet appartenant à la catégorie des droits extrapatrimoniaux. En d'autres termes, l'indisponibilité empêche toute circulation de la chose entre deux ou plusieurs patrimoines, à supposer qu'elle puisse être inscrite dans le patrimoine originaire de son titulaire. De cette façon, il est impossible, pour le patient, de s'en déposséder. Il ressort que la gratuité de l'acte de disposition n'emporte aucune incidence sur sa validité. En consacrant le principe selon lequel « *le corps humain, ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial* »¹⁰⁹², c'est à tort que le législateur a autorisé le don des éléments et des produits du corps humain de la personne vivante. Assurément, s'il est possible d'en faire don, c'est qu'ils peuvent faire l'objet d'un acte de disposition. Vraisemblablement, les éléments et les produits du corps humain de la personne

¹⁰⁸⁸ HASSLER (T.), *op. cit.*, p. 5.

¹⁰⁸⁹ LOISEAU (G.), *Typologie des choses hors du commerce*, RTD. civ., 2000, n°01, p. 47.

¹⁰⁹⁰ Article 16-5 du code civil.

¹⁰⁹¹ Article L.1111-8 du code civil.

¹⁰⁹² Article 16-1 du code civil.

vivante devraient faire l'objet d'un régime distinct du corps humain qui les abrite. Une fois détachés de leur source, ils pourraient faire l'objet d'un droit patrimonial tout en étant exclus du marché¹⁰⁹³. En effet, le code civil dispose que « *tout ce qui est dans le commerce peut être vendu lorsque des lois particulières n'en ont pas prohibé l'aliénation* »¹⁰⁹⁴. Ainsi, la sacralité du corps serait préservée de toute marchandisation.

Alors que la donnée médicale peut être considérée comme un élément immatériel du corps humain, son caractère personnel empêche toute désaffectation avec le patient. A l'inverse des éléments et des produits humains désaffectés, la donnée médicale personnelle ne peut donc jamais faire l'objet d'un droit patrimonial. En ce sens, le Conseil d'Etat a pu rappeler que « *la protection des données personnelles [...] ne repose pas sur une logique patrimoniale mais sur une logique de droits attachés à la personne.* »¹⁰⁹⁵. En conséquence, les données médicales personnelles ne peuvent faire l'objet d'un acte de disposition ni à titre gratuit, ni à titre onéreux. Cette divergence avec le régime applicable aux éléments et aux produits du corps humain conforte l'idée selon laquelle la donnée médicale mériterait d'être protégée et encadrée par un droit spécifique.

363. Une chose exclue du marché peut, en revanche, être placée dans le commerce juridique. Alors que ces termes sont usuellement confondus, il convient de distinguer l'extrapatrimonialité de l'extracommercialité¹⁰⁹⁶. En effet, « *si tout ce qui est hors du commerce juridique est nécessairement en dehors du marché, la réciproque n'est pas vraie : une chose peut être soustraite aux rapports marchands sans échapper, de façon générale, au commerce juridique* »¹⁰⁹⁷. En principe, les choses situées en dehors du commerce ne peuvent être l'objet d'aucun acte juridique¹⁰⁹⁸. Elles ne peuvent être vendues¹⁰⁹⁹, elles ne peuvent faire l'objet d'un prêt à usage¹¹⁰⁰ et elles ne peuvent s'acquérir par prescription

¹⁰⁹³ LOISEAU (G.), *Typologie des choses hors du commerce, op. cit.*, p. 48.

¹⁰⁹⁴ Article 1598 du code civil.

¹⁰⁹⁵ CE, *Le numérique et les droits fondamentaux, op. cit.*, p. 264.

¹⁰⁹⁶ LOISEAU (G.), *Le droit des personnes, op. cit.*, p. 187.

¹⁰⁹⁷ LOISEAU (G.), *Typologie des choses hors du commerce, op. cit.*, p. 49.

¹⁰⁹⁸ Ancien article 1128 du code civil.

¹⁰⁹⁹ Article 1598 du code civil.

¹¹⁰⁰ Article 1878 du code civil.

acquisitive¹¹⁰¹. Toutefois, considérer qu'une chose placée hors du marché peut être l'objet de relations juridiques revient à admettre que son extracommercialité peut être relative. En ce sens, Rémy Libchaber explique que l'extracommercialité peut être limitée à l'inaliénabilité de la chose¹¹⁰². La commercialité d'une chose inaliénable peut donc être limitée à son prêt ou à sa location¹¹⁰³. Dès lors, une chose protégée par un droit extrapatrimonial peut entrer dans le commerce juridique sans jamais être rendue disponible, transmissible ou prescriptible. De cette façon, « *l'inaliénabilité fait rentrer les choses dans le circuit juridique, se contentant qu'il n'y ait pas de perte de propriété définitive* »¹¹⁰⁴. Il en résulte que l'extracommercialité peut être frappée d'une restriction partielle à certaines personnes ou à certains types de convention¹¹⁰⁵.

En dépit de l'extrapatrimonialité de la donnée médicale personnelle, celle-ci peut faire l'objet de convention ayant vocation à encadrer son traitement conformément aux limites des « *polices administratives spéciales* »¹¹⁰⁶ que sont la loi Informatique et Libertés modifiée et le RGPD. Effectivement, « *ce n'est pas tout commerce de données personnelles qui est illicite, seulement celui qui serait en contradiction avec les possibilités limitées qui leur ont été assignées par le législateur* »¹¹⁰⁷. Alors que la donnée médicale personnelle est indisponible, son usage, par tout responsable de traitement ou par tout sous-traitant, peut être organisé au sein d'une convention. D'ailleurs, l'article 28 du RGPD exige que le traitement de données personnelles effectué par un sous-traitant, qui agit au nom et pour le compte d'un responsable de traitement¹¹⁰⁸, soit régi par un acte juridique définissant l'objet et la durée du traitement, sa nature et sa finalité, le type de données à caractère personnel et les catégories de personnes concernées ou encore les modalités d'exercice de leurs droits¹¹⁰⁹. En pratique,

¹¹⁰¹ Article 2260 du code civil.

¹¹⁰² LIBCHABER (R.), *Biens (Civ.)*, RDT civ., mai 2016, actu. décembre 2019, § 113.

¹¹⁰³ LIBCHABER (R.), *Biens (Civ.)*, *op. cit.*, § 113.

¹¹⁰⁴ LIBCHABER (R.), *Biens (Civ.)*, *op. cit.*, § 112.

¹¹⁰⁵ Voir : GALLOUX (J.-C.), *Réflexions sur la catégorie des choses hors du commerce: l'exemple des éléments et des produits du corps humain en droit français*, Les Cahiers de droit, vol. 30, 1989. n°4, p. 1011.

¹¹⁰⁶ Termes empruntés à OCHOA (N.), *Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition*, RFDA, 2016, n°06, p.1157.

¹¹⁰⁷ OCHOA (N.), *op. cit.*, p. 1165.

¹¹⁰⁸ Article 4.8 du RGPD.

¹¹⁰⁹ MARTIAL-BRAZ (N.), *Le contrat entre responsable de traitement et sous-traitant*, Dalloz IP / IT, 2021, n° 04, p. 181 à p. 187.

une convention portant sur les données médicales personnelles du patient est systématiquement conclue entre le télémedecin et le fournisseur d'une solution de télémédecine mais encore entre le promoteur d'une recherche dans le domaine de la santé et son investigateur.

Tout en respectant l'inaliénabilité de la donnée médicale personnelle, la conventionnalité du traitement des données médicales personnelles tend à accroître leur protection. Assurément, les actes juridiques tiennent lieu de loi à ce qui les ont faits¹¹¹⁰. Autrement dit, ce qui a été déterminé dans le contrat, conformément au droit positif, s'impose aux parties. De surcroît, la force obligatoire du contrat le rend opposable par les tiers. En effet, les tiers peuvent opposer le contrat signé entre les parties contractantes¹¹¹¹. Ainsi, tout manquement contractuel ayant causé un préjudice pour le tiers suffit à engager la responsabilité délictuelle du débiteur défaillant. De cette façon, le patient concerné par le traitement de ses données médicales personnelles pourrait engager la responsabilité délictuelle du responsable de traitement ou du sous-traitant les ayant détournées de leur finalité déterminée, explicite et légitime, ou les ayant conservées au-delà de la durée nécessaire à l'accomplissement de la finalité définie dans la convention. Si le patient est un tiers à la convention encadrant le traitement de ses données médicales personnelles, il n'en demeure pas moins qu'il bénéficie toujours de la qualité de « personne concernée » et qu'il jouit d'un droit à l'autodétermination informationnelle sur celles-ci. En définitive, les conventions d'exploitation d'informations personnelles « *protègent la personne contre les contractants ou contre elle-même et participent de l'approche personnaliste du droit* »¹¹¹². Alors que les conventions relatives aux données personnelles permettent de définir et d'encadrer la finalité et les moyens du traitement conformément aux dispositions du droit à la protection des données personnelles, la personne concernée peut toujours faire obstacle à sa mise en œuvre grâce à l'exercice de ses droits¹¹¹³.

¹¹¹⁰ Article 1103 du code civil.

¹¹¹¹ LATINA (M.), *Contrat : généralités (Civ.)*, RDT civ., mai 2017, actu. février 2020, § 150.

¹¹¹² MALLET-POUJOL (N.), *Appropriation de l'information : l'éternelle chimère*, Recueil Dalloz, 1997, n°38, p. 334.

¹¹¹³ Alors que la finalité et les moyens du traitement de données personnelles sont déterminés par le responsable de traitement, qui en définit donc l'usage, la personne concernée peut, au moyen de ses droits, en contrôler cet usage.

364. Compte tenu de ce qui précède, la donnée médicale personnelle, qualifiée de chose anthropomorphique personnelle, fait l'objet d'un droit extrapatrimonial la plaçant en dehors du marché. Cependant, son extrapatrimonialité n'emporte qu'une extracommercialité partielle. En effet, la chose anthropomorphique personnelle est située dans le commerce juridique pour les actes encadrant son traitement dans le respect des normes applicables en matière de protection des données à caractère personnel.

Paragraphe 2 : Le statut de la donnée médicale anonymisée

365. L'anonymisation de la donnée médicale personnelle a pour conséquence la rupture du lien entre la chose anthropomorphique et le patient (A). Si la donnée médicale à caractère personnel meurt, la chose anthropomorphique demeure et devient une chose sans maître. Alors susceptible d'appropriation et de marchandisation, il apparaît nécessaire de protéger l'humanité qu'elle renferme contre toute dérive mercantile en la qualifiant de *chose commune* (B).

A) L'apparition d'une chose commune désaffectée

366. Le groupe de travail « Article 29 »¹¹¹⁴ a défini l'anonymisation comme « *une technique appliquée aux données à caractère personnel afin d'empêcher irréversiblement leur identification* »¹¹¹⁵. Si plusieurs procédés peuvent être utilisés pour y parvenir, deux principales techniques d'anonymisation exposées par le G29 ont été retenues par la CNIL. En premier lieu, les techniques de randomisation permettent de transformer les données à caractère personnel de façon à ce qu'elles ne se réfèrent plus à la personne concernée. La randomisation altère « *la véracité des données afin d'affaiblir le lien entre les données et l'individu. Si les données sont suffisamment incertaines, elles ne peuvent plus être rattachées à un individu en particulier.* »¹¹¹⁶. En second lieu, les techniques de généralisation consistent à diluer « *les attributs des personnes concernées en modifiant leur échelle ou leur ordre de*

¹¹¹⁴ Autrement appelé le « G29 ».

¹¹¹⁵ Groupe de travail « Article 29 », *Avis 05/2014 sur les Techniques d'anonymisation*, 10 avril 2014, p.7.

¹¹¹⁶ Groupe de travail « Article 29 », *Avis 05/2014 sur les Techniques d'anonymisation*, *op. cit.*, p.13.

grandeur respectif »¹¹¹⁷. Les données ne sont plus personnelles dans la mesure où elles deviennent communes à un ensemble d'individus.

Quel que soit le mécanisme d'anonymisation utilisé, la donnée personnelle devient effectivement anonyme lorsque trois critères sont réunis¹¹¹⁸. D'abord, il ne doit plus être possible d'individualiser une personne physique au sein d'un jeu de données anonymisées. Ensuite, il ne doit plus être possible de corréler différents ensembles de données anonymisées concernant un même individu. Finalement, il ne doit plus être possible d'inférer de nouvelles informations sur un individu à partir des données anonymisées¹¹¹⁹. L'effectivité de l'anonymisation des données personnelles s'apprécie en fonction « *des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement* »¹¹²⁰. Pour cela, « *il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci* »¹¹²¹. En d'autres termes, le G29 considère qu'une donnée est véritablement anonymisée lorsque la réidentification de la personne concernée est raisonnablement irréversible. Vraisemblablement, « *ce n'est que si les données sont agrégées par le responsable de leur traitement à un niveau où les événements individuels ne sont plus identifiables que l'ensemble des données résultant peut être qualifié d'anonyme* »¹¹²².

367. La modification de la nature de la donnée personnelle en une donnée anonymisée implique son traitement. En effet, « *l'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible* »¹¹²³. En d'autres termes, l'anonymisation correspond à un traitement de données personnelles pouvant

¹¹¹⁷ Groupe de travail « Article 29 », *Avis 05/2014 sur les Techniques d'anonymisation, op. cit.*, p.18.

¹¹¹⁸ L'individualisation, la corrélation et l'inférence.

¹¹¹⁹ Groupe de travail « Article 29 », *Avis 05/2014 sur les Techniques d'anonymisation, op. cit.*, p.10.

¹¹²⁰ Considérant 26 du RGPD.

¹¹²¹ *Ibid.*

¹¹²² Groupe de travail « Article 29 », *Avis 05/2014 sur les Techniques d'anonymisation, loc. cit.*

¹¹²³ CNIL, *L'anonymisation de données personnelles*, 19 mai 2020. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 07 avril 2021.

intervenir au moment de leur collecte ou à l'issue de la finalité pour laquelle elles ont été originellement collectées.

368. Les données médicales personnelles, collectées initialement à l'occasion de la prise en charge sanitaire du patient, ou de sa participation à une recherche impliquant la personne humaine, peuvent éventuellement faire l'objet d'un traitement ultérieur ayant pour finalité leur anonymisation¹¹²⁴. Ainsi, le traitement ayant pour finalité l'anonymisation des données médicales personnelles du patient n'est licite que s'il est compatible avec la finalité pour laquelle elles ont été initialement produites. Selon le G29, « *l'anonymisation, en tant que traitement ultérieur de données à caractère personnel, peut être jugée compatible avec les finalités originales du traitement, à condition que le processus d'anonymisation soit de nature à produire des informations anonymisées* »¹¹²⁵ de façon irréversible. Le responsable de traitement souhaitant anonymiser les données médicales personnelles des patients n'aurait donc pas à démontrer la compatibilité entre l'anonymisation et la prise en charge sanitaire à la lumière des critères définis à l'article 6.4 du RGPD¹¹²⁶.

En outre, lorsqu'un traitement de données personnelles est ultérieurement mis en œuvre pour une finalité compatible avec la finalité initiale, « *aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel n'est requise* »¹¹²⁷. Néanmoins, les données médicales personnelles étant des données concernant la santé, leur traitement n'est autorisé, par exception, que s'il répond à l'une des dix conditions énumérées à l'article 9.2 du RGPD. Cela signifie que l'anonymisation des données médicales personnelles doit poursuivre un objectif réglementé. A l'aune de ces conditions exhaustives, ce traitement peut être autorisé dans trois hypothèses. En premier lieu, lorsque le patient a donné son consentement explicite pour une ou plusieurs finalités spécifiques¹¹²⁸. Alors que l'anonymisation constitue la finalité principale du traitement, le principe de transparence

¹¹²⁴ Groupe de travail « Article 29 », *Avis 05/2014 sur les Techniques d'anonymisation, op. cit.*, p.7.

¹¹²⁵ Groupe de travail « Article 29 », *Avis 05/2014 sur les Techniques d'anonymisation, op. cit.*, p.9.

¹¹²⁶ L'analyse de l'adéquation entre une finalité initiale et une finalité ultérieure doit tenir compte de l'existence éventuelle d'un lien entre la finalité originelle et la finalité ultérieurement envisagée, du contexte dans lequel les données personnelles ont été collectées, de la nature des données personnelles, des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ainsi que de l'existence de garanties appropriées pour la sécurisation des données personnelles.

¹¹²⁷ Considérant 50 du RGPD.

¹¹²⁸ Article 9.2 a) du RGPD.

implique d'informer la personne concernée des finalités secondaires du traitement. Dans l'hypothèse d'une anonymisation de données médicales, il convient d'informer le patient de l'ensemble des objectifs consécutifs à ce traitement. Si cette finalité secondaire était leur commercialisation, le patient serait alors libre de l'autoriser ou de la refuser. En deuxième lieu, l'anonymisation des données médicales personnelles peut être mise en œuvre lorsqu'elle est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique¹¹²⁹. En troisième lieu, l'anonymisation de ces informations peut intervenir lorsqu'elle est nécessaire à des fins de recherche scientifique¹¹³⁰. La détermination d'une condition autorisant, à titre dérogatoire, l'anonymisation des données médicales personnelles semble hypocrite. Une fois anonymisée, la donnée médicale peut être exploitée pour n'importe quelle autre finalité. Autrement dit, la donnée médicale rendue anonyme peut être traitée pour des finalités détournées en toute légalité. Alors, pourquoi exiger la détermination d'une condition légitimant l'anonymisation des données médicales personnelles par l'établissement ou le professionnel de santé dépositaire si, une fois la finalité accomplie, celui-ci peut en faire un libre usage ?

Quoi qu'il en soit, le traitement aux fins d'anonymisation des données médicales personnelles du patient peut être licitement mis en œuvre dès lors qu'il s'inscrit en conformité avec les dispositions du RGPD. Assurément, la donnée médicale anonymisée est créée à partir d'une donnée médicale personnelle. En ce sens, la CNIL affirme que « *les données traitées dans le cadre du processus d'anonymisation sont des données à caractère personnel* »¹¹³¹. Par conséquent, les règles applicables en matière de protection des données personnelles demeurent applicables au traitement ayant pour objet cette transformation.

369. Il en ressort que le patient concerné par l'anonymisation de ses données médicales personnelles conserve certains de ses droits, à tout le moins pendant ce processus de transformation. Dans un premier temps, l'établissement ou le professionnel de santé responsable de traitement doit, dans la mesure du possible, en informer le patient concerné¹¹³². Le respect de ce droit essentiel pour la personne concernée ne devrait pas poser

¹¹²⁹ Article 9.2 i) du RGPD.

¹¹³⁰ Article 9.2 j) du RGPD.

¹¹³¹ CNIL, Délibération n° 2016-047 suite à la demande d'autorisation n°1894953, 25 février 2016.

¹¹³² Article 11.2 du RGPD.

de difficulté. En effet, les données médicales étant formalisées au sein d'un dossier constitué pour chaque patient¹¹³³, les professionnels et les établissements de santé disposent, à ce stade, des éléments d'identification permettant son information individuelle. De surcroît, sauf à ce que l'anonymisation soit effectuée par un outil totalement automatisé, seule une personne physique soumise au secret professionnel médical peut être habilitée à accéder à ces données confidentielles aux fins de leur anonymisation¹¹³⁴. S'agissant de cette sous-catégorie de données de santé, l'information relative à l'anonymisation des données médicales du patient apparaît réalisable. C'est pourquoi elle doit être, quoi qu'il en coûte, privilégiée.

Le G29 estime qu'en vertu des principes d'équité et de responsabilité prévus par le RGPD, les responsables de traitement devraient fournir les informations aux personnes concernées bien avant les délais réglementaires¹¹³⁵. De cette façon, les personnes concernées seraient davantage placées en capacité d'exercer leurs droits en lien avec le traitement de leurs données personnelles. Le responsable de traitement ayant l'intention de traiter les données médicales personnelles du patient pour une finalité ultérieure à sa prise en charge médicale doit donc préalablement l'en informer¹¹³⁶. En effet, il convient d'attendre un certain laps de temps entre la délivrance de l'information relative au traitement projeté et le commencement de sa mise en œuvre. A l'instar du délai de réponse du responsable de traitement aux demandes d'exercice des droits de la personne concernée¹¹³⁷, le délai entre l'information portant sur un traitement ultérieur et sa réalisation pourrait être d'un mois. En l'espèce, il semble indispensable que la personne concernée par l'anonymisation de ses données personnelles en soit informée le plus en amont possible.

Une fois avertie du traitement ayant pour finalité l'anonymisation de ses données personnelles, il ressort des dispositions du RGPD que la personne concernée peut toujours s'y opposer¹¹³⁸. Mathilde Cavalier souligne que « *le maintien d'un mécanisme utilisant la volonté du patient tient au fait que, malgré l'apparition de cette nouvelle chose, elle procède*

¹¹³³ Cf. Paragraphe 2 de la Section 1 du Chapitre 1 du Titre 1 de la Première partie de la présente thèse.

¹¹³⁴ Cf. Paragraphe 193.

¹¹³⁵ Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, 29 novembre 2017, actu. 11 avril 2018, p. 18.

¹¹³⁶ Article 14.4 du RGPD.

¹¹³⁷ Article 12.3 du RGPD.

¹¹³⁸ Article 11.2 du RGPD.

d'une donnée personnelle »¹¹³⁹. Cela signifie que la personne concernée peut, en toute circonstance, maîtriser l'usage de ses données personnelles en refusant qu'elles lui échappent définitivement. D'une certaine façon, « *l'existence même de la donnée anonymisée reste donc marquée par une volonté du patient qui est à l'origine de sa naissance* »¹¹⁴⁰. Néanmoins, si le responsable de traitement démontre qu'il n'est pas en mesure d'identifier la personne concernée au moment de l'anonymisation de ses données – encore – personnelles, ses droits d'accès, de rectification, d'effacement, de limitation et de portabilité ne s'appliquent pas. En effet, le responsable de traitement qui procède à une anonymisation de données personnelles n'est pas tenu de « *conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter* »¹¹⁴¹ le RGPD. Toutefois, le législateur européen prévoit que le responsable de traitement doit répondre à la demande d'exercice de l'un de ces droits dès lors que la personne concernée fournit des informations complémentaires permettant de l'identifier. En revanche, une fois le traitement effectué, la donnée devenue anonyme est irréversiblement identifiable. Le cas échéant, « *il semble effectivement impossible d'accéder individuellement et personnellement à celle-ci.* »¹¹⁴². Par conséquent, la personne concernée perdra, à tout jamais, son droit à l'autodétermination informationnelle sur ses données anonymisées.

370. En raison de l'absence de clarté de l'article 11 du RGPD¹¹⁴³, il paraît nécessaire de préciser que les droits de la personne concernée sur ses données personnelles ne subsistent que pendant leur processus d'anonymisation. Une fois transformée en information anonyme, il n'y a plus lieu d'appliquer les principes relatifs à la protection des données personnelles.

¹¹³⁹ CAVALIER (M.), *La propriété des données de santé*, Marion GIRER (dir.), Thèse de Doctorat, Droit, Université Lyon III, 2016, p. 73.

¹¹⁴⁰ CAVALIER (M.), *op. cit.*, p. 74.

¹¹⁴¹ Article 11.1 du RGPD.

¹¹⁴² CAVALIER (M.), *op. cit.*, p. 70.

¹¹⁴³ « Article 11 - Traitement ne nécessitant pas l'identification :

1. Si les finalités pour lesquelles des données à caractère personnel sont traitées n'imposent pas ou n'imposent plus au responsable du traitement d'identifier une personne concernée, celui-ci n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le présent règlement.

2. Lorsque, dans les cas visés au paragraphe 1 du présent article, le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. En pareils cas, les articles 15 à 20 ne sont pas applicables, sauf lorsque la personne concernée fournit, aux fins d'exercer les droits que lui confèrent ces articles, des informations complémentaires qui permettent de l'identifier. ».

En effet, le RGPD ne s'applique pas « *au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche* »¹¹⁴⁴. Cela signifie que les personnes physiques ou morales qui traitent des données rendues anonymes ne sont pas soumises au cadre juridique applicable aux données à caractère personnel. En effet, « *l'utilisation d'un processus d'anonymisation crée une nouvelle donnée anonyme et sur laquelle aucun droit personnel ne peut être revendiqué par le patient* »¹¹⁴⁵. La donnée anonymisée est désaffectée de l'individu duquel elle émane. Ainsi, la donnée anonymisée ne comporte plus d'attribut de la personnalité spécifique à une personne physique. L'intégrité morale de l'individu ne requiert donc plus de protection par les droits de la personnalité. Dans ce cas, quels sont le statut et le régime applicables à la donnée anonymisée ?

Selon Mathilde Cavalier, « *même si elles ne sont aujourd'hui pas saisies directement en tant qu'objet par le droit, [les données anonymes] n'ont nécessairement pas d'autre statut que celui de bien et donc susceptible d'un droit de propriété au profit du collecteur* »¹¹⁴⁶. Autrement dit, l'auteur considère que la donnée anonymisée devient un bien meuble incorporel appropriable. Assurément, la donnée anonymisée n'étant plus rattachée à son titulaire, elle se transforme en une chose sans maître susceptible d'appropriation et d'intégrer le marché unique européen¹¹⁴⁷.

371. Compte tenu de ce qui précède, la chose anthropomorphique, détachée du corps du patient et de sa personnalité, peut-elle faire l'objet d'un droit patrimonial ? En l'état actuel du droit positif, cette assomption apparaît licite. Il en ressort que les établissements de santé privés et les professionnels de santé libéraux pourraient légalement vendre les dossiers médicaux qu'ils auraient préalablement anonymisés. Aussi, les patients pourraient demander la copie de leurs dossiers médicaux, ou procéder à l'extraction du contenu de leur DMP, afin de les anonymiser pour les aliéner. L'absence de définition du statut de la donnée médicale anonymisée peut donc conduire à l'instrumentalisation du corps humain. En effet, celui-ci pourrait être observé comme un générateur de données commercialisables. Alors, les

¹¹⁴⁴ Considérant 26 du RGPD.

¹¹⁴⁵ CAVALIER (M.), *op. cit.*, p. 70.

¹¹⁴⁶ CAVALIER (M.), *op. cit.*, p. 191.

¹¹⁴⁷ Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *JOUE* L 303/59, 28 novembre 2018.

individus les plus vulnérables pourraient monnayer leurs données médicales anonymisées et les professionnels de santé pourraient tirer profit de la maladie. Seuls les établissements investis d'une mission de service public ne pourraient commercialiser les données médicales recueillies et produites à l'occasion de la prise en charge sanitaire des patients¹¹⁴⁸. En effet, les données médicales anonymisées¹¹⁴⁹ par les professionnels de santé exerçant au sein de tels établissements sont des informations publiques¹¹⁵⁰ accessibles¹¹⁵¹ et réutilisables¹¹⁵² gratuitement à l'exception des frais liés aux coûts supportés pour leur communication et leur mise à disposition¹¹⁵³. Le processus d'anonymisation de la donnée médicale personnelle permet simplement de contourner l'application du cadre juridique relatif à la protection des données personnelles. Une fois anonymisée, la donnée médicale est délestée de tout rempart contre sa marchandisation.

372. Si la donnée médicale anonymisée n'est plus reliée au patient, elle demeure un élément immatériel de son corps humain. Même anonyme, la chose anthropomorphique consiste en la réification de la condition physiologique d'un individu. Elle porte donc en elle une certaine humanité qui devrait être sauvegardée au moyen d'un régime juridique particulier. Selon Grégoire Loiseau, les éléments et produits détachés du corps sacré peuvent être instrumentalisés comme des choses¹¹⁵⁴. Cependant, l'auteur précise que « *le droit des choses pourrait en revanche être utilement mis à profit pour donner aux éléments et produits, une fois prélevés, un statut respectueux de leur nature humaine, qui les différencie de la communauté des biens* »¹¹⁵⁵. De cette même façon, la donnée médicale anonymisée, détachée du corps humain et désaffectée de la personnalité du patient, devrait être soumise au droit des choses. Ainsi, elle échapperait à la catégorie des biens et bénéficierait d'un statut respectueux de la sacralité du corps duquel elle provient. De surcroît, la protection concédée à la chose anthropomorphique anonymisée par le régime du droit des choses autorise son libre usage

¹¹⁴⁸ Cf. Paragraphe 419.

¹¹⁴⁹ Articles L.313-1-2 et R.322-3 du code des relations entre le public et l'administration.

¹¹⁵⁰ Article L.300-2 du code des relations entre le public et l'administration.

¹¹⁵¹ Article L. 311-1 du code des relations entre le public et l'administration.

¹¹⁵² Article L. 321-1 du code des relations entre le public et l'administration.

¹¹⁵³ Articles R. 311-11 et L.324-1 du code des relations entre le public et l'administration.

¹¹⁵⁴ LOISEAU (G.), *Typologie des choses hors du commerce*, op. cit., p. 49.

¹¹⁵⁵ LOISEAU (G.), *Pour un droit des choses*, op. cit., p. 3018.

tout en l'écartant du marché. Au demeurant, la donnée médicale anonymisée, étant par nature une chose anthropomorphique, devrait appartenir à la catégorie des choses communes.

B) L'application d'un régime protecteur contre les dérives mercantiles

« Au vrai, la chose commune peut être la source possible de biens nouveaux. »¹¹⁵⁶.

373. Si la donnée médicale anonymisée n'était pas régie par un statut particulier, elle deviendrait un *res nullius*. Cette chose sans maître n'ayant jamais fait l'objet d'une appropriation pourrait, eu égard à son changement de statut, être appropriée *de facto* par le responsable de traitement ayant procédé à la création de cette chose nouvelle. Ainsi, le responsable de l'anonymisation de la chose anthropomorphique personnelle en deviendrait le propriétaire naturel. En effet, « la désaffectation de la chose la rend à nouveau disponible entre les mains de son [nouveau] titulaire »¹¹⁵⁷. Celui-ci pourrait alors en réserver l'usage exclusif ou l'aliéner en dépit de son humanité. Il y aurait alors une distinction entre le sort réservé aux données médicales anonymisées dans le secteur public et celles traitées dans le secteur privé¹¹⁵⁸.

Afin de prévenir l'enclosure de la donnée médicale anonymisée par les professionnels de santé du secteur privé, et les dérives mercantiles pouvant résulter de sa patrimonialité, le législateur devrait soustraire la donnée médicale anonymisée à la communauté des biens. En ce sens, Grégoire Loiseau énonce que le respect particulier dû à une catégorie de chose, ou à une chose particulière, peut être inscrit dans la loi indépendamment des règles de droit commun applicables aux choses ou aux biens¹¹⁵⁹. En d'autres termes, une protection spécifique à la chose anthropomorphique anonymisée pourrait résulter de la loi. Selon un courant doctrinal, les objets devant échapper au droit des biens devraient être soumis au droit des choses. Lorsque cet objet apparaît relativement inépuisable et disponible pour l'usage de tous, il peut être inscrit parmi les choses communes. En effet, « dans une vision renouvelée

¹¹⁵⁶ LOISEAU (G.), *Pour un droit des choses*, op. cit., p. 3016.

¹¹⁵⁷ LOISEAU (G.), *Typologie des choses hors du commerce*, op. cit., p. 51.

¹¹⁵⁸ Cf. Paragraphes 156, 371, 506.

¹¹⁵⁹ LOISEAU (G.), *Pour un droit des choses*, op. cit. p. 3015.

¹¹⁵⁹ *Ibid.*

[de la chose commune], plus « normative », l'idée a été défendue que la qualification puisse être utilisée pour réserver une chose à l'usage commun, en excluant l'appropriation individuelle »¹¹⁶⁰. Certainement, Grégoire Loiseau affirme que cette « catégorie devient alors une sorte de refuge pour mettre certaines choses à l'abri des ambitions individuelles des hommes »¹¹⁶¹. De la même façon, Mélanie Clément-Fontaine atteste que « c'est parce qu'il y a une réelle volonté de laisser à l'usage commun certaines choses qu'elles sont qualifiées de choses communes »¹¹⁶². Identiquement, Marie-Alice Chardeaux assure que « cette qualification permet de soustraire certaines ressources à la propriété exclusive, afin d'en garantir l'usage commun »¹¹⁶³. La qualification juridique des choses communes apparaît alors comme un mécanisme juridique utilitaire. Rémy Libchaber a ainsi constaté que la qualification d'un objet en chose commune « ne résultait pas d'une contrainte spécifique que la nature exercerait sur le droit, mais à l'inverse d'une volonté juridique de soustraire dans leur ensemble ces biens à toute emprise individuelle »¹¹⁶⁴. Si le régime des choses communes était applicable aux données médicales anonymisées, celles-ci seraient alors préservées de toute appropriation. Assurément, il existe des objets qui, en raison de leur appartenance à l'humanité, ne peuvent être traités comme de simples biens. A l'inverse des biens, la condition de chose a le mérite de respecter l'être qui en est la source¹¹⁶⁵.

374. Héritée du droit romain, la notion des *res communes* a été consacrée à l'article 714 du code civil dès sa création en 1803. Depuis, le législateur considère qu'« il est des choses qui n'appartiennent à personne et dont l'usage est commun à tous »¹¹⁶⁶. Traditionnellement, le statut des choses communes était appliqué aux ressources naturelles perpétuelles telles que l'air, la mer, l'eau ou la lumière. Progressivement, cette catégorie juridique a intégré des

¹¹⁶⁰ ROCHFELD (J.), *Quel modèle pour construire des communs ?*, In PARANCE (B.), DE SAINT VICTOR (J.), CNRS, 2014, p. 112.

¹¹⁶¹ LOISEAU (G.), *Pour un droit des choses*, op. cit., p. 3016.

¹¹⁶² CLEMENT-FONTAINE (M.), *Un renouveau des biens communs : des biens matériels aux biens immatériels*, In : Faculté de droit et des sciences sociales de Poitiers - Actes & Colloques, Les modèles propriétaires - Actes du colloque international organisé par le CECOJI - En hommage au professeur Henri-Jacques LUCAS, LGDJ, 2012, p. 51.

¹¹⁶³ CHARDEAUX (M.-A.), *Nommer la prérogative d'usage des choses communes*, Recueil Dalloz, 2019, n°40, p. 2195 ; CHARDEAUX (M.-A.), *Les choses communes*, Thèse de Doctorat, Droit, Université Paris I, LGDJ, 2006, préf. LOISEAU (G).

¹¹⁶⁴ LIBCHABER (R.), *Biens (Civ.)*, op. cit. § 273.

¹¹⁶⁵ LOISEAU (G.), *Pour un droit des choses*, op. cit., p. 3015.

¹¹⁶⁶ Article 714 du code civil.

objets de différentes natures dont, essentiellement, des choses immatérielles et intangibles¹¹⁶⁷. La lettre de l'article 714 du code civil ne limite pas la notion des choses communes à une catégorie d'objet et « *permet de s'émanciper de la liste traditionnelle des choses communes* »¹¹⁶⁸. Il revient donc au législateur, voire au juge, l'opportunité d'y introduire toute chose devant échapper à la propriété. L'élargissement de la catégorie des choses communes aux objets immatériels témoigne d'une recherche d'équilibre face à leur appropriation grandissante¹¹⁶⁹. L'inscription de toute donnée médicale anonymisée au sein de cette catégorie juridique, indépendamment de son statut public ou privé, permettrait d'assurer sa non-appropriation tout en garantissant son usage par tous.

375. Effectivement, le statut des choses communes emporte leur inappropriation au profit d'un usage commun au bénéfice de tous. En d'autres termes, Jamel Djoudi explique que « *tout le monde occupe ces choses mais personne ne les acquiert* »¹¹⁷⁰. Précisément, le critère de la mise à disposition des choses communes signifie que leur usage est ouvert à tous, « *en libre accès, sans cibler le bénéfice d'une communauté strictement délimitée* »¹¹⁷¹. Néanmoins, les pouvoirs publics doivent définir une gouvernance relative à leur libre usage. En effet, l'article 714 du code civil complète que « *des lois de police règlent la manière d'en jouir* ». Ainsi, la mise à disposition des choses communes doit faire l'objet d'une régulation et d'une protection étatique. A ce titre, l'Etat pourrait garantir l'accessibilité des données médicales anonymisées à tout individu qui souhaiterait en faire un usage conformément à l'ordre public et aux bonnes mœurs. Si les données médicales anonymisées faisaient l'objet d'une jouissance commune organisée et garantie par l'Etat, elles pourraient être utilisées simultanément par une multitude d'acteurs non rivaux. Mises à la disposition de tous, ces données indéfiniment duplicables et inépuisables échapperaient à tout désir d'appropriation et, par suite, à toute aliénation.

¹¹⁶⁷ Voir : PARANCE (B.), DE SAINT VICTOR (J.), *Repenser les biens communs*, CNRS éditions, 2014.

¹¹⁶⁸ CLEMENT-FONTAINE (M.), *Un renouveau des biens communs : des biens matériels aux biens immatériels*, *loc. cit.*

¹¹⁶⁹ Voir : CLEMENT-FONTAINE (M.), *loc. cit.* ; FERAL-SCHUHL (C.), PAUL (C.), *Numérique et libertés : un nouvel âge démocratique*, Rapport d'information déposé par la commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, Assemblée nationale, octobre 2015, p. 230 à p. 234.

¹¹⁷⁰ DJOUDI (J.), *Occupation*, Répertoire de droit civil, juillet 2018, paragraphe 29.

¹¹⁷¹ FERAL-SCHUHL (C.), PAUL (C.), *op. cit.*, p. 234.

376. Soumettre les données médicales anonymisées au régime de l'article 714 du code civil permettrait de reconnaître une nouvelle ressource en tant que *commun numérique*¹¹⁷². Celles-ci pourraient alors constituer un nouveau *domaine commun informationnel* inspiré du domaine public¹¹⁷³. En 2015, le législateur a tenté d'entériner la création d'un *domaine commun informationnel* dans l'avant-projet de loi pour une république numérique soumis à une consultation publique¹¹⁷⁴. L'article 8 proposait de protéger les ressources communes appartenant au domaine public contre les pratiques d'appropriation conduisant à en interdire l'accès. Ce projet incluait les éléments immatériels ayant fait l'objet d'une divulgation publique sans être protégés par un droit spécifique, les œuvres et les inventions dont la durée de protection légale a expiré, ainsi que les archives publiques. Finalement, cette initiative a été abandonnée compte tenu des impacts sur la propriété intellectuelle des auteurs et des éditeurs qui n'auraient jamais pu protéger leurs créations fondées sur les communs de la connaissance¹¹⁷⁵. Si un nouveau *domaine commun informationnel* venait à émerger, il consisterait simplement au regroupement des choses communes numériques dont, évidemment, les données médicales anonymisées. Comme le suggère la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, il semble alors « possible de faire usage de l'article 714 du code civil afin de reconnaître une ressource en tant que commun numérique, en confiant à la puissance publique le rôle de garant de la jouissance commune, si nécessaire par une loi de police »¹¹⁷⁶. Ainsi, l'intégration d'une donnée médicale anonymisée au sein d'une base de données, et sa réutilisation à des fins d'innovation, n'emporteraient pas sa réservation privative. En effet, seuls les résultats issus de son exploitation peuvent éventuellement faire l'objet d'un droit de propriété¹¹⁷⁷.

377. Inscrire les données médicales anonymisées parmi les choses communes permettrait, conjointement, de lutter contre l'asservissement du corps humain, de favoriser leur

¹¹⁷² FERAL-SCHUHL (C.), PAUL (C.), *op. cit.*, p. 235.

¹¹⁷³ Voir : OSTROM (E.), *Gouvernance des biens communs, pour une nouvelle approche des ressources naturelles*, Révisé par Laurent Baechler, De Boeck, 2010 ; LUCAS-SCHLOETTER (A.), *Le « domaine commun informationnel »*, Dalloz IP/IT, 2018, n° 02, p. 90 à p. 93.

¹¹⁷⁴ Disponible en ligne sur le site [www.republique-numerique.fr].

¹¹⁷⁵ MAUREL (L.), *La reconnaissance du « domaine commun informationnel » : tirer les enseignements d'un échec législatif*, In ALIX (N.), BANCEL (J.-L.), CORIAT (B.), SULTAN (F.), *Vers une République des biens communs ?*, Les liens qui libèrent, 2018, Chapitre 9.

¹¹⁷⁶ FERAL-SCHUHL (C.), PAUL (C.), *op. cit.*, p. 235.

¹¹⁷⁷ Cf. Paragraphes 416 s.

circulation et de promouvoir les initiatives innovantes dans le domaine de la santé tout en protégeant les droits fondamentaux du patient. L'ouverture et la circulation des données médicales apparaissent absolument essentielles à l'évolution du système de santé. En effet, leur exploitation concourt au développement d'outils d'aide au diagnostic et à la décision médicale, à l'amélioration des stratégies préventives, diagnostiques et thérapeutiques personnalisées ou encore à l'efficacité de l'épidémiologie et de la santé publique. Au mépris de certaines allégations contraires, le laboratoire d'innovation numérique de la CNIL a démontré que les données anonymisées possédaient une utilité macroscopique et portaient en elles un potentiel d'utilisation¹¹⁷⁸. L'application d'un régime protecteur contre la marchandisation de la donnée médicale anonymisée profiterait donc également à l'innovation. En effet, la chose anthropomorphique anonymisée demeurerait à la libre disposition de tout porteur de projet souhaitant l'exploiter pour toute finalité. Par exemple, les acteurs pourraient vérifier la faisabilité d'un projet avant de l'entreprendre et de requérir l'accès à des données médicales personnelles dont la granularité serait plus fine. Ce libre accès aux communs numériques profiterait également aux porteurs de projets connexes à la santé ne répondant pas à un motif d'intérêt public ou scientifique légitimant l'accès à des données médicales pseudonymisées.

Au même titre que le principe de gratuité gouvernant l'utilisation des éléments et des produits du corps humain préviendrait leur commercialisation et leur trafic¹¹⁷⁹, l'usage libre et gratuit de la chose anthropomorphique anonymisée l'en prémunirait. Une fois anonymisée, la donnée médicale ne pourrait jamais faire l'objet d'un droit de propriété et la chose anthropomorphique ne pourrait être observée comme un objet de mercantilisation.

¹¹⁷⁸ Voir : HARY (E.), *Quels usages pour les données anonymisées ?*, Laboratoire d'Innovation Numérique de la CNIL, 14 novembre 2017.

¹¹⁷⁹ CAIRE (A.-B.), *Le corps gratuit : réflexions sur le principe de gratuité en matière d'utilisation de produits et d'éléments du corps humain*, RDSS, 2015, n°05, p. 866.

Section 2 : L'inappropriabilité de la donnée médicale

« Avec le concept de propriété de l'information personnelle, c'est tout le rapport de l'homme à lui-même qui se détermine dans une terrible équation appropriation-disposition. »¹¹⁸⁰.

378. La question de l'appropriation de l'information, et conséquemment des données personnelles et anonymes, fait débat depuis plusieurs décennies. Nicolas Binctin a constaté que le statut juridique de la donnée et son intégration dans le régime commun ou le régime spécial du droit des biens étaient discutés depuis plus de trente ans¹¹⁸¹. Alors qu'un courant doctrinal plaide en faveur d'une « *approche propriétaire des données* »¹¹⁸², les acteurs institutionnels résistent contre cette tendance tandis que le législateur reste muet sur le sujet. Il n'empêche que « *la question de l'appropriation des données est le corollaire de l'enjeu économique que celles-ci représentent* »¹¹⁸³. En effet, tout objet possédant une certaine valeur emporte un désir d'appropriation. A l'heure où l'information constitue l'or noir sur lequel repose notre société numérique, il apparaît nécessaire de résoudre la question de l'appropriation de la donnée médicale avant que le législateur ne finisse, sous des pressions économiques ou politiques, par entériner les allégations empiriques. En considération du statut et du régime que nous accordons aux données médicales personnelles et anonymes¹¹⁸⁴, celles-ci ne pourraient faire ni l'objet d'une propriété mobilière de droit commun (**Paragraphe 1**), ni l'objet d'une propriété intellectuelle spéciale¹¹⁸⁵ (**Paragraphe 2**).

Paragraphe 1 : Le rejet du régime de la propriété mobilière

379. Bien qu'elle présente indéniablement une valeur économique, la nature extrapatrimoniale de la chose anthropomorphique dresse un obstacle à son appropriation (**A**).

¹¹⁸⁰ MALLET-POUJOL (N.), *Appropriation de l'information : l'éternelle chimère*, op. cit., p. 332.

¹¹⁸¹ BINCTIN (N.), *Retour sur un cadre juridique complexe et en pleine évolution*, In Rapport du Think-tank Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018, p. 47.

¹¹⁸² Expression empruntée à DESTREGUIL (M.), *Plaidoyer en faveur d'une approche propriétaire des données personnelles*, Revue Juridique Personnes et Famille, 2019, n°03, p. 05.

¹¹⁸³ BINCTIN (N.), op. cit., p. 50.

¹¹⁸⁴ Cf. Paragraphes 349 à 377.

¹¹⁸⁵ WATRIN (L.), *Les données scientifiques saisies par le droit*, Thèse de Doctorat, Droit, Université Aix-Marseille, Institut Francophone pour la Justice et la Démocratie, 2019, p. 318 s.

Ainsi, aucun possesseur de la donnée médicale personnelle ou anonyme ne pourrait jamais disposer d'un *abusus* à son égard ni en devenir le propriétaire (B).

A) *L'impossible appropriation de la donnée médicale*

380. Eu égard à sa nature extrapatrimoniale, la chose anthropomorphique ne peut jamais être l'objet d'un droit de propriété mobilière. Telle que conçue dans cette étude, la donnée médicale personnelle est une chose attachée aux droits de la personnalité alors que la donnée médicale anonyme appartient aux choses communes. En revanche, si les choses anthropomorphiques personnelles et anonymes ne bénéficiaient pas d'un statut et d'un régime *ad hoc*, elles seraient, par défaut, qualifiées de *bien*. Le cas échéant, elles pourraient être appréhendées pour intégrer le patrimoine de l'individu ayant revendiqué un droit privatif sur leur incorporalité. Ce dernier pourrait notamment en jouir et en disposer de la manière la plus absolue qui soit¹¹⁸⁶. Compte tenu de l'émergence des biens informationnels et des plaidoyers en faveur d'un droit de propriété sur les données à caractère personnel, il apparaît opportun de protéger la sacralité inhérente aux choses anthropomorphiques contre toute réservation privative. Par son action, le législateur devrait donc exclure les données médicales personnelles et anonymes de la catégorie des biens.

381. Objectivement, la donnée médicale personnelle ou anonyme correspond à un élément immatériel du corps humain du patient. Cette information, formalisée sur un support littéral ou numérique, devient alors concrètement palpable. Du fait de l'homme ou de l'informatique, elle existe de façon immatérielle. Il s'ensuit que la donnée médicale, personnelle ou anonyme, est qualifiable de chose. Si la donnée médicale est une chose, toutes les choses ne sont pas nécessairement des biens. Certainement, la chose entre dans la catégorie des biens lorsqu'elle s'avère utile pour l'homme et qu'il peut se l'approprier. Autrement dit, les biens doivent être envisagés comme toutes les richesses utiles à l'homme pour satisfaire ses besoins et ses désirs à compter de leur appropriation privative¹¹⁸⁷. Une fois réservés, les biens constituent le patrimoine d'une seule et même personne physique ou morale qui en est le sujet actif et

¹¹⁸⁶ Article 544 du code civil.

¹¹⁸⁷ REBOUL-MAUPIN (N.), *Droit des biens*, Dalloz, 8^e ed., septembre 2020, p. 10.

passif¹¹⁸⁸. Les biens comportent donc une valeur d'usage et d'échange qui peut être positive ou négative¹¹⁸⁹.

Fondamentalement, la donnée médicale personnelle ou anonyme présente de nombreux intérêts tant pour le patient que pour les tiers exploitants. Si elle porte en elle une certaine valeur économique, l'exploitation de la donnée médicale permet également de générer du profit au bénéfice des organismes des secteurs médicaux, industriels ou des nouvelles technologies. Comme en témoigne les cyberattaques dirigées contre les systèmes d'information hospitaliers¹¹⁹⁰, la donnée médicale est particulièrement convoitée et suscite une volonté d'appropriation chez tout individu dont l'exploitation présenterait des avantages. La chose anthropomorphique est également utile au patient puisqu'elle lui permet notamment d'accéder à des prestations de services en santé. Il en ressort que l'utilité et la valeur économique de la donnée médicale sont indéniables. En effet, la CNCDH reconnaît que « *les données personnelles jouent un rôle de plus en plus important dans l'économie numérique actuelle, et sont même au fondement d'un nouveau modèle économique* »¹¹⁹¹. Toutefois, il apparaît que ces critères d'utilité et de valeur ne suffisent pas à qualifier la chose de bien. Par surcroît, celle-ci doit pouvoir être appropriée.

382. Rémy Libchaber indique que l'appropriabilité du bien peut être définie « *comme son aptitude à être soustrait à un usage collectif, au profit d'une dévolution individuelle* »¹¹⁹². En d'autres termes, l'appropriation résulte d'une relation d'appartenance exclusive entre une chose et un individu qui s'en réserve l'utilité par l'exclusion de l'ensemble des tiers. L'appropriabilité procéderait tant de la saisissabilité de la chose que de son exclusivité. C'est pourquoi Frédéric Zénati admet que « *la meilleure protection de l'exclusivité est assurément la main mise sur la chose* »¹¹⁹³. Alors que la donnée a toujours été observée comme un élément tangible, il n'empêche qu'elle consiste en la formalisation d'une information dont

¹¹⁸⁸ Voir : La théorie classique du patrimoine selon Charles Aubry et Charles Rau ; REBOUL-MAUPIN (N.), *op. cit.* p. 28.

¹¹⁸⁹ Voir : LIBCHABER (R.), *op. cit.*, § 17.

¹¹⁹⁰ LIBCHABER (R.), *op. cit.*, § 31.

¹¹⁹¹ CNCDH, Avis du 22 mai 2018, *loc. cit.*

¹¹⁹² LIBCHABER (R.), *op. cit.*, § 31.

¹¹⁹³ ZENATI (F.), *Pour une rénovation de la théorie de la propriété*, Revue trimestrielle de droit civil, Dalloz, 1993, n°02, p. 306.

l'appropriation juridique pose des difficultés matérielles. La chose incorporelle doit donc être distinguée de son support.

Traditionnellement, le critère d'appropriabilité présupposait la matérialité de la chose. En effet, étaient qualifiées de biens les choses qui pouvaient être physiquement accaparées. De cette façon, seules les choses corporelles pouvaient intégrer la catégorie des biens. L'appropriabilité de la chose garantissait sa possession, à savoir sa détention ou sa jouissance. Afin de permettre cette possession au profit du propriétaire, du possesseur ou détenteur du bien, il fallait, au préalable, s'assurer de sa préhension physique. Il en ressort que le critère de l'appropriabilité de la chose résultait de sa potentialité à faire l'objet d'une possession, laquelle consistait en l'emprise matérielle d'une chose corporelle. Cependant, le critère de l'appropriabilité matérielle de la chose n'apparaît plus adapté à l'évolution des objets. Le monde, l'économie et les patrimoines sont dorénavant composés de choses incorporelles. En 1993, Frédéric Zénati considérait déjà que « *seule une mentalité archaïque impose d'écarter l'idée que l'appropriation puisse être assurée d'une autre manière* »¹¹⁹⁴. C'est ainsi que plusieurs auteurs ont écarté le critère de l'appropriabilité de la chose au profit de son unique valeur. Autrement dit, il est désormais admis que la valeur de la chose suffit à la qualifier de bien.

383. C'est ainsi que William Dross a constaté que « *la question de l'extension de la notion de bien à l'intérêt économique paraît se livrer sans détour* »¹¹⁹⁵. De la même façon, Enagnon Gildas Nonnou a remarqué que « *la valeur économique se substitue progressivement à la matérialité comme élément déterminant permettant d'établir qu'une chose constitue un bien et a une vocation patrimoniale* »¹¹⁹⁶. Plus précisément, c'est à l'occasion de ses travaux de thèse portant sur la possession des meubles incorporels qu'Anne Pelissier a affirmé que la chose incorporelle se métamorphose en bien dès lors qu'elle correspond à une valeur pour laquelle est exprimée une volonté de réservation et de commercialisation¹¹⁹⁷. En tant que source de valeur, l'information, personnelle ou anonyme, correspond à un bien meuble

¹¹⁹⁴ *Ibid.*

¹¹⁹⁵ DROSS (W.), *L'extension de la notion de bien à l'intérêt économique substantiel*, In LEVENEUR (L.), *Les nouveaux biens*, Dalloz, janvier 2020, p. 15.

¹¹⁹⁶ NONNOU (E. G.), *La patrimonialité des données personnelles*, La revue Lexbase Afrique-OHADA, 2020, n°38.

¹¹⁹⁷ PELISSIER (A.), *Possession et meubles incorporels*, Dalloz, janvier 2001, p. 111.

incorporel dès lors que « *son titulaire manifeste un souci de réservation et de commercialisation* »¹¹⁹⁸. Le cas échant, l'auteur spécifie que « *ce bien [l'information] est distinct de son support, c'est un bien autonome qui revêt donc un caractère immatériel* »¹¹⁹⁹. Toutefois, la réservation de la valeur du bien incorporel « *ne peut s'accomplir que si la valeur n'est pas exclue du commerce juridique au sens de l'[ancien] article 1128 du code civil* »¹²⁰⁰. Alors que la valeur de la chose incorporelle justifie son intégration dans la catégorie des biens, le législateur peut l'exclure du commerce juridique pour en assurer la protection.

Les choses anthropomorphiques personnelles correspondent à un certain type de chose « *dont la fonction sociale pose leur rapport à la personne autrement que dans une relation d'appartenance* »¹²⁰¹. C'est pourquoi elles requièrent « *une attention particulière, qui ne peut leur être portée qu'en les sortant de la compétition des biens* »¹²⁰². Finalement, la réalité économique comme la valeur patrimoniale d'une chose ne suffisent pas à la faire entrer dans le commerce juridique ou dans le marché¹²⁰³. Si un régime spécifique à la chose anthropomorphique était concédé à la donnée médicale personnelle, celle-ci serait partiellement exclue du commerce juridique, en dépit de sa valeur, par l'effet d'une règle de droit¹²⁰⁴. Subséquemment, elle ne pourrait être ni qualifiée de bien meuble incorporel, ni appropriée. Certainement, on ne peut acquérir les biens exclus du commerce juridique¹²⁰⁵. S'agissant de la donnée médicale anonyme, son inscription parmi les choses communes ôterait, *de jure*, son appropriabilité. Partant, aucune chose anthropomorphique ne pourrait pénétrer aucun patrimoine mobilier.

384. Cependant, le droit positif n'accorde, pour le moment, aucun statut particulier aux données médicales personnelles et anonymes. Etant encore qualifiables de biens meubles incorporels en raison de leur valeur, elles semblent susceptibles d'être l'objet d'un droit privatif. Ainsi, est-il possible qu'en acquérir la propriété ?

¹¹⁹⁸ PELISSIER (A.), *op. cit.*, p. 138.

¹¹⁹⁹ *Ibid.*

¹²⁰⁰ PELISSIER (A.), *op. cit.*, p. 111.

¹²⁰¹ LOISEAU (G.), *Pour un droit des choses, op. cit.*, p. 3015.

¹²⁰² *Ibid.*

¹²⁰³ Voir : LOISEAU (G.), *Typologie des choses hors du commerce, loc. cit.*

¹²⁰⁴ Cf. Paragraphe 369.

¹²⁰⁵ Article 2260 du code civil.

B) L'altération des attributs de la propriété

385. L'appropriation d'un bien meuble incorporel interviendrait par la réservation de sa valeur au profit de l'individu qui le désire. Dorénavant, la réservation des biens incorporels ne s'exprime plus à travers une possession matérielle et exclusive de l'objet, mais au moyen d'un pouvoir de fait exercé sur celui-ci. La possession repose sur la réunion de deux éléments : le *corpus* et *l'animus*. Lorsque le bien meuble est corporel, la possession revient à l'individu qui s'en est matériellement emparé avec l'intention de le réserver privativement. En revanche, lorsque le bien meuble est incorporel, le *corpus* possessoire se manifeste par un pouvoir de fait sur celui-ci. La notion de *pouvoir de fait*, dégagée par Anne Pelissier, consiste en une dimension intellectuelle de la possession par laquelle l'individu marque son pouvoir sur la chose¹²⁰⁶. L'auteur explique que le pouvoir de fait naît d'un rapport économique particulier entre le possesseur et la chose. Ce rapport se manifeste par l'utilisation de la chose, laquelle varie selon sa nature et sa destination¹²⁰⁷. Quand la valeur du bien meuble incorporel est dépendante de son exploitation, « *l'exercice du pouvoir de fait se manifeste, de façon dynamique, par cette exploitation. Le possesseur montre son intérêt pour le bien en assurant sa valorisation économique puisque l'exploitation de la chose permet d'accroître sa valeur* »¹²⁰⁸. Lorsque le bien meuble incorporel dispose d'une valeur intrinsèque, le pouvoir de fait se manifeste simplement par l'utilisation de la chose conformément à sa destination¹²⁰⁹. En d'autres termes, le pouvoir de fait se concrétise par l'accomplissement d'actes matériels ou juridiques dont l'objet est le bien meuble incorporel.

Pour asseoir ce pouvoir de fait, l'exécution de ces actes doit être perçue par les tiers. En effet, « *ce sera l'interprétation de ces signes par les tiers qui conduira à la conscience sociale du pouvoir de fait et, par là même, à la possession* »¹²¹⁰. En somme, « *le pouvoir de fait doit alors se définir comme un rapport de puissance conscient sur une chose dont*

¹²⁰⁶ PELISSIER (A.), *op. cit.*, p. 83.

¹²⁰⁷ PELISSIER (A.), *op. cit.*, p. 101.

¹²⁰⁸ PELISSIER (A.), *op. cit.*, p. 102.

¹²⁰⁹ *Ibid.*

¹²¹⁰ PELISSIER (A.), *op. cit.*, p. 104.

l'existence se traduit naturellement par sa conscience chez les tiers »¹²¹¹. L'acquisition de la propriété des biens meubles pouvant intervenir par le biais de leur possession, « *le pouvoir de fait [...] se présentera alors comme une notion essentielle à la réservation de ces biens pour lesquels un droit privatif n'a pas été organisé* »¹²¹². Partant, l'identification du possesseur de la donnée médicale permettra d'en déterminer le propriétaire éventuel.

386. La notion du pouvoir de fait a inspiré les défenseurs d'un droit de propriété sur les données personnelles. Nicolas Binctin soutient qu'un « *recours au droit commun des biens est possible pour l'appropriation des biens intellectuels et, plus généralement, pour les données, dont les données personnelles* »¹²¹³ à condition d'exercer sur ces derniers une emprise possessoire. Ainsi, l'appropriation de l'information se ferait à travers sa possession intellectuelle. En ce sens, Anne Pelissier estime que « *le recours au pouvoir de fait de la possession permet en effet de désigner le titulaire de l'information et l'autorise à accéder aux mécanismes généraux de protection de son bien* »¹²¹⁴. Eu égard à ces prétentions, il convient d'identifier qui pourrait être le propriétaire des données médicales personnelles du patient dans l'hypothèse où elles constitueraient potentiellement un bien meuble incorporel. Il s'agit donc de distinguer qui exerce un pouvoir de fait sur la donnée médicale avec l'intention de la posséder.

387. Selon Nicolas Binctin, l'emprise possessoire de la donnée à caractère personnel est conférée soit par la maîtrise du secret par lequel elle est protégée, soit par le contrôle de son accès aux tiers. L'auteur considère que « *le secret comme le contrôle permettent la détention comme la possession* »¹²¹⁵ et prouvent l'existence du *corpus*, à savoir, un pouvoir de fait exercé sur la donnée personnelle. Suivant son raisonnement, le contrôle du secret et de l'accès de la donnée personnelle appartiendraient à son émetteur initial. On peut en inférer que la personne concernée bénéficierait d'une emprise possessoire sur les données personnelles qui la concernent. En ce sens, Rémy Libchaber suppose que si nous devons admettre que les attributs de la personne étaient des biens, ils seraient originellement appropriés par « *celui*

¹²¹¹ PELISSIER (A.), *op. cit.*, p. 100.

¹²¹² PELISSIER (A.), *op. cit.*, p. 131.

¹²¹³ BINCTIN (N.), *op. cit.*, p. 57.

¹²¹⁴ PELISSIER (A.), *op. cit.*, p. 138.

¹²¹⁵ BINCTIN (N.), *op. cit.*, p. 59.

qui les tire de lui-même »¹²¹⁶. Le « *secret, le contrôle, ou l'intimité* », qui sont censés permettre une emprise possessoire sur les données personnelles, procèdent directement des droits de la personnalité de la personne concernée. Effectivement, c'est en vertu du droit à la protection des données personnelles et du droit au respect de l'intimité de la vie privée qu'elle jouit de la maîtrise de ses données personnelles. L'ensemble de ces prérogatives n'est donc pas affecté à la chose mais attaché à la personne. En conséquence, l'emprise possessoire de la donnée personnelle ne résulte pas d'une situation de fait à laquelle le droit accorde des effets. Assurément, le pouvoir du patient sur ses données médicales personnelles constitue davantage un pouvoir juridique exercé au moyen de droits subjectifs qu'un pouvoir factuel.

388. Plus spécifiquement, la donnée médicale est produite par le professionnel qui la porte à la connaissance du patient, à moins qu'il n'ait exprimé la volonté d'être tenu dans l'ignorance¹²¹⁷. L'émetteur initial de la donnée médicale personnelle ne serait donc pas le patient mais le professionnel ayant procédé à la consultation ou à l'examen médical¹²¹⁸. Toutefois, le professionnel de santé, producteur ou collecteur de la donnée médicale personnelle du patient, n'en maîtrise ni le secret, ni les accès. Certainement, seul le patient est titulaire du secret médical dont les professionnels de santé sont dépositaires¹²¹⁹. D'une part, seul le patient peut légalement divulguer ses informations médicales. D'autre part, seul le patient peut maîtriser la circulation de sa donnée médicale entre les professionnels concourant à sa prise en charge sanitaire¹²²⁰. En effet, il peut s'opposer à son échange ou refuser son partage en en assumant les conséquences dommageables¹²²¹. De surcroît, le patient a le droit de s'opposer à ce que ses données personnelles fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé¹²²². Il est évident que le professionnel ayant produit ou collecté la donnée médicale personnelle du patient n'exerce aucun pouvoir sur celle-ci. En effet, les professionnels peuvent uniquement en faire usage conformément aux normes

¹²¹⁶ LIBCHABER (R.), *op. cit.*, § 63.

¹²¹⁷ Article L.1111-2 du code de la santé publique.

¹²¹⁸ Cf. Paragraphes 50 à 53.

¹²¹⁹ Cf. Paragraphe 193.

¹²²⁰ Cf. Paragraphes 274 s.

¹²²¹ Cf. Paragraphes 278, 284 et 285.

¹²²² Article 74 de la loi Informatique et Libertés.

juridiques relatives à la protection des données personnelles et aux dispositions du code de la santé publique.

Bien que Nicolas Binctin considère que « *la donnée peut être contrôlée par celui qui la collecte* »¹²²³, ce contrôle est restreint à la détermination de la finalité et des moyens du traitement. Moins qu'un pouvoir de fait ou qu'un pouvoir juridique, les professionnels participant à la prise en charge sanitaire du patient disposent exclusivement d'une autorisation juridique de traitement de ses données médicales personnelles dont les usages sont contrôlés par ce dernier¹²²⁴. Ne possédant ni la maîtrise du secret, ni le contrôle des accès, lesquels ne peuvent appartenir qu'au patient, les tiers ne peuvent jamais exercer une quelconque emprise possessoire sur des données médicales à caractère personnel. De surcroît, Anne Pelissier explique que la présence d'un droit sur le bien incorporel absorbe le pouvoir de fait¹²²⁵. Or, le pouvoir exercé sur les données personnelles résulte des droits de la personnalité attachés à la personne concernée. Compte tenu de ce qui précède, le pouvoir juridique que le patient exerce sur ses données médicales personnelles peut-il avoir pour effet l'acquisition de leur propriété ?

389. En matière de meuble, la présomption acquisitive représente l'un des effets juridiques accordé au pouvoir de fait. L'article 2276 du code civil dispose qu'« *en fait de meubles, la possession vaut titre* ». En conséquence de ce mécanisme juridique, Nicolas Binctin affirme qu'« *en présence d'une chose incorporelle, la possession vaut titre de propriété. Cela permet d'affirmer que la possession d'une donnée grâce au secret, ou au contrôle, offre au possesseur la propriété de cette donnée, en application du droit commun des biens* »¹²²⁶. L'auteur conçoit alors que « *la donnée personnelle peut être vendue, ou louée comme tout bien pour lequel le propriétaire dispose d'un usus, d'un fructus et d'un abusus* »¹²²⁷. Cependant, nous analysons d'abord que le pouvoir juridique de la personne concernée sur ses données personnelles provient de l'exercice de ses droits de la personnalité. Ainsi, la donnée médicale personnelle est soumise au régime des droits extrapatrimoniaux. La maîtrise

¹²²³ BINCTIN (N.), *op. cit.*, p. 49

¹²²⁴ Article 1 de la loi Informatique et Libertés.

¹²²⁵ PELISSIER (A.), *op. cit.*, p.117.

¹²²⁶ BINCTIN (N.), *op. cit.*, p. 59.

¹²²⁷ BINCTIN (N.), *op. cit.*, p. 61.

de la donnée personnelle par la personne concernée ne peut donc jamais emporter son appropriation¹²²⁸. Il en ressort que la donnée médicale personnelle ne peut être qualifiée de bien en raison de son inappropriabilité.

390. En raison de cette extrapatrimonialité, nous déduisons ensuite que la personne concernée ne peut disposer d'un *abusus* sur sa donnée médicale personnelle. En effet, l'*abusus* est défini comme le droit, pour le propriétaire, de disposer de son bien¹²²⁹. Plus précisément, l'article 544 du code civil dispose que « *la propriété est le droit de jouir et disposer des choses de la manière la plus absolue* ». L'*abusus* est ainsi observé comme l'attribut essentiel du droit de la propriété. Le propriétaire d'un bien doit alors pouvoir en disposer juridiquement en les aliénant ou en disposer matériellement en les détruisant. Les actes de disposition impactent donc la composition du patrimoine de l'individu : ils ne peuvent alors porter que sur des biens ou sur des droits patrimoniaux. Seulement, la donnée médicale personnelle, en tant que chose anthropomorphique, ne peut entrer dans le patrimoine de la personne concernée ni, conséquemment, faire l'objet d'un acte de disposition¹²³⁰. C'est ainsi que Danièle Bourcier et Primavera De Filippi concluent que les sujets de droit ne peuvent être « *propriétaires de ces données car ils ne peuvent pas en disposer librement* »¹²³¹. Effectivement, le droit de propriété est composée de trois prérogatives que sont les droits d'user (*usus*), de jouir (*fructus*) et de disposer (*abusus*)¹²³² du bien. En principe, le propriétaire est la personne physique ou morale qui bénéficie de ces trois attributs de la propriété. Exceptionnellement, « *dépouillé de toute autre prérogative [...] le propriétaire demeure encore tel s'il lui reste le droit de disposer* »¹²³³. Il en ressort que l'altération de l'*abusus* réduit à néant le droit de propriété brigué par la personne concernée. Autrement dit, l'altération des attributs de la propriété fait obstacle à un droit de propriété au profit de la personne concernée. Si le pouvoir juridique du patient sur ses données médicales personnelles pouvait être assimilé à un *corpus* possessoire, cette possession intellectuelle ne pourrait donc emporter l'acquisition de leur propriété.

¹²²⁸ Cf. Paragraphe 387.

¹²²⁹ GUINCHARD (S.), DEBARD (T.), *op. cit.*, p. 6.

¹²³⁰ Cf. Paragraphes 362 et 380.

¹²³¹ BOURCIER (D.), DE FILIPPI (P.), *op. cit.*, p. 448.

¹²³² TERRE (F.), SIMLER (P.), *Droit civil. Les biens*, Dalloz, 10^e ed., septembre 2018, p. 132.

¹²³³ SÉRIAUX (A.), *Propriété*, Répertoire de droit civil, juin 2016, § 84.

391. En tout état de cause, la réservation de la propriété de la donnée médicale personnelle par le patient n'apparaît pas nécessaire dans la mesure où elle lui est juridiquement affectée. En effet, le rapport de droit de l'individu sur son information ne résulte pas d'un droit de propriété mais des prérogatives inhérentes aux droits de la personnalité. De cette façon, autrui ne pourra jamais obtenir, par quelque mécanisme que ce soit, la pleine maîtrise des données personnelles de la personne concernée. Certainement, cette maîtrise lui est conférée par des droits extrapatrimoniaux, incessibles et imprescriptibles. Assurément, les droits que la personne concernée détient sur ses données personnelles sont attachées à sa personne jusqu'à sa mort, à moins qu'elle n'ait défini des directives relatives à leur sort après son décès¹²³⁴. La donnée médicale à caractère personnel ne peut donc être appropriée originairement ni par la personne concernée, ni par les tiers. Ainsi, la donnée médicale personnelle ne peut devenir un objet marchand. En revanche, qu'en est-il de l'appropriation des données médicales anonymes ?

392. Eu égard au droit positif en vigueur, les données médicales anonymisées produites par des professionnels de santé exerçant dans le secteur privé sont qualifiables de biens. En effet, les données anonymisées présentent une utilité dans la mesure où leur exploitation conduit à leur valorisation économique¹²³⁵. Ainsi, la donnée médicale anonymisée, en tant que bien meuble incorporel, devient un bien incorporant le patrimoine de l'individu ayant exprimé la volonté d'en réserver la valeur et d'en devenir le propriétaire. Toutefois, la particularité des données médicales anonymisées réside dans la désaffectation d'une chose initialement soumise au régime des droits de la personnalité de la personne concernée. Le responsable de traitement qui procède à l'anonymisation de la donnée médicale personnelle crée une nouvelle chose devenue appropriable. Le cas échéant, à qui appartient la donnée médicale anonymisée ?

Si la donnée médicale personnelle était un bien meuble incorporel approprié par la personne concernée, la donnée médicale anonymisée constituerait un bien nouveau issu d'un bien préexistant. Il existerait alors un conflit de propriété entre la personne concernée propriétaire de sa donnée médicale personnelle et le créateur de la nouvelle donnée

¹²³⁴ Article 85 de la loi Informatique et Libertés.

¹²³⁵ Cf. Paragraphes 377 et 432.

anonymisée. Toutefois, il apparaît que la donnée médicale personnelle ne peut être appropriée. Il s'ensuit que la personne concernée ne peut revendiquer aucun droit de propriété sur la donnée médicale anonymisée. Assurément, la chose anthropomorphique personnelle étant dépourvue de propriété initiale, il s'ensuit que la donnée médicale anonymisée est une chose n'ayant encore jamais été appropriée. Par conséquent, le seul mode d'appropriation envisageable tient dans son occupation.

En tant que « *mode originaire d'acquisition, l'occupation est un moyen d'acquérir une chose en en prenant volontairement possession, c'est-à-dire avec l'intention d'en devenir effectivement le propriétaire* »¹²³⁶. Simplement, l'occupation « *se prouve par le seul fait d'appréhender une chose sans maître en la faisant sienne* »¹²³⁷. Ainsi, la donnée médicale anonymisée serait originairement acquise par la première personne physique ou morale l'ayant occupée. Par défaut, le traitement ayant pour finalité l'anonymisation de la donnée médicale personnelle traduit la volonté de créer un nouveau bien meuble incorporel afin de l'exploiter. La réservation de cette valeur suffit à caractériser l'*animus* et à considérer le responsable de traitement comme le propriétaire initial de la donnée médicale anonymisée. En ce sens, Elise Daragon relève que « *l'information est, en principe, appropriée dès son origine ; (...) elle appartient toujours (...) à son auteur, c'est-à-dire à celui qui la met en forme* »¹²³⁸.

393. Toutefois, l'appropriabilité de la donnée médicale anonymisée engendre des risques de patrimonialisation de la personne humaine¹²³⁹. La réservation de la chose anthropomorphique anonymisée apparaît alors tout aussi contestable que l'appropriation des données médicales personnelles¹²⁴⁰. L'enjeu de la préservation de la dignité humaine commande alors d'exclure la donnée médicale anonymisée de la catégorie des biens. Ainsi que nous l'envisageons, la consécration d'un statut spécifique à la chose anthropomorphique anonyme permettrait d'élaborer un nouveau commun numérique soumis au régime des

¹²³⁶ TERRE (F.), SIMLER (P.), *op. cit.*, p. 320.

¹²³⁷ LIBCHABER (R.), *op. cit.*, § 42.

¹²³⁸ DARAGON (E.), *Etude sur le statut juridique de l'information*, Recueil Dalloz, 1998, n°07, p. 66.

¹²³⁹ Cf. Paragraphe 372.

¹²⁴⁰ Cf. Paragraphe 355.

choses communes¹²⁴¹. Comme l'affirme Rose-Noëlle Schütz, « *les choses communes ne peuvent faire l'objet, ni d'une propriété individuelle, ni d'une propriété collective : rebelles à toute appropriation, elles ne sont pas des biens* »¹²⁴². A cet instant, la création d'une nouvelle donnée médicale anonyme et son occupation ne généreraient pas un nouveau bien appropriable. En effet, « *bien que la possession ne soit pas liée à l'existence d'un droit, il faut néanmoins que la chose, objet de la possession, puisse être l'objet du droit* »¹²⁴³. Or, en tant que commun numérique, la chose anthropomorphique anonyme ne pourrait être affectée à un maître qui puisse en disposer privativement : la chose anthropomorphique anonyme ne peut être l'objet du droit de propriété.

394. Compte tenu du développement du numérique, de l'incorporalité et du commerce des données, il apparaît indispensable d'accorder un statut et un régime spécifiques à la chose anthropomorphique, d'abord lorsqu'elle est à caractère personnel, puis lorsqu'elle est anonyme. De cette façon, la chose anthropomorphique ne pourrait jamais être l'objet d'un droit de propriété mobilière. Néanmoins, cet élément immatériel du corps humain peut-il devenir l'objet d'un droit de propriété intellectuelle ?

Paragraphe 2 : Le rejet du régime du droit de la propriété intellectuelle

395. La donnée médicale personnelle ou anonyme réifie le corps humain du patient et révèle sa condition physiologique. Cette retranscription technique et médicale, fidèle à l'état du vivant, ne correspond pas à la définition des œuvres de l'esprit créatives et originales (**A**). De surcroît, si la donnée médicale était une œuvre de l'esprit originale, le patient ne saurait en être l'auteur. En effet, même si la donnée médicale provient du corps humain du patient, celle-ci est créée et formalisée par le professionnel de santé (**B**).

¹²⁴¹ Cf. Paragraphes 373 s.

¹²⁴² SCHÜTZ (R.-N.), *Inaliénabilité*, Répertoire de droit civil, juin 2014, § 53.

¹²⁴³ TERRE (F.), SIMLER (P.), *op. cit.*, p. 159.

A) L'absence de création originale protégeable

396. A la fois soucieux de la protection des droits de la personnalité de la personne concernée et favorable au développement de l'économie numérique, un courant doctrinal propose de soumettre les données personnelles au droit spécial de la propriété intellectuelle, et plus particulièrement au droit d'auteur. *A priori*, l'application de ce régime paraît conciliable avec la nature spécifique de la chose anthropomorphique. D'une part, la réservation de l'économie des créations immatérielles s'appréhende au moyen de la propriété intellectuelle¹²⁴⁴. La donnée médicale immatérielle, objet d'une propriété intellectuelle, deviendrait alors un droit incorporel attaché à son titulaire. Certainement, le droit d'auteur offre à son titulaire une maîtrise et une exclusivité sur l'objet immatériel. D'autre part, la dualité du droit d'auteur présente tant une facette extrapatrimoniale qu'une facette patrimoniale¹²⁴⁵. L'appropriation de la donnée médicale par le droit d'auteur permettrait alors de protéger les intérêts moraux de son créateur et de satisfaire ses intérêts patrimoniaux à travers son exploitation. En effet, le droit d'auteur « *se décompose en certains droits incessibles (les droits moraux, qui donnent notamment à l'auteur un contrôle inaliénable sur la diffusion et sur la modification de son œuvre) et en droits cessibles (les droits patrimoniaux, et notamment le droit d'exploitation). Ces caractéristiques en font-elles la solution idéale pour les données personnelles ?* »¹²⁴⁶.

En dépit de ces attraits, il convient d'abord de pallier la confusion entretenue par certains auteurs entre le droit et son objet¹²⁴⁷. D'aucuns « *affirment que, parce qu'ils sont immatériels, les meubles incorporels ne peuvent consister qu'en des droits* »¹²⁴⁸. Pourtant, le droit doit avoir pour objet une chose, fût-elle immatérielle. Spécifiquement, les droits de propriété intellectuelle ont pour objet une création ; et l'objet de cette création, dans le droit d'auteur, porte sur une œuvre de l'esprit¹²⁴⁹. Il en ressort que la donnée médicale ne peut

¹²⁴⁴ VIVANT (M.), BRUGUIERE (J.-M.), *Droit d'auteur et droits voisins*, Dalloz, 4^e ed., janvier 2019, p. 8.

¹²⁴⁵ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 57.

¹²⁴⁶ MATTATIA (F.), YAÏCHE (M.), *Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I)*, Revue Lamy Droit de l'immatériel, 2015, n°114, p. 62.

¹²⁴⁷ Voir : PELISSIER (A.), *op. cit.*, p.112.

¹²⁴⁸ *Ibid.*

¹²⁴⁹ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 150.

devenir l'objet du droit d'auteur qu'à la condition d'être une œuvre de l'esprit. Il n'en demeure que toute œuvre de l'esprit n'est pas protégeable par le droit d'auteur. Effectivement, encore faut-il qu'elle présente un caractère original¹²⁵⁰. Dans l'affirmative, en tant qu'œuvre de l'esprit originale, la donnée médicale serait automatiquement appréhendée par son auteur du seul fait de sa création¹²⁵¹. Seulement, la donnée médicale a la particularité d'être générée par le professionnel de santé à l'occasion de la prise en charge sanitaire du patient. Dès lors, qui du patient ou du professionnel de santé s'en trouverait titulaire ? L'opportunité de l'application du régime du droit d'auteur à la donnée médicale réside dans l'inaliénabilité des attributs intellectuels et moraux intimement attachés au créateur d'une œuvre émanant de son esprit. Seulement, l'application du régime du droit d'auteur à la donnée médicale ne présenterait un intérêt que si l'auteur était le patient. Dans cette unique hypothèse, le droit d'auteur « *permet la prise en compte d'une dimension morale, d'un lien intime entre le patient et sa donnée tout en permettant d'assurer une exploitation économique de celle-ci* »¹²⁵². A défaut, il s'agirait d'abandonner l'invocation de ce régime.

397. En premier lieu, il convient de déterminer si la donnée médicale peut être qualifiée d'œuvre de l'esprit. Alors que cette qualification est un préalable indispensable à l'application du régime du droit d'auteur, le législateur n'a pas pris le soin d'en définir la notion. Celui-ci se borne à protéger « *les droits des auteurs sur toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination* »¹²⁵³. En l'absence de définition légale, cette acception a été spécifiée par la doctrine. C'est ainsi que Michel Vivant et Jean-Michel Bruguière ont largement circonscrit l'œuvre de l'esprit à tout travail créatif résultant de l'intervention de l'homme et passant par la réalisation d'une forme¹²⁵⁴. Trois conditions cumulatives doivent donc être réunies pour qu'une œuvre advienne.

398. D'abord, le travail effectué doit être créatif, il doit en résulter une création. Le centre national de ressources textuelles et lexicales définit la création comme le « *résultat de*

¹²⁵⁰ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 277.

¹²⁵¹ Article L.111-1 al. 1 du code de la propriété intellectuelle.

¹²⁵² CAVALIER (M.), *op. cit.*, p. 375.

¹²⁵³ Article L.121-1 du code de la propriété intellectuelle.

¹²⁵⁴ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 158.

l'exercice du pouvoir qu'a l'homme de construire, de former, avec le concours d'une faculté spécifiée, un produit qui s'insère parmi les choses déjà existantes »¹²⁵⁵. En d'autres termes, la création consiste en la capacité, pour une personne physique, d'imaginer et de concevoir quelque chose de nouveau. En somme, la création présuppose la créativité de l'individu. C'est pourquoi la jurisprudence considère que la retranscription de la réalité ne correspond pas à un travail créatif¹²⁵⁶. Partant, la révélation de découvertes par la mise à jour de l'existant ne peut être perçue comme une création. En effet, « *celui qui se contente de révéler une réalité préexistante [...] ne peut prétendre à un droit d'auteur* »¹²⁵⁷. De la même manière, l'exécution d'un savoir-faire technique ne peut donner prise au droit d'auteur¹²⁵⁸. En effet, le travail créatif ne doit être confondu ni avec une compétence professionnelle, ni avec une prestation de services techniques¹²⁵⁹.

Compte tenu de ces précisions, la donnée médicale ne répond pas aux critères de création de l'œuvre. D'une part, la donnée médicale est produite par le professionnel de santé dans le cadre d'une relation sanitaire. Cette production d'informations médicales requiert une compétence technique indispensable et inhérente à la prise en charge sanitaire du patient. Assurément, tout acte de prévention, de diagnostic ou de soins est dispensé à l'appui de ces informations à la fois personnelles et objectives. D'autre part, la donnée médicale doit exactement retranscrire l'état de santé du patient, son exacte condition physiologique¹²⁶⁰. La chose anthropomorphique est alors observée comme un élément immatériel du corps humain du patient. La donnée médicale, qu'elle soit personnelle ou anonyme, consiste en la réification d'une réalité existante au moyen de compétences médicales professionnelles. Elle

¹²⁵⁵ Lexicographie du mot « création » proposée par le CNRTL. Disponible en ligne sur le site [<https://www.cnrtl.fr>]. Consulté le 26 mai 2021.

¹²⁵⁶ CA, Paris, Pôle 5, ch. 1, 6 Juin 2012, n° 10/21371, JurisData n°2012-016964 : LEPI, 2012, n° 09, p. 02, note C. Bernault ; CCE, 2013, n° 06, chron. 6, B. Montels ; RLDI, 2012, n° 84, 2817 ; TGI, Paris, 4 juin 2010 : Légipresse, 2010, n° 274, p. 129 ; LPA, 2010, n° 196, p. 10, note E. Derieux ; TGI, Paris, 8 oct. 2010 : : Légipresse, 2010, n° 277, p. 333 ; Propr. intell., 2011, n° 38, p. 83, obs. A. Lucas ; CA, Paris, 4e ch., sect. A, 5 Décembre 2007, n° 06/15937, JurisData n°2007-350003 : D., 2008, n° 07, p. 461, J.-M. Bruguière ; CCE, 2008, comm. 17, Ch. Caron ; Légipresse 2008, n° 251, III, p. 83, A. Maffre-Baugé.

¹²⁵⁷ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 171.

¹²⁵⁸ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 172.

¹²⁵⁹ CA, Aix-en-Provence, 9 mars 2011, n° 2011/111, JurisData n° 2011-009638 : RLDI, 2011, n° 70, p. 27, obs. M. Trézéguet ; CA, Paris, 24 juin 2005, 4e ch., sect. B, n° 03/11140, JurisData n° 2005-279386 : CCE, 2005, comm. 131, note C. Caron ; Cass. soc., 13 nov. 2008, n° 06-45.99 : Semaine sociale Lamy, 2009, n° 1383, p. 6, obs. M. Blatman ; Propr. intell., 2009, n° 31, p. 158, obs. A. Lucas. ; Civ. 1^{ère}, 20 oct. 2011, n° 10-21.251 : LEPI, 2012, n° 03, obs. F. Herpe.

¹²⁶⁰ Cf. Paragraphe 15.

n'est aucunement le fruit d'un travail créatif. Bien au contraire, la production de la donnée médicale doit être indispensablement fiable et intègre, qualitative, standard et technique. La collecte et la production de la donnée médicale excluent donc toute créativité.

399. Ensuite, la création doit provenir de l'intervention humaine d'une personne physique¹²⁶¹. Bien que les données médicales soient majoritairement collectées et produites par le professionnel de santé lors de l'anamnèse et de l'examen clinique du patient¹²⁶², certaines informations sont directement générées par des dispositifs médicaux connectés et immédiatement intégrées dans les dossiers médicaux du patient¹²⁶³. Le déploiement de cabines de téléconsultation ou l'interopérabilité entre certaines applications mobiles en santé référencées dans l'Espace numérique de santé¹²⁶⁴ démontrent que la donnée médicale peut provenir de la machine. Autrement dit, la donnée médicale ne résulte pas nécessairement de l'intervention d'une personne physique jouissant de la personnalité juridique. Si la donnée médicale pouvait être qualifiée d'œuvre de l'esprit, il y aurait alors une distinction entre les informations médicales produites par le professionnel de santé et celles générées par la machine. Par exemple, la tension artérielle systolique et diastolique relevée manuellement par le professionnel de santé serait protégée par le régime du droit d'auteur alors que celle calculée par un tensiomètre électronique en serait exclue. Pourtant, il s'agirait d'informations strictement identiques comportant potentiellement la même valeur économique. Toutefois, leurs modalités de production suffiraient à engendrer une discrimination quant à leur réservation. Quel serait le sort des électrocardiogrammes, des électroencéphalogrammes, des clichés d'imagerie médicale et de toute autre donnée médicale produite par une machine ? Seraient-elles exclues du champ de ce droit de propriété intellectuelle ? Appartiendraient-elles à l'utilisateur de la machine ? Seraient-elles la propriété du patient se livrant à l'examen ? Tomberaient-elles dans le domaine public du fonds commun de la création ? Les auteurs qui affirment que « *la donnée peut être intégrée dans l'article L.111-1 du Code de propriété intellectuelle en considérant que c'est une œuvre de l'esprit* »¹²⁶⁵ ne tiennent

¹²⁶¹ Voir : BENSAMOUN (A.), *Ceci est... une œuvre d'art ! La question des créations générées par une intelligence artificielle*, L'Observatoire, 2020, n° 55, p. 104 à p. 106.

¹²⁶² Cf. Paragraphes 50 à 53.

¹²⁶³ *Ibid.*

¹²⁶⁴ Article L.1111-13-1 du code de la santé publique.

¹²⁶⁵ LANDREAU (I.), *Le RGPD, un pas dans la bonne direction ?*, In Rapport du Think-tank Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018, p. 89.

compte ni des limites, ni des conséquences liées à l'application d'un tel régime sur la donnée personnelle.

400. Finalement, « *l'intervention de l'homme qui caractérise la création doit se matérialiser dans une forme pour pouvoir être appréhendée par le droit d'auteur* »¹²⁶⁶. L'œuvre suppose une concrétisation minimale, peu importe qu'elle soit définitive. En effet, l'article L.111-2 du code de la propriété intellectuelle dispose que « *l'œuvre est réputée créée, indépendamment de toute divulgation publique, du seul fait de la réalisation, même inachevée, de la conception de l'auteur* ». C'est ainsi que l'œuvre doit seulement revêtir une forme perceptible par les sens, quel qu'en soit le genre ou l'expression¹²⁶⁷. L'information médicale personnelle ou anonyme consiste en une réalité préexistante qui prend véritablement forme dès l'instant où elle véhicule un message perceptible par autrui : une condition physiologique. Concrètement, la donnée médicale se matérialise dès l'instant où les conditions physiques, psychiques et biologiques intrinsèques au patient sont traduites et formulées dans un langage compréhensible. Par exemple, les battements du cœur, en tant que réalité biologique, deviennent une donnée médicale lorsqu'ils translatent une fréquence cardiaque. A partir de cette donnée médicale objective, le professionnel de santé pourra, par son interprétation, produire d'autres données médicales relatives au diagnostic clinique. En effet, la fréquence cardiaque peut révéler une bradycardie, une tachycardie ou des troubles du rythme cardiaque. La production des données médicales repose donc sur la traduction de leur interprétation. Tandis que la chose anthropomorphique se réalise systématiquement à travers une forme, il n'empêche que cet unique critère ne permet pas de la qualifier d'œuvre de l'esprit.

401. Dans l'hypothèse où la donnée médicale était qualifiable d'œuvre de l'esprit, sa protection par le droit d'auteur serait conditionnée par son originalité. Michel Vivant et Jean-Michel Bruguière perçoivent l'originalité comme la pierre angulaire de cette protection. Certainement, l'originalité est une condition permettant de reconnaître ou de refuser l'application du régime du droit d'auteur¹²⁶⁸. En d'autres termes, une œuvre n'est protégeable

¹²⁶⁶ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 176.

¹²⁶⁷ BERNAULT (C.), *Œuvres protégées. Règles générales (CPI, art. L. 112-1 et L. 112-2)*, JurisClasseur Civil, Fasc. 1135, Annexes V° Propriété littéraire et artistique, mars 2017, actu. mars 2021, § 11.

¹²⁶⁸ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 294.

que si elle apparaîtrait originale. La notion d'originalité a notamment été définie par la jurisprudence européenne comme le reflet de la personnalité de l'auteur à travers ses choix libres et créatifs¹²⁶⁹. Or, ni l'élément immatériel du corps humain du patient, ni le diagnostic médical ne portent l'empreinte du professionnel de santé collecteur ou producteur. D'une part, la chose anthropomorphique retranscrit strictement et fidèlement des faits existants. D'autre part, la médecine est une science qui s'appuie sur des données probantes. En effet, la médecine empirique est guidée par le principe épistémologique de l'« *evidence-based medicine* »¹²⁷⁰. Cette méthode, qui consiste à fonder les décisions médicales sur des données scientifiques probantes et hiérarchisées, a conduit à la standardisation et à la protocolisation de la pratique médicale. En ce sens, Élie Azria explique que « *l'EBM est rapidement devenue le nom générique d'un système aux atours de rationalité scientifique, producteur et prescripteur de normes médicales* »¹²⁷¹. Bien que la pratique clinique n'exclut pas l'intuition personnelle et subjective du professionnel de santé, le processus de la décision médicale implique l'application de résultats scientifiques pertinents et adaptés au cas particulier de chaque patient. Sauf à s'inscrire dans le charlatanisme, la production de données médicales et de diagnostics médicaux n'est pas libre de fantaisie et ne peut laisser place à l'arbitraire projetant la personnalité du professionnel de santé. Faute d'originalité, si la donnée médicale était une œuvre de l'esprit, elle n'emporterait aucun effet juridique.

B) La titularité des droits d'auteur

402. En admettant que la donnée médicale personnelle puisse véritablement devenir une œuvre de l'esprit originale, une seule question animerait tous les débats : qui en serait l'auteur ? Placé au cœur de l'économie de l'immatériel, « *le droit d'auteur, comme, au vrai, les autres propriétés intellectuelles, confère une valeur de marché à l'œuvre en érigeant une barrière propre à « sortir » ce bien de l'usage commun* »¹²⁷². En effet, l'article L.111-1 du code de la propriété intellectuelle annonce que « *l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et*

¹²⁶⁹ CJUE, 1er décembre 2011, aff. C-145/10, *Painer c/ Axel Springer AG* : CCE, 2012, comm. 26, C. Caron ; Prop. intell., 2012, n° 01, p. 30, obs. A. Lucas ; D., 2012, n° 07, p. 471, note N. Martial-Braz, infra, obs. J. Daleau ; RTD com., 2012, n° 01, p. 109, obs. F. Pollaud-Dulian.

¹²⁷⁰ En français, l'*evidence-based medicine* (EBM) signifie « médecine fondée sur des données probantes ».

¹²⁷¹ AZRIA (E.), *Le soignant et la standardisation des pratiques médicales*, Laennec, t. 61, 2013, n°3, p. 34.

¹²⁷² VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 13.

opposable à tous ». De ce fait, la personne physique qui crée une œuvre de l'esprit originale bénéficie de la réservation de ses utilités économiques et perçoit la rémunération consécutive à son exploitation. L'identification de l'auteur de la donnée médicale présenterait davantage un enjeu économique qu'un enjeu moral lié à la préservation et au contrôle de l'œuvre « originale ». Evidemment, « *le marché potentiel de la création est réservé à son auteur* »¹²⁷³.

403. Michel Vivant et Jean-Michel Bruguière constatent que « *l'auteur ne peut être rien d'autre que celui qui a créé l'œuvre* »¹²⁷⁴. En conséquence logique, « *les réels détenteurs de la propriété intellectuelle sur nos données sont ceux qui les créent* »¹²⁷⁵. En admettant que la donnée médicale soit qualifiable d'œuvre de l'esprit originale, son propriétaire en serait le créateur. Mais alors, qui serait le créateur de la donnée médicale du patient ?

Tandis que la donnée médicale préexiste au sein du patient source, celle-ci est collectée ou produite grâce aux compétences techniques du soignant dans le cadre de son activité professionnelle¹²⁷⁶. Autrement dit, le créateur de la donnée médicale serait indéniablement le professionnel de santé. Le patient duquel émane des données médicales brutes ne saurait donc être observé comme l'auteur d'une création objet d'un droit de propriété intellectuelle¹²⁷⁷. En ce sens, Valérie Peugeot rappelle que « *les informations brutes et les données ne sont pas couvertes [par le droit d'auteur] ; le droit d'auteur ne concerne que la forme que l'on donne aux informations, et en Europe, le droit sui generis rend propriétaire la cohérence dans une base de données, et non les données elles-mêmes* »¹²⁷⁸. Simple émetteur d'une information brute, le patient ne serait pas le créateur des éléments immatériels de son corps humain. De surcroît, « *si un droit de propriété intellectuelle était consacré au bénéfice de la personne dont les données sont issues cela porterait atteinte aux principes mêmes de la propriété intellectuelle* »¹²⁷⁹, laquelle récompense l'investissement d'un travail créatif. Si la donnée médicale était une œuvre de l'esprit originale, le droit

¹²⁷³ *Ibid.*

¹²⁷⁴ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 350.

¹²⁷⁵ MATTATIA (F.), YAÏCHE (M.), *op. cit.* p. 62.

¹²⁷⁶ Cf. Paragraphes 16 et 50 à 53.

¹²⁷⁷ DESCHANEL (C.), *op. cit.*, § 20.

¹²⁷⁸ PEUGEOT (V.), *Données personnelles : sortir des injonctions contradictoire*, 13 avril 2014. Article disponible en ligne sur le site [www.vecam.org]. Consulté le 4 février 2021.

¹²⁷⁹ DESCHANEL (C.), *op. cit.*, § 20.

d'auteur profiterait alors au professionnel de santé l'ayant formalisée. Ce dernier serait alors titulaire de droits moraux et de droits patrimoniaux sur la donnée médicale du patient.

404. Les droits moraux de l'auteur consistent en quatre prérogatives perpétuelles, inaliénables, imprescriptibles et extrapatrimoniales¹²⁸⁰. Premièrement, le professionnel de santé créateur de la donnée médicale bénéficierait de la paternité de la donnée médicale au mépris de la personne concernée¹²⁸¹. Il y aurait donc une distinction entre le patient source regardé comme un simple support d'informations brutes et le créateur d'une donnée médicale technique. Deuxièmement, le créateur de la donnée médicale pourrait défendre le respect des données médicales¹²⁸². Etant donné que les diagnostics médicaux correspondent à des informations médicales, le médecin pourrait alors contester les contre-avis médicaux. Troisièmement, le professionnel de santé auteur de la donnée médicale du patient aurait le droit de la divulguer¹²⁸³. Si cette prérogative n'était pas limitée aux conditions d'échange et de partages des données médicales entre les personnes dépositaires du secret professionnel, elle porterait gravement atteinte au respect de l'intimité de la vie privée du patient. Quatrièmement, après cession de l'exploitation de la donnée médicale auprès d'un cessionnaire, son créateur pourrait décider de la retirer¹²⁸⁴.

Force est de constater les similitudes entre les droits moraux de l'auteur et les droits que la personne concernée détient sur ses données personnelles. Si le professionnel de santé était l'auteur de la donnée médicale, il émergerait un conflit entre ces deux droits personalistes. En effet, Cécile Deschanel remarque une analogie entre le droit de rectification de la personne concernée¹²⁸⁵ et le droit de repentir de l'auteur¹²⁸⁶, ou encore entre le droit d'effacement des données¹²⁸⁷ et le droit de retrait de l'œuvre¹²⁸⁸. Si les droits moraux du créateur de la donnée médicale appartenaient à un autre individu que la personne

¹²⁸⁰ Article L. 121-1 du code de la propriété intellectuelle.

¹²⁸¹ Article L. 121-1 du code de la propriété intellectuelle.

¹²⁸² Article L.121-1 du code de la propriété intellectuelle.

¹²⁸³ Article L.121-2 du code de la propriété intellectuelle.

¹²⁸⁴ Article L.121-4 du code de la propriété intellectuelle.

¹²⁸⁵ Article 16 du RGPD.

¹²⁸⁶ Article L.121-4 du code de la propriété intellectuelle.

¹²⁸⁷ Article 17 du RGPD.

¹²⁸⁸ Article L.121-4 du code de la propriété intellectuelle.

concernée, l'exercice des prérogatives morales de l'auteur et l'exercice des droits du patient sur ses données médicales seraient réciproquement entravés. En effet, deux entités différentes détiendraient des pouvoirs personalistes équivalents à l'égard d'un même objet. Dès lors, comment concilier le droit de divulgation de l'œuvre avec les droits d'opposition au traitement et d'effacement des données personnelles ? Bien que les droits moraux de l'auteur relèvent des droits de la personnalité dans la mesure où une œuvre de l'esprit est reliée à son créateur par un cordon ombilical¹²⁸⁹, le producteur de la donnée médicale n'est pas intimement rattaché à l'élément immatériel du corps humain d'autrui. En effet, seul le patient est profondément attaché à ses données médicales. Nul autre individu que le patient concerné ne devrait alors être titulaire d'un droit de la personnalité sur sa chose anthropomorphique. Le rapport de droit entre la donnée médicale et une personne physique doit exclusivement être consubstantiel au patient qui en est la source. L'application du régime du droit d'auteur à la donnée médicale aurait potentiellement pu être conçue à la seule condition que le patient en soit l'unique attributaire.

405. S'il était *de jure* octroyé à la personne concernée, il semblerait que le régime dualiste du droit d'auteur présenterait deux avantages. D'une part, il paraîtrait que les droits moraux de l'auteur renforceraient le contrôle du patient sur l'usage de ses données médicales personnelles. D'autre part, il paraîtrait que les droits patrimoniaux de l'auteur rétabliraient le déséquilibre économique entre les exploitants des données médicales et le patient. Tout en conservant les droits de la personnalité qu'il détient sur ses données médicales personnelles, le patient aurait pu en céder l'utilisation et l'exploitation au moyen d'une licence onéreuse. L'association Génération Libre propose même que « *le citoyen créateur de base de données consent[e] par écrit à un gestionnaire de plateforme de la donnée, dans un contrat de licence à l'exploitation catégorielle de sa donnée selon une finalité déterminée* »¹²⁹⁰. En apparence, le régime du droit d'auteur semble permettre de « *lutter contre les formes nouvelles d'exploitation des données personnelles* »¹²⁹¹ étant donné que « *chacun pourrait gérer ses données en les louant, prêtant, récupérant, etc.* »¹²⁹². Nonobstant ces agréments, la CNCDH

¹²⁸⁹ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 56.

¹²⁹⁰ LANDREAU (I.), *op. cit.*, p. 92.

¹²⁹¹ CNCDH, Avis du 22 mai 2018, *loc. cit.*

¹²⁹² *Ibid.*

signale toutefois que « *l'application du concept de propriété est contestable philosophiquement et juridiquement, et n'apporte pas de réponses adéquates* »¹²⁹³.

406. D'abord, les droits de l'auteur ont pour effets de bloquer et de limiter l'exploitation de l'œuvre. Le traitement des données médicales du patient à des fins de prise en charge sanitaire ou de recherche dans le domaine de la santé serait alors conditionné par la cession d'une licence au profit de leur exploitant. Les possibilités d'usage de la donnée médicale ne seraient plus encadrées par l'article 9.2 du RGPD, mais seraient conditionnées par la volonté contractuelle du patient. Partant, l'instauration d'un droit d'auteur en faveur des personnes concernées sur leurs données personnelles risquerait de renforcer le clivage social entre les plus pauvres et les plus riches¹²⁹⁴. Certainement, la volonté contractuelle de céder une licence sur ses données médicales pourrait être viciée par la contrainte économique.

En outre, l'exclusivité du monopole d'exploitation de la donnée médicale paralyserait le principe de la libre circulation des données personnelles. Le treizième considérant du RGPD dispose qu'« *afin d'assurer un niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union, et d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur, un règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques [...] pour offrir aux personnes physiques de tous les États membres un même niveau de droits opposables et d'obligations et de responsabilités pour les responsables du traitement et les sous-traitants, et pour assurer une surveillance cohérente du traitement des données à caractère personnel, et des sanctions équivalentes dans tous les États membres, ainsi qu'une coopération efficace entre les autorités de contrôle des différents États membres* ». Le droit à la protection des données personnelles édifie une police administrative spécifique qui régleme les traitements de données personnelles sans qu'il n'y ait besoin de recourir à une réservation propriétaire. Assurément, le corpus juridique relatif à la protection des données personnelles garantit plus de protection aux personnes concernées que ne pourrait l'offrir un droit de propriété privatiste. Les données médicales doivent rester librement exploitables, sous le contrôle du patient concerné et dans le respect de ses droits, pour les finalités autorisées à l'article 9.2 du RGPD et selon les conditions spéciales des articles 66 et suivants

¹²⁹³ *Ibid.*

¹²⁹⁴ CNIL, *Vie privée à l'horizon 2020*, Cahiers IP Innovation & Prospective, n°01, 2012, p. 56.

de la loi Informatique et Libertés. L'affectation de la donnée médicale au patient suffit donc à assurer la protection du patient en dehors de toute forme d'appropriation.

407. Ensuite, les droits patrimoniaux de l'auteur sont temporaires. Passé un certain délai, la création tombe dans le domaine public. Valérie Peugeot s'inquiète alors du sort des données médicales personnelles à l'issue du temps de protection accordé à la personne concernée ou à ses ayants droit. L'auteur considère que le « *régime de propriété intellectuelle est totalement inapproprié : au bout de quel délai les données sortiraient-elles de la propriété de leur (co)producteur qu'est l'utilisateur ? Au moment où elles n'ont plus de valeur sur le marché de l'économie de l'attention ?* »¹²⁹⁵.

408. Finalement, contrairement aux droits moraux et patrimoniaux de l'auteur, les aspects moraux et patrimoniaux inhérents à la donnée médicale personnelle sont indissociables. En effet, l'individu dispose d'un droit de la personnalité à l'égard de ses informations, quand bien même elles comporteraient des attributs pécuniaires. Jérémy Antippas explique que « *les droits dits « patrimoniaux » de la personnalité apparaissent inutiles sitôt que l'on admet qu'un même droit de la personnalité, serait-il extrapatrimonial, peut permettre de réaliser des opérations économiques* »¹²⁹⁶. C'est ainsi que la jurisprudence de la première chambre civile de la cour de cassation exclut la reconnaissance d'un droit patrimonial sur l'image, mais ne récuse pas toute valeur économique de l'image de la personne en en concevant les exploitations contractuelles¹²⁹⁷. Bien que les droits de la personnalité soient de nature extrapatrimoniale, il apparaît admissible de concéder le droit d'exploiter les attributs de sa personnalité en contrepartie d'une compensation financière¹²⁹⁸. Concevoir une rémunération en contrepartie de l'exploitation des données médicales ne serait donc pas contraire à la nature extrapatrimoniale de la chose anthropomorphique. Certainement, « *grâce à la théorie des droits de la personnalité, la patrimonialité tendrait à s'installer au sein de ces éléments traditionnellement considérés comme extrapatrimoniaux en raison de leur lien intime avec*

¹²⁹⁵ PEUGEOT Valérie, *Données personnelles : sortir des injonctions contradictoire*, 13 avril 2014. Article disponible en ligne sur le site [www.vecam.org]. Consulté le 4 février 2021.

¹²⁹⁶ ANTIPPAS (J.), *Propos dissidents sur les droits dits « patrimoniaux » de la personnalité*, RTD com., 2012, n°01, p. 36.

¹²⁹⁷ LOISEAU (G.), *La crise existentielle du droit patrimonial à l'image*, Recueil Dalloz, 2010, n°08, p. 450.

¹²⁹⁸ Cf. Paragraphe 450.

l'âme d'une personne »¹²⁹⁹. Bien qu'elle soit extrapatrimoniale, la donnée médicale peut donc revêtir un aspect économique. Néanmoins, son exclusion du marché a pour effet de l'écarter de tout circuit économique. Au demeurant, la valorisation de la donnée médicale provient davantage de son exploitation – dont le résultat peut engendrer des produits économiques – que de sa valeur intrinsèque. En effet, la valorisation économique du traitement de la donnée médicale personnelle ou anonyme n'est pas déterminée par son caractère patrimonial. La sacralisation de la chose anthropomorphique ne s'oppose donc pas à ce que le patient profite possiblement de la valorisation du traitement de l'élément immatériel de son corps humain à l'instant où il permet de générer un profit commercial¹³⁰⁰.

409. Pour l'heure, « *les données personnelles en tant que ressources incorporelles ne bénéficient donc d'aucun statut juridique dans le régime de droit existant* »¹³⁰¹. Pour corriger cette lacune de la loi¹³⁰², il apparaît urgent de créer un régime spécifique à la chose anthropomorphique avant qu'un droit voisin des créateurs de données ne soit constitué¹³⁰³.

¹²⁹⁹ NONNOU (E. G.), *loc. cit.*

¹³⁰⁰ Cf. Paragraphe 450.

¹³⁰¹ BOURCIER (D.), DE FILIPPI (P.), *op. cit.*, p. 447.

¹³⁰² « [...] il y a lacune de la loi lorsqu'il n'existe pas de norme applicable pour régler une situation, alors que la science juridique estime qu'il aurait dû y en avoir une » : HO DINH (A.-M.), *Le « vide juridique » et le « besoin de loi »*, pour un recours à l'hypothèse du non-droit, *L'Année sociologique*, vol. 57, 2007, n° 2, p. 419.

¹³⁰³ Tel que proposé par l'association Génération Libre dans le Rapport du Think-tank Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018.

Conclusion du chapitre

410. La nature extrapatrimoniale de la chose anthropomorphique, qu'elle soit à caractère personnel ou anonyme, s'oppose à toute forme d'appropriation, que ce soit par le droit de la propriété mobilière ou par le droit de la propriété intellectuelle. L'exclusion de l'appropriation de la donnée médicale personnelle tend à renforcer sa protection au titre des droits de la personnalité et, communément, à lui conférer une certaine sacralité.

411. D'une part, accorder un droit de propriété sur des données à caractère personnel contreviendrait aux droits concédés à la personne concernée, ainsi qu'aux principes juridiques de protection des données personnelles. Certainement, la cession des données à caractère personnel ne permettrait plus, aux personnes desquelles elles émanent, d'en contrôler ni d'en maîtriser les usages, « *même si ces utilisations vont à l'encontre de leur dignité* »¹³⁰⁴. L'appropriation des données personnelles « *aurait pour conséquence de nous faire passer d'un régime de liberté réglementée de traiter des données à un régime de liberté absolue* »¹³⁰⁵ au mépris des lois de police qui en assurent la protection. L'acquéreur de la donnée personnelle pourrait alors en disposer de la façon la plus absolue sans que la personne concernée ne puisse opposer son autodétermination informationnelle. Autrement dit, l'exercice du droit de propriété de l'acquéreur de la donnée médicale personnelle entraverait les droits que le patient détient sur celle-ci. Pis encore, le droit de propriété romprait le lien entre la donnée médicale personnelle et le patient concerné. Alors que les droits de la personnalité sont inaliénables et imprescriptiblement rattachés à la personne concernée, un « *«droit de propriété» implique en effet le «droit d'être dépossédé»* »¹³⁰⁶.

412. D'autre part, l'appropriation de la donnée médicale personnelle ou anonyme porterait atteinte à la dignité des personnes. D'abord, lorsqu'elles sont encore à caractère personnel, leur appropriation « *est, du point de vue éthique, inconcevable dans la mesure où l'individu ne dispose pas de lui-même, pas plus qu'il ne vend ses informations* »¹³⁰⁷. Dans l'affirmative,

¹³⁰⁴ BOURCIER (D.), DE FILIPPI (P.), *op. cit.*, p. 448.

¹³⁰⁵ OCHOA (N.), *op. cit.*, p. 1165.

¹³⁰⁶ CNIL, *Vie privée à l'horizon 2020*, Cahiers IP Innovation & Prospective, 2012, n°01, p. 55.

¹³⁰⁷ MALLET-POUJOL (N.), *Appropriation de l'information : l'éternelle chimère*, *op. cit.*, p. 333.

« le risque de marchandisation de ses données personnelles est évident »¹³⁰⁸. Ensuite, qu'elle que soit leur nature, « la monétisation de ces données [médicales] ne comporterait-elle pas une violation de certaines prérogatives d'ordre public ? S'il est interdit de commercialiser certaines parties du corps humain, est-il acceptable de commercialiser les données qui représentent des informations émanant du corps humain ? »¹³⁰⁹.

413. La consécration légale des régimes juridiques spécifiques à la chose anthropomorphique personnelle et anonyme pallierait les risques inhérents à la patrimonialisation ainsi qu'à la commercialisation des données médicales. De surcroît, l'extrapatrimonialité de cet objet exclu du marché n'interdirait pas la valorisation économique des résultats issus de son exploitation, notamment en matière de recherches, d'études et d'évaluations dans le domaine de la santé¹³¹⁰.

¹³⁰⁸ CNCDH, Avis du 22 mai 2018, *loc. cit.*

¹³⁰⁹ BOURCIER (D.), DE FILIPPI (P.), *op. cit.*, p. 446 à p. 447.

¹³¹⁰ Article 72 de la loi Informatique et Libertés modifiée.

Chapitre 2 : La valorisation économique du traitement de la donnée médicale extrapatrimoniale

« Un des enjeux des données personnelles tient en effet aux nombreux revenus, de natures très diverses, qui peuvent en être tirés. »¹³¹¹.

414. En raison du statut et du régime juridique que nous consacrons à la donnée médicale¹³¹², ses utilités économiques ne peuvent faire l'objet ni d'une réservation privative, ni d'un commerce juridique à titre onéreux. De surcroît, celle-ci ne peut être ni appréciée monétairement, ni valorisée directement. Les exploitants de la donnée médicale ne peuvent donc générer des profits financiers à partir d'une information médicale prise en tant que telle. Cependant, l'extrapatrimonialité de la chose anthropomorphique et son exclusion du marché ne s'opposent pas à ce que le responsable de son traitement puisse indirectement tirer parti de ses utilités économiques à travers la valorisation des résultats consécutifs à sa réutilisation (**Section 1**). En revanche, le statut que nous conférons à la donnée médicale empêche le patient de profiter financièrement de son traitement. D'une part, il ne peut l'exploiter économiquement au moyen de sa mise à disposition. D'autre part, le monopole d'exploitation des résultats issus de sa réutilisation revient au titulaire des droits patrimoniaux sur la création intellectuelle (**Section 2**). Néanmoins, l'équité¹³¹³ nous incite à considérer le patient, source d'une matière essentielle aux recherches rétrospectives en santé, dans l'équation économique du progrès et de l'innovation sanitaire.

¹³¹¹ ANCIAUX (A.), FARCHY (J.), *Données personnelles et droit de propriété : quatre chantiers et un enterrement*, Revue internationale de droit économique, Vol. XXIX, 2015, n° 03, p. 315.

¹³¹² Cf. Paragraphe 466.

¹³¹³ L'équité est ici entendue comme l'appréciation juste de ce qui est dû à chacun.

Section 1 : La valorisation économique de l'exploitation¹³¹⁴ de la donnée médicale au profit du responsable de traitement

« *La donnée est par ailleurs un actif stratégique dont la valeur est davantage liée à la réutilisation qu'à l'utilisation première.* »¹³¹⁵.

415. A l'exclusion de tout droit patrimonial, le responsable de traitement ne bénéficie, sur la donnée médicale, que d'un droit d'usage temporaire encadré par les normes de police administrative relatives à la protection des données personnelles. Grâce à cet *usus*, le responsable de traitement jouit du droit d'exploiter les données médicales du patient dès lors qu'il poursuit une finalité de recherche et d'innovation dans le domaine de la santé répondant à un motif d'intérêt public (**Paragraphe 2**). Consécutivement, l'exploitant de la donnée médicale détiendra éventuellement des droits réels sur les résultats de la recherche rétrospective fondée sur la réutilisation de la chose anthropomorphique du patient, indépendamment de toute prérogative sur cette dernière (**Paragraphe 1**). En effet, il convient de distinguer la donnée médicale de la création intellectuelle élaborée à partir de la réutilisation de cette matière première.

Paragraphe 1 : Les droits de l'exploitant sur les résultats du traitement de la donnée médicale

416. Il est certain que la donnée médicale ne peut être réservée par le droit de la propriété intellectuelle¹³¹⁶. En revanche, la personne physique ou morale qui l'exploite peut éventuellement détenir un droit privatif sur les résultats consécutifs à son traitement et les valoriser pécuniairement. C'est ainsi que le producteur d'une base de données médicales à caractère personnel peut éventuellement détenir un droit *sui generis* sur son contenu (**A**). De la même manière, l'auteur ou l'inventeur d'une création intellectuelle, élaborée à partir du

¹³¹⁴ L'exploitation est ici entendue comme l'utilisation d'une chose et sa mise à profit pour un objectif donné, qu'il soit, ou non, économique.

¹³¹⁵ Etude d'impact du projet de loi relatif à la gratuité et aux modalités de la réutilisation des informations du secteur public, 29 juillet 2015, p. 18.

¹³¹⁶ Cf. Paragraphes 395 à 409.

traitement de la chose anthropomorphique du patient, peut en posséder la propriété incorporelle afin d'en tirer un profit économique (B).

A) La valorisation du contenu de la base de données médicales à caractère personnel

« A partir du moment où les données ont déjà bénéficié d'un financement pour les produire, le principe de gratuité doit prévaloir »¹³¹⁷.

417. Indépendamment du droit d'auteur accordé au créateur de la structure originale d'une base de données¹³¹⁸, le producteur de son contenu¹³¹⁹ jouit d'un droit *sui generis* sur celui-ci. Bien que le droit *sui generis* soit intégré dans la partie relative à la propriété littéraire et artistique du code de la propriété intellectuelle, il ne permet aucune appropriation des éléments qui y sont intégrés¹³²⁰. En effet, le droit *sui generis* a vocation à protéger l'investissement substantiel des moyens matériel, humain et financier déployés pour la constitution, la vérification ou la présentation du contenu de la base de données¹³²¹. Le droit du producteur d'une base de données tend ainsi à « *défendre l'investissement qu'implique l'activité de collecte et de traitement des données contre les risques de pillage de la totalité ou d'une partie substantielle du contenu de la base* »¹³²². A cet effet, le droit *sui generis* permet d'interdire l'extraction¹³²³ ou la réutilisation¹³²⁴ de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base de données¹³²⁵. En revanche, le producteur d'une base de données ne peut interdire l'extraction ou la réutilisation

¹³¹⁷ CUGGIA (M.), POLTON (D.), WAINRIB (G.), COMBES (S.), Mission de préfiguration du Health Data Hub, Rapport officiel du Ministère des solidarités et de la santé, octobre 2018, p. 18.

¹³¹⁸ Article L.122-3 du code de la propriété intellectuelle.

¹³¹⁹ Le producteur d'une base de données au sens de l'article L.341-1 al. 2 du code de la propriété intellectuelle est « *entendu comme la personne qui prend l'initiative et le risque des investissements correspondants* ».

¹³²⁰ BENSAMOUN (A.), *Création et données : différence de notions = différence de régime ?*, Dalloz IP/IT, 2018, n° 02, p. 85 à p. 89.

¹³²¹ Article L.341-1 du code de la propriété intellectuelle.

¹³²² PASSA (J.), *La propriété de l'information : un malentendu ?*, Droit et Patrimoine, 2001, n° 91.

¹³²³ Article L.342-1 1° du code de la propriété intellectuelle : « *L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit* ».

¹³²⁴ Article L.342-1 2° du code de la propriété intellectuelle : « *La réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme* ».

¹³²⁵ Article L.342-1 du code de la propriété intellectuelle.

d'une partie qualitativement ou quantitativement non substantielle de son contenu par la personne qui y a licitement accès¹³²⁶, à moins que « *ces opérations excèdent manifestement les conditions d'utilisation normale de la base de données* »¹³²⁷. Le droit *sui generis* vise donc à prévenir tout comportement déloyal ou parasitaire entraînant une atteinte à l'investissement économique supporté pour l'élaboration du contenu de la base. Ce droit ne préserve que le contenu de la base entendu comme un ensemble d'informations dont le rassemblement a nécessité un investissement économique substantiel. Tel que le souligne Sylvain Chatry, « *l'objet du droit sui generis n'est pas constitué des données prises de manière individuelle, mais, selon une approche globale, il est composé de l'ensemble des données collectées par le producteur et insérées dans la base* »¹³²⁸. En d'autres termes, le droit *sui generis* ne protège ni la création des éléments constitutifs de la base, ni les données prises individuellement¹³²⁹. Certainement, ce droit de propriété intellectuelle a davantage vocation à protéger l'économie engagée par celui qui supporte les risques des investissements correspondants¹³³⁰. Le droit *sui generis* peut alors être observé comme un droit économique accordé à l'exploitant des éléments obtenus pour la constitution du contenu de la base, en l'occurrence, les données médicales produites initialement à l'occasion de la prise en charge sanitaire du patient.

418. Plus qu'un simple droit d'interdire, la dimension économique du droit *sui generis* favorise un retour sur l'investissement économique engagé pour la constitution, la vérification ou la présentation du contenu de la base. En ce sens, la cour d'appel de Paris considère que ce droit est destiné « *à rentabiliser l'investissement affecté à la constitution d'un ensemble informationnel* »¹³³¹. C'est pourquoi « *le droit d'interdire du producteur de base de données [...] a pour corollaire le droit d'autoriser* »¹³³². Le producteur de la base de

¹³²⁶ Article L.342-3 1° du code de la propriété intellectuelle.

¹³²⁷ Article L.342-2 du code de la propriété intellectuelle.

¹³²⁸ CHATRY (S.), *Droits des producteurs des bases de données*, JurisClasseur Civil, Fasc. 1650, Annexe V° propriété littéraire et artistique, 1^{er} décembre 2018, actu. 1^{er} juin 2021, § 28.

¹³²⁹ CJCE, 9 novembre 2004, aff. C-203/02, *The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd* : Propriété industrielle, 2005, n° 01, comm. 7, P. Kamina ; CCE, 2005, n° 01, comm. 2, C. Caron ; RTD com., 2005, n° 01, p. 90, obs. F. Pollaud-Dulian.

¹³³⁰ Article L.341-1 al. 2 du code de la propriété intellectuelle.

¹³³¹ CA, Paris, pôle 5, ch. 2, 23 mars 2012, n°10/11168, JurisData n° 2012-011871 : D., 2015, n° 15 , p. 908, note T. Lancrenon ; RTD com., 2015, n° 02, p. 294, note F. Pollaud-Dulian ; CCE, 2012, n° 7-8, , comm. 76, A. Debet.

¹³³² MACREZ (F.), *Contrats de consultation et d'exploitation de bases de données*, JurisClasseur Communication, , Fasc. 700, 1^{er} octobre 2016, § 10.

données protégée peut alors consentir à l'utilisation et à l'exploitation onéreuses de son contenu au moyen d'un contrat de cession de droits ou d'un contrat de licence¹³³³. En contrepartie du paiement d'un prix, le producteur de la base de données peut ainsi autoriser un strict droit de consultation des éléments intégrés dans celle-ci. Le cas échéant, le licencié ne pourra accomplir que des actes non substantiels sur son contenu dans le cadre d'une utilisation normale¹³³⁴. Au surplus, l'utilisateur qui souhaite exploiter le contenu de la base de données doit obtenir l'autorisation d'en effectuer des extractions ou des réutilisations substantielles. Ces autorisations peuvent être limitées à un nombre d'utilisateurs, à un nombre de données, ou à des finalités déterminées et spécifiques. Si l'exploitation des données médicales, pseudonymisées ou anonymisées, intégrées dans une base de données privée peut être rémunérée (2), la question des redevances de réutilisation des informations produites par le secteur public pose davantage de difficultés en raison de l'articulation des différents régimes juridiques applicables (1).

1. La valorisation des bases de données médicales produites par des organismes chargés d'une mission de service public

419. C'est par le truchement de la loi pour une République numérique¹³³⁵ que les pouvoirs publics ont affermi le principe de l'ouverture des données publiques. Cette ambition politique a été objectivée par l'obligation, pour les administrations, de mettre les documents administratifs qu'elles détiennent à disposition en ligne, ou de les communiquer aux personnes qui en font la demande¹³³⁶. Le droit à la communication de ces documents a pour corollaire le droit de réutiliser les informations qu'ils contiennent¹³³⁷. Le législateur a facilité l'accès aux données publiques au moyen de leur ouverture dans l'optique que ces « *ressources intellectuelles* » soient exploitées à des fins d'innovation¹³³⁸. Néanmoins, pour que l'ouverture et la réutilisation des données publiques puissent satisfaire cet objectif, il

¹³³³ Article L.342-1 al. 2 du code de la propriété intellectuelle.

¹³³⁴ MACREZ (F.), *op. cit.*, § 16.

¹³³⁵ Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n°0235, 8 octobre 2016, texte n°1.

¹³³⁶ Article L.311-1 du code des relations entre le public et l'administration.

¹³³⁷ Article L.321-1 du code des relations entre le public et l'administration.

¹³³⁸ BENABOU (V.-L.), *La loi pour une République numérique et la propriété intellectuelle*, Dalloz IP/IT, 2016, n° 11, p. 531.

convenait de limiter les droits de propriété intellectuelle détenus sur les documents produits ou reçus par l'administration. C'est ainsi que les dispositions de la loi pour une République numérique ont instauré « *une exception nouvelle au droit d'auteur mais aussi au droit sui generis des producteurs de bases de données* »¹³³⁹. De toute évidence, tant la normalisation que l'efficacité du régime de réutilisation des données publiques exigeaient une modification du droit de la propriété intellectuelle. Dorénavant, le code des relations entre le public et l'administration prévoit que les informations publiques communiquées ou publiées par les administrations peuvent être gratuitement réutilisées par toute personne à d'autres fins que celles de la mission de service public pour les besoins de laquelle elles ont été produites¹³⁴⁰, nonobstant les éventuels droits de propriété intellectuelle détenus par l'administration¹³⁴¹. Ainsi, les organismes chargés d'une mission de service public n'ont plus la possibilité « *de se retrancher derrière leurs droits de propriété intellectuelle pour faire obstacle à la libre réutilisation de leurs bases de données* »¹³⁴². En ce sens, le Conseil d'Etat a jugé qu'une personne morale de droit public, en sa qualité de producteur d'une base de données publiques, ne pouvait opposer son droit *sui generis* pour refuser une demande de réutilisation des informations qui y sont contenues¹³⁴³.

420. En outre, le code des relations entre le public et l'administration pose un principe de gratuité de la réutilisation des informations publiques¹³⁴⁴ qui sont colligées dans les bases de données publiques produites par l'administration. En effet, l'établissement d'une redevance en contrepartie de la réutilisation du contenu de ces bases constitue une exception strictement

¹³³⁹ BENABOU (V.-L.), *La loi pour une République numérique et la propriété intellectuelle*, loc. cit.

¹³⁴⁰ Articles L.321-1 et L.324-1 du code des relations entre le public et l'administration.

¹³⁴¹ Article L.321-3 al. 1 du code des relations entre le public et l'administration ; BOURGEOIS (M.), COUSIN (G.), *Les apports de la loi pour une République numérique en matière de propriété intellectuelle*, La semaine juridique - entreprise et affaires, 2016, n° 49, p. 32 à p. 37 ; CORNU (M.), *Ouverture des données : les trompe-l'œil de la loi*, Dalloz IP/IT, 2016, n° 11, p. 515 à p. 519 ; AZZI (T.), *Open data et propriété intellectuelle, État des lieux au lendemain de l'adoption de la loi pour une République numérique*, Recueil Dalloz, 2017, n° 11, p. 583 à p. 592 ; MARCHAND (J.), *L'accès et la réutilisation des données publiques dans le cadre de la loi pour une République numérique*, In CHATRY (S.), GOBERT (T.), *Numérique. Nouveaux droits, nouveaux usages*, Actes du colloque organisé le 10 mars 2017 à l'Université de Perpignan Via Domitia, Mare & Martin, 2017, p. 35 à p. 49 ; BERNAULT (C.), *Ouverture des données publiques et propriété intellectuelle*, Dalloz IP/IT, 2018, n° 02, p.103 à p. 106.

¹³⁴² CLUZEL-METAYER (L.), *La loi pour une République numérique : l'écosystème de la donnée saisi par le droit*, AJDA, 2017, n°06, p. 340.

¹³⁴³ CE, 10e et 9e ch., 08 février 2017, n° 389806, *Société NotreFamille.com*, Lebon 2017 ; ADJA, 2017, n°06, p. 318, note D. Poupeau ; La Semaine Juridique Administrations et Collectivités territoriales, 2017, n° 41, comm. 2241, N. Gabayet ; AJ Collectivités Territoriales, 2017, n° 06, p. 350, note J.-D. Dreyfus.

¹³⁴⁴ Article L.324-1 du code des relations entre le public et l'administration.

limitée. D'une part, le versement d'une redevance de réutilisation ne peut être envisagé seulement lorsque les administrations « *sont tenues de couvrir par des recettes propres une part substantielle des coûts liés à l'accomplissement de leurs missions de service public* »¹³⁴⁵. Ce tempérament n'est applicable que pour celles « *dont l'activité principale consiste en la collecte, la production, la mise à disposition ou la diffusion d'informations publiques* »¹³⁴⁶ et « *lorsque la couverture des coûts liés à cette activité principale est assurée à moins de 75 % par des recettes fiscales, des dotations ou des subventions* »¹³⁴⁷. Les administrations remplissant ces deux conditions cumulatives sont inscrites sur une liste fixée par décret en Conseil d'Etat¹³⁴⁸. D'autre part, « *la réutilisation peut également donner lieu au versement d'une redevance lorsqu'elle porte sur des informations issues des opérations de numérisation des fonds et des collections des bibliothèques, y compris des bibliothèques universitaires, des musées et des archives* »¹³⁴⁹. Par ailleurs, « *ces [deux] exceptions sont elles-mêmes encadrées, de sorte que même les administrations en principe « éligibles » au mécanisme de redevances peuvent être contraintes de permettre la réutilisation gratuite de certaines informations* »¹³⁵⁰. En effet, pour les cas où le législateur autorise exceptionnellement l'établissement d'une redevance de réutilisation au profit de l'administration, son instauration est, par surcroît, limitée aux catégories d'informations figurant sur une liste fixée par décret¹³⁵¹. Il apparaît que les possibilités d'instauration d'une redevance de réutilisation des informations publiques sont particulièrement étroites¹³⁵².

Afin de déterminer si le principe de gratuité instauré à l'article L.324-1 du code des relations entre le public et l'administration trouve à s'appliquer aux bases de données médicales personnelles produites par les établissements investis d'une mission de service

¹³⁴⁵ *Ibid.*

¹³⁴⁶ Article R.324-4-1 du code des relations entre le public et l'administration.

¹³⁴⁷ *Ibid.*

¹³⁴⁸ Article L.324-4 du code des relations entre le public et l'administration.

¹³⁴⁹ Article L.324-2 du code des relations entre le public et l'administration.

¹³⁵⁰ LALLET (A.), NGUYEN DUY (P.), *Diffusion et réutilisation des informations publiques : « Open data » - données ouvertes*, Répertoire de contentieux administratif, septembre 2020, § 311.

¹³⁵¹ Articles L.324-5 et D.324-5-1 du code des relations entre le public et l'administration.

¹³⁵² Voir : CLUZEL-METAYER (L.), *Le code face aux données*, In KOUBI (G.), CLUZEL-METAYER (L.), Cluzel-Métayer, Lucie, TAMZINI (W.) (dir.), *Lectures critiques du code des relations entre le public et l'administration*, LGDJ, 2018.

public, il convient de qualifier si ces données correspondent aux *informations publiques* qui font l'objet du droit de réutilisation.

421. L'article L.321-2 du code des relations entre le public et l'administration énonce que les informations contenues dans des documents dont la communication ne constitue pas un droit pour toute personne ne sont pas considérées comme des *informations publiques* pouvant être librement communiquées et réutilisées. L'application du droit commun de la réutilisation des documents administratifs semble donc conditionnée par l'étendue de la communicabilité des informations du secteur public qu'ils renferment. Autrement dit, seules les données qualifiées d'*informations publiques* peuvent faire l'objet d'une réutilisation après communication. L'enjeu consiste donc à identifier la nature des données médicales produites par le secteur public ; à discerner si elles constituent, ou non, des *informations publiques*. Etant donné que la qualification d'une *information publique* dépend de son caractère communicable, la question qui se pose est de savoir si les données médicales personnelles des patients peuvent être communiquées à des tiers. Pour répondre à cette interrogation, il convient d'examiner les possibilités d'accès aux données médicales personnelles intégrées dans une base de données produites par un établissement investi d'une mission de service public. A cet effet, une distinction entre les données médicales nominatives et les données médicales pseudonymisées s'impose.

Lorsque les données médicales personnelles sont nominatives, leur accès constitue un droit réservé à la personne concernée¹³⁵³. Certainement, les informations dont la communication porterait atteinte à la vie privée et au secret médical ne sont communicables qu'à l'intéressé¹³⁵⁴. Il s'ensuit que les données médicales personnelles semblent exclues du champ du droit commun de la réutilisation à raison de leur nature lorsqu'elles permettent d'identifier directement la personne concernée.

En revanche, lorsque la donnée médicale personnelle est pseudonymisée, sa communicabilité n'est plus restreinte à l'intéressé. En effet, « *pour tous les documents non communicables, s'il est possible d'occulter ou de disjoindre les mentions entraînant leur non-communicabilité, le document est communiqué avec occultation ou disjonction des mentions*

¹³⁵³ Cf. Paragraphe 189.

¹³⁵⁴ Article L.311-6 du code des relations entre le public et l'administration.

en cause »¹³⁵⁵. Le cas échéant, il convient « *de concilier le droit d'accès public aux documents officiels et le droit à la protection des données à caractère personnel* »¹³⁵⁶. Assurément, la réutilisation des données médicales pseudonymisées issues de bases de données produites par l'administration correspond à un traitement de données personnelles. D'une part, la préservation de l'identité du patient permet de sauvegarder le secret professionnel médical. Les dispositions des articles L.311-6 du code des relations entre le public et l'administration et L.1111-7 du code de la santé publique deviennent donc inapplicables. D'autre part, tout traitement de données médicales pseudonymisées peut être mis en œuvre dès l'instant où il est réputé conforme aux principes gouvernant la protection des données personnelles et, le cas échéant, après qu'il ait été autorisé par l'autorité de contrôle. Pour que les réutilisateurs des données personnelles puissent les intégrer dans des services à forte valeur économique ou sociale ajoutée ¹³⁵⁷, « *il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* »¹³⁵⁸. Les conditions légales et réglementaires encadrant la réutilisation des données médicales pseudonymisées sont finalement identiques qu'elles soient intégrées dans une base de données produite par le secteur public ou par le secteur privé. Pour autant, le droit commun de la réutilisation des informations publiques, fixant un principe de gratuité, trouve-t-il à s'appliquer aux données médicales pseudonymisées lorsqu'elles sont produites par l'administration ?

422. Dans un avis du 31 juillet 2008, la CADA estimait que la communication des documents couverts par l'un des secrets mentionnés à l'article L.311-6 du code des relations entre le public et l'administration ne constituait pas un droit pour toute personne dans la mesure où ils ne sont accessibles qu'aux intéressés¹³⁵⁹. A l'inverse, si la pseudonymisation des données médicales personnelles permet de lever le secret ayant vocation à les protéger,

¹³⁵⁵ DOUVILLE (T.), *Droit des données à caractère personnel, op. cit.*, p. 351.

¹³⁵⁶ Article 86 du RGPD.

¹³⁵⁷ L'ouverture des données du secteur public a principalement pour objectif de « proposer de nouvelles ressources pour l'innovation économique et sociale : les données partagées trouvent des réutilisateurs qui les intègrent dans de nouveaux services à forte valeur ajoutée économique ou sociale. » *In* L'ouverture des données publiques, Les actions du Gouvernement, mis à jour le 19 avril 2021. Disponible en ligne sur le site [www.gouvernement.fr]. Consulté le 16 juillet 2021.

¹³⁵⁸ Considérant 13 du RGPD.

¹³⁵⁹ CADA, avis n° 20082716, 31 juillet 2008.

elles deviendraient, *a priori*, communicables à toute personne non détentrice du secret professionnel médical¹³⁶⁰. En effet, l'accès aux données médicales pseudonymisées n'est pas conditionné par la qualité du demandeur mais par la conformité du traitement aux dispositions relatives à la protection des données personnelles. En ce sens, les dispositions de l'article L.312-1-2 du code des relations entre le public et l'administration conçoivent la communication des informations couvertes par le secret professionnel médical après occultation des mentions protégées. Ainsi, les données médicales pseudonymisées pourraient être considérées comme des *informations publiques* soumises au droit commun de la réutilisation et, conséquemment, au principe de gratuité. Par suite, tout établissement participant à une mission de service public ayant constitué une base de données médicales pseudonymisées, telle qu'un entrepôt de données de santé¹³⁶¹, devraient en garantir la réutilisation gratuite par toute personne justifiant de garanties appropriées en matière de protection des données personnelles. En dehors des deux exceptions autorisant l'établissement d'une redevance de réutilisation¹³⁶², les établissements investis d'une mission de service public ne pourraient ni valoriser, ni recouvrer l'investissement économique supporté pour la constitution, la vérification ou la présentation du contenu d'une telle base de données.

423. Bien que nous soutenons que les données médicales pseudonymisées produites par l'administration constituent des *informations publiques* au sens du code des relations entre le public et l'administration¹³⁶³, d'aucuns diront que leur caractère personnel s'oppose à une telle qualification. Le cas échéant, les données médicales pseudonymisées produites par des personnes morales de droit public seraient uniquement observées comme *des données de la sphère publique*. Dans une pareille hypothèse, le droit commun de la réutilisation s'en trouverait-il écarté ? Les magistrats des juridictions administratives Alexandre Lallet et Pearl Nguyen Duy ont précisé que « *la reconnaissance législative d'un principe de libre réutilisation des informations publiques entrant dans le champ d'application du régime de droit commun ne signifie nullement que la réutilisation d'autres données relevant de la* »

¹³⁶⁰ CADA, avis n° 20041039, 1^{er} avril 2004.

¹³⁶¹ CNIL, *Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?*, 28 novembre 2019. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 29 juillet 2021.

¹³⁶² Cf. Paragraphe 419.

¹³⁶³ En raison, par exemple, du risque de réidentification du patient concerné.

sphère publique » *serait prohibée par principe* »¹³⁶⁴. En l'absence d'une telle interdiction, il faut comprendre que la réutilisation des *données de la sphère publique* est permise. En revanche, la réutilisation des *données de la sphère publique* ne saurait entrer dans le régime de droit commun de la réutilisation des *informations publiques*¹³⁶⁵. Leur communication en vue de leur exploitation se trouve donc exclusivement encadrée par des régimes spéciaux dérogeant à ce droit commun. Il en advient que la réutilisation des bases de données de l'administration, constituées de *données de la sphère publique*, est régie par le droit *sui generis* de la propriété intellectuelle. Si les données médicales pseudonymisées produites par le service public hospitalier étaient qualifiables de *données de la sphère publique*, l'administration pourrait faire valoir son droit *sui generis* afin de valoriser ses bases de données. L'établissement d'une licence de réutilisation à titre onéreux pourrait alors être concédée en vertu du deuxième alinéa de l'article L.342-1 du code de la propriété intellectuelle. En effet, « *les deux éléments les plus différenciants du régime de droit commun sont le principe de gratuité de la réutilisation et l'intervention de la CADA* »¹³⁶⁶. Cette acception signifierait-elle que la tarification de la réutilisation des données médicales pseudonymisées produites par le service public hospitalier puisse être librement fixée par l'administration ? Le simple critère de la communicabilité de l'information pseudonymisée permet-il de les qualifier de *données de la sphère publique* et de s'affranchir du principe de gratuité qui gouverne la réutilisation des *informations publiques* ?

424. Si les données médicales pseudonymisées échappaient au droit commun de la réutilisation des *informations publiques*, l'instauration d'une redevance de réutilisation pourrait être licitement établie sur le fondement du droit de la propriété intellectuelle. Néanmoins, cette dérogation devrait être observée comme une entrave aux principes d'égalité et de non-discrimination dégagés par le Conseil d'Etat¹³⁶⁷. Effectivement, les réutilisateurs des bases de données de l'administration subiraient une différence de traitement selon que les informations médicales qui y sont intégrées aient été préalablement pseudonymisées ou

¹³⁶⁴ LALLET (A.), NGUYEN DUY (P.), *Diffusion et réutilisation des informations publiques : « Open data » - données ouvertes*, op. cit., § 386.

¹³⁶⁵ CADA, conseil, n° 20062674, 29 juin 2006.

¹³⁶⁶ LALLET (A.), NGUYEN DUY (P.), *Diffusion et réutilisation des informations publiques : « Open data » - données ouvertes*, op. cit., § 387.

¹³⁶⁷ CE, 10 mai 1974, n° 88032 et 88148, *Denoyez et Chorques*, Rec. Lebon, 1974, p. 274 ; AJDA, 1974, p. 298, chron. M. Franc et M. Boyon.

anonymisées. Dans l'hypothèse où les données médicales pseudonymisées par l'administration étaient uniquement qualifiées de *données de la sphère publique*, celles-ci seraient soumises au principe de redevance du droit *sui generis* des producteurs des bases de données¹³⁶⁸. A l'inverse, les données médicales anonymisées par l'administration, parce qu'elles sont librement communicables¹³⁶⁹, sont qualifiées d'*informations publiques* et donc soumises au principe de gratuité du droit administratif. Pourtant, les usagers souhaitant réutiliser des informations du secteur public, qu'ils s'agissent d'informations médicales pseudonymisées ou anonymisées extraites d'une base de données de l'administration, doivent être placés dans une situation similaire qui ne justifie objectivement et rationnellement aucune différence de traitement¹³⁷⁰. Le principe d'égalité, qui « *implique que toutes les personnes placées dans une situation identique soient traitées de la même manière* »¹³⁷¹, « *est plus profondément un « droit à l'égalité des droits »* »¹³⁷². Seulement, le caractère personnel de la donnée tend à engendrer une différence de traitement entre les usagers souhaitant réutiliser les éléments substantiellement qualitatifs ou quantitatifs d'une base de données médicales produite par le service public.

Cependant, le caractère nominatif, pseudonymisé ou anonymisé de la donnée médicale n'emporte aucune conséquence sur les investissements économiques dépensés pour la production de la base de données éventuellement protégée par le droit *sui generis*. Certainement, le droit *sui generis* n'a pas vocation à protéger les efforts fournis pour la production des données mais le travail exigé pour leur rassemblement au sein d'une base¹³⁷³. Alors, ni le caractère de la donnée, ni l'étendue de sa communicabilité ne devraient devenir des critères conditionnant l'établissement d'une redevance de réutilisation au profit de l'administration. Partant, les dispositions relatives au *principe de gratuité* et à *l'exception de*

¹³⁶⁸ Cf. Paragraphe 420.

¹³⁶⁹ Article L.312-1-2 du code des relations entre le public et l'administration.

¹³⁷⁰ Voir : CE, 10 avril 2015, n°377207, *Société Red Bull on Premise et autre*, Rec. Lebon T., p. 675 ; Dr. fisc., 2015, n° 26, comm. 434, note B. Bohnert.

¹³⁷¹ LASSERRE (B.), *L'égalité des citoyens dans la République*, Discours prononcé à l'École nationale de la magistrature le jeudi 29 novembre 2018, 20 juillet 2021.

¹³⁷² SAUVE (J.-M.), *Principe d'égalité et droit de la non-discrimination*, Intervention lors du Colloque intitulé « *10 ans de droit de la non-discrimination* » organisé par le Défenseur des droits, 5 octobre 2015.

¹³⁷³ Arrêt CJCE, 9 novembre 2004, aff. C-203/02, *The British Horceracing Board Ltd e.a. c/ William Hill Organization Ltd* : « *la notion d'investissement lié à l'obtention du contenu d'une base de données doit [...] s'entendre comme désignant les moyens consacrés à la recherche d'éléments existants et à leur rassemblement dans ladite base, à l'exclusion des moyens mis en œuvre pour la création même d'éléments* ».

*redevance*¹³⁷⁴ devraient généralement concerner la réutilisation de toute information du secteur public rassemblée dans les bases de données médicales produites par l'administration indépendamment de leur caractère pseudonymisé ou anonymisé.

425. Lors d'un discours prononcé à l'école nationale de la magistrature, Bruno Lasserre a exposé que « *la différence de traitement doit être en rapport avec l'objet de la norme qui l'établit* »¹³⁷⁵. Seulement, la différence de traitement dans l'application du principe de gratuité entre la réutilisation des *informations publiques* et la réutilisation des *informations de la sphère publique* n'est formellement motivée par aucune norme. Vraisemblablement, ni le législateur, ni le juge, ni la CADA n'interdisent ou n'autorisent explicitement l'application du principe de gratuité à la réutilisation des informations exclues du régime de droit commun¹³⁷⁶. Dès lors, la solution ne résiderait-elle pas dans l'articulation des différents régimes juridiques tant applicables aux informations du secteur public qu'aux données à caractère personnel ?

Alors que le traitement des données médicales à caractère personnel, intégrées dans les bases de données de l'administration, est régi par le droit à la protection des données personnelles, les modalités de réutilisation de leur contenu pourraient être conjointement organisées par le droit de réutilisation des *informations publiques*. Selon Jean-Bernard Auby, les dispositions de la loi générale ayant le même objet que celles de la loi spéciale ne s'effacent que lorsqu'elles s'avèrent inconciliables¹³⁷⁷. En effet, « *ce retrait [du régime général de la loi n° 78-753 du 17 juillet 1978] n'est pas systématique* »¹³⁷⁸ et « *laisse place souvent à des combinaisons diverses, sous forme de complémentarité ou de concurrence* »¹³⁷⁹. D'une part, il apparaît que ces deux régimes juridiques ne portent pas sur

¹³⁷⁴ Chapitre IV du Titre II du Livre III du code des relations entre le public et l'administration.

¹³⁷⁵ LASSERRE (B.), *loc. cit.*

¹³⁷⁶ A d'autres égards, dans un conseil n°20162674 rendu le 29 juin 2016, la CADA a considéré que les informations contenues dans une convention de délégation de service public communiquées à un avocat en vue de leur réutilisation à des fins commerciales « *ne sont donc pas des informations publiques au sens de cette loi [du 17 juillet 1978] et ne sont dès lors pas régies par son chapitre II relatif à la réutilisation de ces informations publiques. Pour autant, la réutilisation à des fins commerciales de ces informations n'est interdite par aucun texte de portée générale.* ».

¹³⁷⁷ AUBY (J.-B.), *DONNÉES PUBLIQUES. – Droits d'accès. Étendue*, JurisClasseur Administratif, Fasc. 109-60, 24 avril 2018, actu. 20 janvier 2021, § 23.

¹³⁷⁸ *Ibid.*

¹³⁷⁹ AUBY (J.-B.), *op. cit.*, § 24

le même objet. D'autre part, leur conciliation semble concevable dans la mesure où ils se complètent sans jamais se chevaucher. Ainsi, la réutilisation des données médicales pseudonymisées intégrées dans les bases de données produites par l'administration pourrait être organisée par le code des relations entre le public et l'administration, quand bien même leur communication obéirait au régime spécial du droit à la protection des données personnelles. Sauf exception de redevance, l'ensemble des informations issues du secteur public et contenues dans des documents ou des fichiers constitués par l'administration seraient, sans aucune distinction, soumises au principe de gratuité.

426. Tandis que les administrations visées à l'article L.300-2 du code des relations entre le public et l'administration ne peuvent librement établir une redevance pour la réutilisation du contenu des bases de données médicales qu'elles produisent, tout autre producteur semble pouvoir en valoriser le traitement au moyen du droit *sui generis*. Il s'ensuit que pour deux investissements exactement similaires, la portée des droits de propriété intellectuelle accordés au producteur d'une base de données médicales varie en fonction du secteur auquel il est rattaché.

Néanmoins, le principe de gratuité de la réutilisation des informations produites dans le cadre d'une mission de service public a pour avantage de « *fournir des opportunités de création de valeur économique et sociale [...] et d'offrir un puissant vecteur de transformation de la puissance publique* »¹³⁸⁰. Bien que les administrations ne puissent amortir les investissements liés à la production des bases de données médicales, l'Etat profite indirectement de l'économie générée à partir de leur réutilisation et de leur exploitation. En effet, « *plusieurs études européennes montrent que la baisse d'une redevance ou sa suppression entraîne mécaniquement une augmentation de la réutilisation des données concernées* »¹³⁸¹. C'est ainsi que « *le passage à la gratuité [...] pour les organismes chargés d'une mission de service public administrative, a entraîné une multiplication par 20 des volumes de données téléchargées, soit un bénéfice social estimé à 114 millions d'euros par*

¹³⁸⁰ Compte rendu du Conseil des ministres du 31 juillet 2015, *Gratuité et modalités de la réutilisation des informations du secteur public*. Disponible en ligne sur le site [www.gouvernement.fr]. Consulté le 23 juillet 2021.

¹³⁸¹ Etude d'impact du projet de loi relatif à la gratuité et aux modalités de la réutilisation des informations du secteur public, 29 juillet 2015, p. 17.

*an, pour un manque à gagner de 6 millions d'euros par an de redevances environ »¹³⁸². Même si la réutilisation des données médicales à des fins de recherche, d'innovation ou de santé publique présuppose la constitution d'une base dédiée qui ne saurait être valorisée, les résultats consécutifs à leur traitement peuvent engendrer de nouveaux droits de propriété intellectuelle ou industrielle dont l'exploitation produira de nouvelles valeurs économiques. Certainement, l'extrapatrimonialité des données médicales doit être distinguée de l'éventuelle patrimonialité des résultats issus de leur traitement. Toutefois, l'absence de contrepartie directement offerte aux administrations pourrait décourager la constitution et la production de bases de données médicales aux fins de recherche, d'innovation, de santé publique et d'entrepôts de données de santé. Assurément, ce rassemblement de données médicales exige un travail de collecte, d'extraction, de pseudonymisation, de standardisation, d'organisation et de structuration financièrement et humainement conséquent. Seulement, le principe de gratuité s'oppose à la finalité du droit *sui generis* par lequel le législateur a souhaité « *avantager celui qui a travaillé sur cet assemblage de données* »¹³⁸³. Les administrations peuvent alors se sentir lésées lorsque ces investissements, pourtant étrangers à leurs missions principales, profitent aux tiers réutilisateurs qui sauront en tirer un profit économique.*

427. Compte tenu de ce qui précède, il semble étonnant que la Plateforme nationale des données de santé, autrement appelée Health Data Hub, puisse tarifier l'accès aux bases de données du Système national des données de santé (SNDS) dont elle assure la mise à disposition. En effet, l'article L.1461-5 du code de la santé publique prévoit que l'accès aux données de santé pseudonymisées et intégrées dans les différentes bases de données du SNDS est gratuit pour les traitements demandés par l'autorité publique ainsi que pour les recherches réalisées exclusivement pour les besoins des services publics administratifs. A l'inverse, il faut comprendre que cet accès s'avère payant pour les acteurs du secteur privé. Alors qu'aucune norme juridique ne précise cette possibilité, le Health Data Hub annonce facturer et collecter « *les revenus de la tarification liés à la mise à disposition des données* »¹³⁸⁴. Pourtant, le Health Data Hub est un groupement d'intérêt public qui cumule « *des missions*

¹³⁸² *Ibid.*

¹³⁸³ DESCHANEL (C.), *L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité ?*, Revue Lamy Droit de l'immatériel, 2019, n°156, § 19.

¹³⁸⁴ Health Data Hub, *Charte Responsable de données*. Disponible en ligne sur le site [<https://www.health-data-hub.fr>], consulté du 09 juillet 2021.

de service public administratif et des missions industrielles et commerciales »¹³⁸⁵. Les missions qui relèvent d'un service public administratif concernent « *globalement celles qui se rattachent à la mission de mise à disposition des données du patrimoine du Hub* »¹³⁸⁶. Cette entité publique correspond donc aux personnes de droit public chargées d'une mission de service public visées à l'article L.300-2 du code des relations entre le public et l'administration. De plus, Eric Péchillon souligne qu'« *il apparaît [...] que le système de données de santé constitue un bien public qui ne peut être approprié par aucun des acteurs du système* »¹³⁸⁷. Cela signifie que les informations pseudonymisées du SNDS, qui sont réunies, organisées et mises à disposition par le Health Data Hub, pourraient être gratuitement réutilisées par les porteurs de projets autorisés à les traiter. En outre, le Health Data Hub est responsable de l'enrichissement de la « base principale » du Système national des données de santé¹³⁸⁸ ainsi que de la constitution d'un catalogue de bases de données ne couvrant pas l'ensemble de la population française¹³⁸⁹. Il s'ensuit que le Health Data Hub peut être observé comme le producteur des jeux et des bases de données pseudonymisées extraites du Système national des données de santé et minimisées conformément à la finalité du traitement projeté. Si ces différentes bases de données peuvent être considérées comme des documents produits par une administration dans le cadre de ses missions de service public, comment justifier la tarification de l'accès à leur contenu ? Deux hypothèses pourraient expliquer cette dérogation au principe de gratuité.

En premier lieu, il est supposé que le législateur ait écarté la conciliation des régimes généraux et spéciaux¹³⁹⁰ de sorte que l'accès aux données pseudonymisées du SNDS ne soit encadré que par le régime spécial du code de la santé publique et du droit à la protection des données¹³⁹¹. Il suffit de lire l'avenant à la convention constitutive de l'ancien Institut national des données de santé pour constater que « *le groupement d'intérêt public « Plateforme des données de santé » est régi par le règlement (UE) 2016/679 du Parlement européen et du*

¹³⁸⁵ CUGGIA (M.), POLTON (D.), WAINRIB (G.), COMBES (S.), *op. cit.*, p. 57.

¹³⁸⁶ *Ibid.*

¹³⁸⁷ PECHILLON (E.), *L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ?*, L'information psychiatrique, Vol. 91, 2015, n° 08, p. 649.

¹³⁸⁸ Article R.1461-3 III. 1° du code de la santé publique.

¹³⁸⁹ Article R.1461-3 III. du code de la santé publique.

¹³⁹⁰ Cf. Paragraphe 423.

¹³⁹¹ Articles L.1460-1 à L.1462-2 du code de la santé publique.

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 »¹³⁹², ainsi que par « *l'article L.1462-1 et L.1462-2 du code de la santé publique* »¹³⁹³. L'application du régime commun de la réutilisation des informations du secteur public serait alors exclue pour les données médicales pseudonymisées¹³⁹⁴. En revanche, l'accès aux bases de données anonymisées et agrégées mises à disposition par le Health Data Hub sont librement et gratuitement accessibles en « *open source* »¹³⁹⁵.

En deuxième lieu, il est présumé que les conditions permettant d'établir l'exception de redevance puissent être élargies à la réutilisation des informations mises à disposition par le Health Data Hub. D'une part, la principale mission de ce groupement d'intérêt public consiste à « *réunir, organiser et mettre à disposition les données du système national des données de santé* »¹³⁹⁶. Le Health Data Hub semble donc remplir la première condition selon laquelle seules les personnes morales de droit public « *dont l'activité principale consiste en la collecte, la production, la mise à disposition ou la diffusion d'informations publiques* »¹³⁹⁷ sont autorisées à établir des redevances de réutilisation. D'autre part, les groupements d'intérêt public sont dotés d'une autonomie financière¹³⁹⁸. Si le Health Data Hub couvrait les coûts liés à cette activité à plus de 75 % par des recettes propres, la deuxième des conditions de l'article R. 324-4-1 du code des relations entre le public et l'administration serait également satisfaite. Dès lors, le Health Data Hub pourrait être ajouté à la liste, fixée par décret, des catégories d'administrations autorisées, en raison de la nature de leur activité et des conditions de leur financement, à établir des redevances¹³⁹⁹.

¹³⁹² Article 1 de l'arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé », *JORF* n°0278, 30 novembre 2019, texte n° 13.

¹³⁹³ *Ibid.*

¹³⁹⁴ *Cf.* Paragraphe 421.

¹³⁹⁵ Article L.1461-2 du code de la santé publique.

¹³⁹⁶ Article L.1462-1 du code de la santé publique.

¹³⁹⁷ Article R.324-4-1 du code des relations entre le public et l'administration.

¹³⁹⁸ Article 98 de la loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit, *JORF* n°0115, 18 mai 2011.

¹³⁹⁹ Article L.324-4 du code des relations entre le public et l'administration.

428. Au demeurant, les administrations inéligibles à l'instauration d'une redevance ont intérêt à constituer, puis à partager, leurs bases de données médicales pseudonymisées en partenariat avec le Health Data Hub. En effet, ce groupement « *peut tarifier des services en lien avec ses missions et reverser une partie de ses recettes aux partenaires tels que les producteurs de données qui ont contribué à leur réalisation* »¹⁴⁰⁰. Bien que le fondement de la tarification de l'accès aux données médicales pseudonymisées contenues dans les bases qu'il met à disposition ne soit pas juridiquement établi, la charte des responsables de données du Health Data Hub annonce qu'il « *reverse au partenaire responsable de données sa quote-part, laquelle permet de couvrir une partie de l'effort financier de collecte, mise en forme, mise en qualité, standardisation et documentation de la base initiale* »¹⁴⁰¹. Concrètement, les établissements concourant au service public hospitalier, ou encore les organismes publics de recherche, peuvent conventionner avec le Health Data Hub afin d'obtenir un appui pour l'organisation, en base, des données médicales pseudonymisées dont ils sont dépositaires. Ensuite, cette nouvelle base a vocation à intégrer le catalogue du SNDS contre le versement d'une rétribution financière déterminée en fonction des conditions tarifaires d'accès par les utilisateurs. En conséquence, le SNDS peut également comprendre « *des données de registres, de cohortes de recherche, d'entrepôts de données hospitalières, etc.* »¹⁴⁰². Par l'intermédiaire du Health Data Hub, les administrations soumises au principe de gratuité peuvent valoriser financièrement le travail correspondant à la création des bases de données médicales et favoriser leur réutilisation au profit de tout porteur de projet poursuivant l'une des six finalités énumérées au III de l'article L.1461-1 du code de la santé publique, y compris la recherche et l'innovation dans le domaine de la santé¹⁴⁰³. Cette incitation économique

¹⁴⁰⁰ Article 3 de l'arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé », *JORF* n°0278, 30 novembre 2019, texte n° 13.

¹⁴⁰¹ Health Data Hub, *Charte Responsable de données*. Disponible en ligne sur le site [<https://www.health-data-hub.fr>], consulté du 09 juillet 2021.

¹⁴⁰² Ibid.

¹⁴⁰³ « *Le système national des données de santé a pour finalité la mise à disposition des données, dans les conditions définies aux articles L. 1461-2 et L. 1461-3, pour contribuer : 1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ; 2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ; 3° A la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ; 4° A l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ; 5° A la surveillance, à la veille et à la sécurité sanitaires ; 6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.* ».

pourrait contribuer à pallier le manque de partage des données médicales¹⁴⁰⁴ générées à l'occasion de la prise en charge sanitaire du patient, ou de sa participation à des recherches impliquant la personne humaine, au profit de la recherche et de l'innovation en santé.

2. La valorisation des bases de données médicales produites par le secteur privé

429. A l'inverse, le droit *sui generis* recouvre sa vigueur lorsqu'il est octroyé au producteur d'une base de données relevant du droit privé. Ainsi, les professionnels de santé exerçant dans le secteur privé peuvent librement valoriser les extractions et les réutilisations quantitativement ou qualitativement substantielles du contenu des bases de données médicales pseudonymisées qu'ils ont produites. Grâce au retour sur l'investissement engagé, ce droit de propriété littéraire et artistique encourage l'organisation et la structuration des données médicales pseudonymisées, ou anonymisées, en vue de leur réutilisation. *In fine*, la valorisation des bases de données soumises au droit privé profite à la collectivité lorsque leur réutilisation a notamment pour finalité « *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* »¹⁴⁰⁵. Néanmoins, la réutilisation des données médicales contenues dans des bases constituées par des producteurs de droit privé ne devrait-elle pas être garantie dès l'instant où les principes régissant la protection des données personnelles sont effectivement respectés ?

430. Bien que le droit *sui generis* contribue à la « *prise en compte de la dimension économique des bases de données et aussi des fruits qu'elles génèrent* »¹⁴⁰⁶, il a également pour fonction d'interdire toute réutilisation de leur contenu. Par l'exercice du droit *sui generis*, le producteur d'une base de données médicales peut alors empêcher toute réutilisation des informations qu'il y a colligées. Pourtant, compte tenu des enjeux relatifs au partage et à la réutilisation de la donnée médicale dans le domaine de la santé¹⁴⁰⁷, cette

¹⁴⁰⁴ Voir : VILLANI (C.), LONGUET (G.), Rapport au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur l'intelligence artificielle et les données de santé, Compte rendu de l'audition publique du 21 février 2019 et de la présentation des conclusions du 21 mars 2019.

¹⁴⁰⁵ Article 9.2 i) du RGPD.

¹⁴⁰⁶ CAVALIER (M.), *op. cit.*, p. 115.

¹⁴⁰⁷ Voir : VILLANI (C.), LONGUET (G.), *loc. cit.*

ressource première ne devrait-elle pas être qualifiée de « donnée d'intérêt général »¹⁴⁰⁸ ? C'est implicitement ce qu'a consacré la loi relative à l'organisation et à la transformation du système de santé¹⁴⁰⁹ en élargissant le SNDS à l'ensemble des informations médicales recueillies à l'occasion de tous les actes – en partie – financés par l'Assurance maladie. C'est ainsi que l'ensemble des données médicales produites par les professionnels de santé exerçant en secteur privé alimenteront systématiquement les bases du Système national des données de santé afin d'être mises à disposition par le Health Data Hub. Cette nouvelle disposition peut entraîner deux conséquences.

Premièrement, les professionnels de santé du secteur privé ayant produit une base de données médicales pourraient être concurrencés par le Health Data Hub. En effet, les utilisateurs des données médicales à des fins de recherche et d'innovation dans le domaine de la santé pourraient préférer s'adresser à ce groupement afin de bénéficier de jeux de données dont l'accès est « *aisé et unifié, transparent et sécurisé* »¹⁴¹⁰, d'un accompagnement « *dans la prise en main et le traitement des données de santé* »¹⁴¹¹ et d'une offre technologique à l'état de l'art. En conséquence, les producteurs de bases de données médicales du secteur privé trouveraient, eux aussi, un intérêt à établir un partenariat avec le Health Data Hub afin de participer activement à cet écosystème tout en valorisant les efforts déployés pour la constitution, la vérification ou la présentation de la base.

Deuxièmement, les professionnels de santé du secteur privé qui ne souhaiteraient pas constituer de bases de données médicales, ou ceux qui désireraient interdire la réutilisation de leur contenu, ne pourront pas empêcher leur intégration dans le SNDS ainsi que leur réunion, leur organisation et leur mise à disposition par le Health Data Hub. En effet, « *le droit du producteur de base de données ne permet pas d'empêcher la constitution d'une base*

¹⁴⁰⁸ Voir : Rapport relatif aux données d'intérêt général du Conseil d'Etat, du Conseil général de l'économie et de l'Inspection générale des finances, septembre 2015, p. 2 : « [...] imposer l'ouverture de certaines données détenues par des personnes privées pourrait concourir à l'intérêt général (i) en permettant une conduite plus efficace de politiques publiques sectorielles, (ii) en assurant une meilleure information des citoyens, (iii) en concourant à la recherche scientifique, (iv) ou en bénéficiant au développement économique ».

¹⁴⁰⁹ Article 41 de la loi n° 2019-774 du 24 juillet 2019.

¹⁴¹⁰ www.health-data-hub.fr.

¹⁴¹¹ *Ibid.*

nouvelle par la collecte indépendante - c'est-à-dire sans accès à la base existante - d'informations identiques à celles contenues dans cette dernière »¹⁴¹².

431. Quel que soit le fondement¹⁴¹³ en vertu duquel le producteur d'une base de données médicales peut financièrement la valoriser, le prix versé en contrepartie de la réutilisation de son contenu doit être limité aux investissements liés à sa constitution. En d'autres termes, la valorisation de la constitution des bases de données médicales ne doit avoir pour seul objet que l'amortissement des investissements qu'elle a nécessités. Assurément, la tarification de la réutilisation du contenu d'une base de données médicales doit viser à rentabiliser le travail engendré par ce traitement sans jamais valoriser l'information médicale extrapatrimoniale. Dès lors, le prix correspondant à la cession des droits du producteur d'une base de données médicales, ou à la licence concédée pour la réutilisation de son contenu, ne peut englober la potentielle valeur économique de l'information médicale en raison de son exclusion du marché¹⁴¹⁴. En effet, l'intégration de la donnée médicale au sein d'une base protégée par le droit *sui generis* ne modifie en rien sa situation au regard du régime juridique qui est le sien¹⁴¹⁵. La vente du contenu d'une base de données ne peut donc correspondre en la vente des informations médicales qui la composent, mais au transfert onéreux des droits réels appartenant à son producteur. De la même manière, le montant du prix déboursé pour la réutilisation du contenu d'une base de données médicales ne doit générer aucune suspicion quant à une vente déguisée de données médicales. A l'instar du plafonnement des redevances de réutilisation des informations du secteur public, la tarification correspondant à la réutilisation du contenu de toute base de données médicales ne devrait jamais dépasser « *le montant total des coûts liés à la collecte, à la production, à la mise à la disposition du public ou à la diffusion* »¹⁴¹⁶ de ses éléments. Alors même que la chose anthropomorphique est extrapatrimoniale, sa réutilisation peut potentiellement créer des nouveaux produits indépendamment protégeables et valorisables par les droits de la propriété intellectuelle.

¹⁴¹² PASSA (J.), *loc. cit.*

¹⁴¹³ Au moyen du droit *sui generis*, ou de l'exception des redevances de réutilisation des informations du secteur public, ou par l'intermédiaire du Health Data Hub.

¹⁴¹⁴ Cf. Paragraphe 361.

¹⁴¹⁵ DESCHANEL (C.), *op. cit.*, § 19.

¹⁴¹⁶ Article L.324-1 du code des relations entre le public et l'administration.

B) La valorisation des créations et inventions consécutives à la réutilisation des données médicales

432. Une fois organisées au sein d'une base, les données médicales pseudonymisées ou anonymisées peuvent être réutilisées à des fins étrangères à la prise en charge sanitaire du patient. Indépendamment de la valorisation subséquente à la production d'une base de données, l'opération de traitement consistant en l'analyse des données médicales peut éventuellement être valorisée. En effet, l'utilisateur secondaire des données médicales peut dégager des résultats protégeables par le droit de la propriété intellectuelle nonobstant leur nature extrapatrimoniale. L'objet de cet exposé ne consiste pas à étudier la titularité des droits sur la création intellectuelle, mais à démontrer que les résultats du traitement de la donnée médicale extrapatrimoniale sont économiquement valorisables. Ce postulat sera illustré à travers le traitement des données médicales à des fins de recherche et d'innovation dans le domaine de la santé. Ainsi que le constate Marie Cornu, « *l'activité scientifique est en effet, en bonne part, une activité de création, donnant naissance à des œuvres au sens du code de la propriété intellectuelle* »¹⁴¹⁷.

433. Premièrement, les travaux de recherche dans le domaine de la santé, résultant d'un traitement des données médicales, sont couramment présentés au sein d'un écrit scientifique. Certainement, « *le chercheur est aussi souvent un auteur dans l'accomplissement de sa tâche* »¹⁴¹⁸. Si les écrits scientifiques médicaux permettent de fonder la légitimité et la reconnaissance du chercheur, ils représentent également un patrimoine scientifique, source de revenus et de financement¹⁴¹⁹. Désormais, « *le résultat est une connaissance dont il faut assurer la commercialisation* »¹⁴²⁰, laquelle profite tantôt au chercheur, tantôt à son employeur, tantôt à son éditeur.

¹⁴¹⁷ CORNU (M.), *Création scientifique et statut d'auteur*, Hermès, La Revue, Vol. 57, 2010, n°02, p. 85.

¹⁴¹⁸ *Ibid.*

¹⁴¹⁹ Lesquels varient selon la nature de l'œuvre ainsi que ses conditions de publication, de diffusion et d'exploitation.

¹⁴²⁰ ROBIN (A.), *Le patrimoine scientifique de l'Etat, un patrimoine immatériel en quête de statut*, Revue Communication Commerce Électronique, octobre 2014, n°10, étude 18, § 4.

434. D'abord, l'écrit scientifique est valorisable au moyen du droit d'auteur. En effet, le législateur considère l'écrit scientifique comme une œuvre de l'esprit¹⁴²¹ dont la propriété incorporelle appartient, en principe, à l'auteur¹⁴²². Alors que les données scientifiques – en l'occurrence les données médicales – échappent à toute forme de propriété, la présentation de leur analyse au sein d'un manuscrit scientifique est protégeable par le droit d'auteur dès lors qu'elle manifeste, par une expression particulière, les réflexions personnelles de l'auteur marquant l'empreinte de sa personnalité¹⁴²³. Ainsi, les travaux de recherche portant sur un même jeu de données médicales peuvent faire l'objet d'interprétations différentes dont chaque présentation originale peut donner prise au droit d'auteur. Certainement, « *il est dans la nature de l'évolution scientifique [...] que des publications renouvelées ou nouvelles, portant sur les mêmes données et ayant le même objet, voient le jour et adaptent la présentation des connaissances* »¹⁴²⁴.

435. Ensuite, la publication de l'œuvre scientifique peut être valorisée par l'attribution d'une dotation au bénéfice de l'institution hospitalière à laquelle le chercheur est rattaché. Cette dotation, correspondant aux crédits de financement des missions d'enseignement, de recherche, de référence et d'innovation (MERRI), est calculée selon le mécanisme du système d'interrogation, de gestion et d'analyses des publications scientifiques (SIGAPS) permettant d'attribuer un score de points en fonction « *de la « qualité » de la revue où est parue la publication et de la position du chercheur sur la liste des coauteurs de cette publication* »¹⁴²⁵. Le SIGAPS classe les revues médicales et biomédicales en leur attribuant un pointage par catégorie : « *8 points pour une revue classée « A », 6 points pour une revue classée « B », 4 points pour une revue classée « C », 3 points pour une revue classée « D », 2 points pour une revue classée « E » et 1 point pour une revue classée « NC »* »¹⁴²⁶. De la même façon, ce système accorde des points aux auteurs et contributeurs de la publication scientifique selon la position du nom du chercheur dans la liste des coauteurs. Cet ordre doit alors être défini selon la part de contribution de chacun dans les travaux de recherche :

¹⁴²¹ Article L.112-2 1° du code de la propriété intellectuelle.

¹⁴²² Cf. paragraphe 403.

¹⁴²³ CA, Paris, Pôle 5, Ch. 2, 1^{er} avril 2011, n°10/03052.

¹⁴²⁴ CA, Riom, ch. Comm., 11 janvier 2006.

¹⁴²⁵ GINGRAS (Y.), KHELFAOUI (M.), *L'effet SIGAPS : la recherche médicale française sous l'emprise de l'évaluation comptable*, Zilsel, février 2021, n°08, p. 149.

¹⁴²⁶ GINGRAS (Y.), KHELFAOUI (M.), *op. cit.*, p. 151.

« occuper la première ou la dernière position de la liste des coauteurs d'un article vaut 4 points, la seconde position vaut 3 points, la troisième ou l'avant-dernière position valent 2 points, tout autre position valant 1 point »¹⁴²⁷. Le score SIGAPS correspond au produit de la multiplication du nombre de points accordés à la catégorie de la revue par le nombre de points attribués au chercheur selon son rang. C'est ainsi qu'un chercheur positionné en tête de la liste des coauteurs d'une œuvre scientifique publiée dans une revue de catégorie « A » obtient un score de 32 points, lesquels sont finalement convertis en valeur monétaire.

Yves Gingras et Mahdi Khelifaoui rapportent qu'en « 2017, par exemple, un point SIGAPS valait 648 euros. Par conséquent, la publication d'un article dans une revue de catégorie A pouvait rapporter jusqu'à près de 21 000 euros [...] Une fois fixée, cette somme est versée, dans le cadre de la dotation MERRI du ministère de la Santé, à l'institution de rattachement du chercheur de façon récurrente durant quatre années consécutives, soit un total de 84 000 euros »¹⁴²⁸. Indépendamment des droits de propriété intellectuelle sur l'œuvre scientifique, les publications massives permettent à une même institution d'accumuler des points SIGAPS et d'assurer la perception d'une dotation de plusieurs centaines de milliers d'euros sur plusieurs années. A titre d'exemple, les auteurs précités annoncent que des chercheurs d'une institution de l'AP-HM ayant publié 77 articles dans une revue classée dans la catégorie « NC » pour la seule année 2017 ont obtenu 308 points SIGAPS, « soit près de 200 000 euros qui, versés durant 4 ans à l'AP-HM, rapporteront au total 800 000 euros à l'institution »¹⁴²⁹. L'extrapatrimonialité de la donnée médicale et son exclusion du marché n'interdisent certainement pas la valorisation des publications scientifiques consécutives à son traitement.

436. Deuxièmement, le traitement de la donnée médicale contribue au développement de logiciels, qu'ils soient des systèmes algorithmiques ou d'intelligence artificielle¹⁴³⁰. Effectivement, de tels systèmes sont conçus, entraînés, validés et mis à l'essai à l'aide de jeux de données de haute qualité et « suffisamment pertinents, représentatifs, exempts

¹⁴²⁷ GINGRAS (Y.), KHELFAOUI (M.), *op. cit.*, p. 152.

¹⁴²⁸ GINGRAS (Y.), KHELFAOUI (M.), *op. cit.*, p. 153.

¹⁴²⁹ GINGRAS (Y.), KHELFAOUI (M.), *op. cit.*, p. 169.

¹⁴³⁰ Article 3.1 du projet de règlement européen relatif à l'intelligence artificielle ;

d'erreurs et complets au regard de la destination du système »¹⁴³¹. Dans le domaine de la santé, ces logiciels sont donc, en substance, créés à partir du traitement des données médicales des patients. En dépit de l'extrapatrimonialité de cette matière première, le logiciel dont l'écriture est originale¹⁴³² est privativement réservable par le droit d'auteur. Aussi surprenant que cela puisse paraître, les programmes informatiques, entendus comme des logiciels¹⁴³³, sont unanimement considérés comme des œuvres littéraires¹⁴³⁴. En conséquence, le titulaire des droits d'auteur sur le logiciel jouit de prérogatives patrimoniales sur celui-ci : il peut alors en tirer un profit économique considérable à travers son exploitation et sa commercialisation. Dans l'hypothèse où ces logiciels, développés à partir des éléments immatériels du corps humain du patient, sont « *destinés par le fabricant à une ou plusieurs des fins médicales visées dans la définition de la notion de dispositif médical, [ils] constituent, en soi, des dispositifs médicaux* »¹⁴³⁵. Le cas échéant, leur mise en service et leur mise sur le marché européen sont préalablement conditionnées par leur conformité aux exigences de sécurité et de performances énoncées par le nouveau règlement européen relatif aux dispositifs médicaux¹⁴³⁶, garantie par l'apposition du marquage « CE ». A cet instant, ces logiciels bénéficient du principe de libre circulation des marchandises sur le marché intérieur. Ainsi, l'exploitation de la donnée médicale à des fins de développement de l'intelligence artificielle dans le domaine de la santé concourt directement à la croissance de l'industrie ainsi qu'à la croissance économique¹⁴³⁷. Selon Bpifrance, le recensement annuel des startups françaises du secteur comptait 102 entreprises en 2019, contre 191 en 2020¹⁴³⁸. A l'échelle

¹⁴³¹ Considérant 44 du projet de règlement européen relatif à l'intelligence artificielle.

¹⁴³² Cass. Ass. Plén., 7 mars 1986, n°83-10.477, *Société Babolat c/ Pachot*, Bull. civ. ; D. 1986, p. 405, note B. Edelman ; RIDA, 1986, n° 03, p. 136, note A. Lucas.

¹⁴³³ Arrêté du 22 décembre 1981 enrichissement du vocabulaire de l'informatique, *JORF* du 17 janvier 1982, numéro complémentaire, p. 625. Le logiciel est ici défini comme un « *ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données (en anglais : software)* ».

¹⁴³⁴ Selon l'article 1.1 de la directive du conseil du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur, *JOCE* L 122/42, 17 mai 1991, : « *les États membres protègent les programmes d'ordinateur par le droit d'auteur en tant qu'œuvres littéraires au sens de la convention de Berne pour la protection des œuvres littéraires et artistiques.* ».

¹⁴³⁵ Considérant 19 du règlement 2017/745.

¹⁴³⁶ Règlement (UE) 2017/745 du parlement européen et du conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n°178/2002 et le règlement (CE) n°1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, *JOUE* L 117, 5 mai 2017.

¹⁴³⁷ Cf. Paragraphe 438.

¹⁴³⁸ NÈME (M.), *Panorama des startups santé françaises utilisant l'IA*, 7 juillet 2020. Disponible en ligne sur le site [<https://lehub.bpifrance.fr>]. Consulté le 20 août 2021.

mondiale, « *le marché de l'intelligence artificielle en santé s'élève en 2020 à 4,9 milliards de dollars [...] pour atteindre 45 milliards de dollars en 2026* »¹⁴³⁹. A l'évidence, l'exploitation de la donnée médicale contribue au développement de ce secteur florissant.

437. Troisièmement, le traitement des données médicales du patient peut éventuellement contribuer à la création d'une innovation technique dans le domaine de la santé. En ce cas, l'inventeur peut en réserver le monopole d'exploitation pendant une durée de vingt ans à compter du jour de la demande de dépôt d'un brevet d'invention auprès de l'institut national de la propriété industrielle¹⁴⁴⁰. Ce titre de propriété industrielle est délivrable sous réserve que l'invention soit une activité inventive nouvelle, susceptible d'application industrielle¹⁴⁴¹. A compter de son inscription, la finalité du brevet est d'être exploité. Cette exploitation peut intervenir directement par le breveté ou indirectement par l'effet d'un contrat de cession ou d'un contrat de licence. A défaut d'exploitation suffisante pendant un certain délai, une demande de licence obligatoire peut être formée par toute personne auprès du tribunal judiciaire¹⁴⁴². Si l'exploitation du brevet contribue à rentabiliser les investissements liés aux travaux de recherche de l'inventeur, et à lui assurer une source de revenus, le brevet profite également à l'ensemble de la société. La licence obligatoire, dérogeant au monopole d'exploitation, démontre ainsi « *que le pouvoir discrétionnaire du breveté sur son bien incorporel est contraint par des impératifs d'ordre économique ou social considérés comme supérieurs* »¹⁴⁴³. Dans le domaine de la santé, les défauts d'exploitation peuvent être préjudiciables à l'économie d'un pays mais également à l'intérêt de la santé publique et, *in fine*, aux patients bénéficiaires de l'innovation¹⁴⁴⁴.

438. Bien qu'il doive répondre à une finalité d'intérêt public¹⁴⁴⁵, le traitement de la chose anthropomorphique à des fins de recherche et d'innovation dans le domaine de la santé est au cœur du développement économique de la société. Alors que les données médicales ne

¹⁴³⁹ *Ibid.*

¹⁴⁴⁰ Article L.611-2 2° du code de la propriété intellectuelle.

¹⁴⁴¹ Article L.611-10 du code de la propriété intellectuelle.

¹⁴⁴² Article L.613-11 du code de la propriété intellectuelle.

¹⁴⁴³ Commentaire sous l'article L.613-15-1 du code de la propriété intellectuelle, Dalloz,

¹⁴⁴⁴ *Cf.* les licences d'office prévues à l'article L.613-16 du code de la propriété intellectuelle.

¹⁴⁴⁵ Article 9.2 du RGPD.

peuvent être commercialisées en raison de leur sensibilité, les résultats issus de leur traitement sont, à l’opposé, des actifs immatériels économiquement valorisables. Les données médicales représentent donc un vivier dont la réutilisation contribue à l’enrichissement du fonds commun de la connaissance et aux avancées scientifiques innovantes tout en présentant des utilités économiques. Compte tenu de ces enjeux, leur exploitation ne présenterait-elle donc pas un devoir pour l’ensemble des acteurs du secteur ?

Paragraphe 2 : L’existence d’un droit d’user de la donnée médicale personnelle

439. Nonobstant la réservation des résultats consécutifs à leur exploitation, le responsable du traitement des données médicales du patient ne détient aucun droit privatif sur celles-ci. Néanmoins, l’exploitant des données médicales à caractère personnel jouit d’un droit d’usage à leur égard, à concurrence des droits octroyés au patient concerné et des limitations légales et réglementaires liées à la protection des données personnelles. En effet, l’utilisation de ces éléments immatériels du corps humain, inappropriables et extrapatrimoniaux, est permise dans le respect des conditions des lois de police qui encadrent leur traitement. Rattachée au patient et n’appartenant à personne, la donnée médicale peut alors être exploitée par toute personne physique ou morale conformément aux dispositions générales du RGPD ainsi qu’aux dispositions particulières de la loi Informatique et Libertés modifiée. Autrement dit, les mécanismes de contrôle *a posteriori* de l’usage des informations personnelles « *ne sont pas justifiés par un rapport de propriété susceptible d’entraver toute utilisation de données personnelles par des tiers, mais prennent en compte les droits de l’individu sur ses données, tout en recherchant l’équilibre entre intérêts et libertés en présence, au regard notamment du caractère privé ou sensible des informations en cause* »¹⁴⁴⁶.

Le responsable de traitement qui désire réutiliser les données médicales du patient à des fins de recherche ou d’innovation en santé doit préalablement obtenir l’autorisation administrative de la CNIL. Cette autorité de contrôle se prononce définitivement après la restitution de l’avis du comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES)¹⁴⁴⁷ suite à l’appréciation du motif

¹⁴⁴⁶ CORNU (M.), ORSI (F.), ROCHFELD (J.), *Dictionnaire des biens communs*, 2^e ed, PUF, 2021, Définition du terme « Information ».

¹⁴⁴⁷ Articles 66 III et 76 de la loi Informatique et Libertés modifiée.

d'intérêt public poursuivi par le porteur du projet. Bien que « *la réforme opérée par le RGPD [...] a notamment eu pour objet de supprimer le régime de déclaration et d'autorisation préalable antérieurement applicable* »¹⁴⁴⁸, il n'empêche que « *l'exigence d'une autorisation préalable à la mise en œuvre d'un traitement de données est devenue résiduelle [...] pour certains traitements de données à caractère personnel dans le domaine de la santé* »¹⁴⁴⁹. En revanche, lorsque le traitement est conforme à une méthodologie de référence homologuée par la CNIL, il peut être mis en œuvre sans autorisation après que son responsable ait attesté de cette conformité auprès de l'autorité de contrôle¹⁴⁵⁰.

440. Avant de s'atteler aux travaux d'analyse des données médicales, le responsable de traitement doit collecter les seules informations nécessaires à la finalité de la recherche, dont la pertinence doit être justifiée au sein d'un protocole scientifique. A cet effet, une base de données de recherche doit être créée conformément aux règles relatives à la protection des données personnelles, dès la conception de ce traitement. Certainement, « *chaque donnée peut être protégée ou non par un droit de propriété intellectuelle et son intégration dans ladite base ne modifie en rien sa situation au regard du régime juridique qui est le sien* »¹⁴⁵¹. L'éventuelle protection du contenu de la base est donc indépendante et s'exerce sans préjudice de celle résultant d'un autre droit sur ses éléments constitutifs¹⁴⁵². Si la base de données de recherche est réservable par le droit *sui generis*, celui-ci n'a aucunement vocation à protéger la création de ses éléments constitutifs, mais uniquement son contenu qualitativement ou quantitativement substantiel¹⁴⁵³. Le droit de propriété intellectuelle possiblement octroyé au producteur d'une base de données n'emporte donc pas l'appropriation des informations qui la composent, lesquelles restent soumises aux règles juridiques qui leur sont spécifiques. Qu'elle donne prise ou qu'elle échappe au droit de la propriété intellectuelle, le producteur de la base de données doit toujours veiller à la licéité de sa constitution et de sa mise à disposition au regard du droit à la protection des données

¹⁴⁴⁸ DOUVILLE (T.), *Droit des données à caractère personnel*, *op. cit.*, p. 110.

¹⁴⁴⁹ *Ibid.*

¹⁴⁵⁰ Article 66.II de la loi Informatique et Libertés modifiée.

¹⁴⁵¹ DESCHANEL (C.), *op. cit.*, § 19.

¹⁴⁵² Article L.341-1 al. 2 du code de la propriété intellectuelle.

¹⁴⁵³ CJCE, 9 novembre 2004, aff. C-46/02, *Fixtures Marketing Ltd.*

personnelles, quand bien même il agirait en qualité de sous-traitant du traitement¹⁴⁵⁴. De la même façon, la mise à disposition de la base de données médicales au profit du responsable de la recherche ne comprend que l'exploitation de son contenu, en l'occurrence les données médicales, pour la réalisation de l'étude scientifique. En d'autres termes, le responsable de la recherche ne peut traiter les données médicales auxquelles il a momentanément accès dans les seules limites du périmètre de l'autorisation octroyée par la CNIL ou, le cas échéant, de la méthodologie de référence à laquelle il a attesté de sa conformité. Le responsable de la recherche est donc l'unique responsable de la conformité du traitement au droit à la protection des données personnelles.

Concrètement, une base de données pseudonymisées doit être constituée pour chaque recherche répondant « à un objectif précis et limité dans le temps »¹⁴⁵⁵. A moins qu'il ne s'agisse d'une « recherche interne »¹⁴⁵⁶, l'organisme qui détient les données médicales du patient¹⁴⁵⁷ les transmet au responsable du traitement, également responsable de la recherche. Pour cela, l'organisme détenteur des données médicales constitue, pour le compte du responsable de la recherche, une base de données pseudonymisées et minimisées à la finalité déterminée dans le protocole scientifique. La constitution de cette base de données de recherche et sa mise à disposition doivent être organisées au sein d'un acte juridique entre le responsable de la recherche et l'organisme détenteur des données médicales, conformément aux dispositions de l'article 28 du RGPD. Ce contrat a pour objet de définir « l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement »¹⁴⁵⁸. Au terme de la durée du traitement, cette base de données de recherche peut être conservée jusqu'à la mise sur le marché du dispositif médical étudié ou jusqu'à deux ans après la dernière publication des résultats de la recherche ou, en cas

¹⁴⁵⁴ Bien que l'opération de traitement consistant en la création d'une base de données de recherche pour le compte du responsable de la recherche est une activité de sous-traitance, il n'empêche que le sous-traitant peut-être le producteur de la base de données.

¹⁴⁵⁵ CNIL, *Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?*, 28 novembre 2019.

¹⁴⁵⁶ Selon la CNIL, une recherche est dite interne lorsqu'elle est menée par à partir de données recueillies dans le cadre du suivi (thérapeutique ou médical) individuel des patients, par les personnels assurant ce suivi et pour leur usage exclusif ; CNIL, *Recherche médicale : quel est le cadre légal ?*, 10 décembre 2018.

¹⁴⁵⁷ Il peut s'agir d'un médecin libéral, d'un établissement de santé ou encore du système national des données de santé.

¹⁴⁵⁸ Article 28.3 du RGPD.

d'absence de publication, jusqu'à la signature du rapport final de la recherche¹⁴⁵⁹. Elle fait ensuite l'objet d'un archivage pour une durée conforme à la réglementation en vigueur jusqu'à sa destruction¹⁴⁶⁰. Après avoir conclu les travaux de recherche, son responsable ne pourra plus réutiliser les données médicales du patient tandis qu'il pourra exploiter les résultats issus de leur analyse.

441. Alors que la réutilisation de la donnée médicale personnelle n'implique jamais son appropriation matérielle ou intellectuelle, ses exploitants disposent d'un droit d'usage éphémère à son égard, pendant la durée de la recherche. A l'instar des choses communes sur lesquelles le législateur a reconnu un droit d'usage régulé par des lois de police¹⁴⁶¹, les données pseudonymisées seraient, elles aussi, accessibles à tout individu qui souhaiterait en faire un usage conformément aux normes juridiques qui les gouvernent. En effet, le traitement des données personnelles « *constitue une activité libre mais réglementée* »¹⁴⁶². Nicolas Ochoa explique que cette activité « *fait l'objet d'une police administrative spéciale, ce qui signifie que la liberté de traiter des données personnelles se trouve autant consacrée qu'amputée préventivement de certains de ses aspects, dans le but de protéger la société contre les effets potentiellement néfastes de son exercice* »¹⁴⁶³. D'une certaine façon, les données médicales personnelles pourraient intégrer le domaine commun informationnel aux côtés des données médicales anonymisées¹⁴⁶⁴. En effet, « *le « propre » de la donnée prise en tant qu'information est d'être commune ; sa destination naturelle, chose non rivale par essence, est d'être librement partagée* »¹⁴⁶⁵. A l'instar des données de référence et des données d'intérêt général, la donnée médicale pourrait être observée comme une donnée stratégique dont le rôle particulier dans la création de valeur économique et sociale

¹⁴⁵⁹ CNIL, Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004), *JORF* n°0160, 13 juillet 2018, texte n° 110.

¹⁴⁶⁰ *Ibid.*

¹⁴⁶¹ Cf. Paragraphe 375.

¹⁴⁶² OCHOA (N.), *op. cit.*, p. 1157.

¹⁴⁶³ *Ibid.*

¹⁴⁶⁴ Cf. Paragraphe 376.

¹⁴⁶⁵ BENABOU (V.-L.), « *Création* » collaborative et données, In ROBIN (A.), *La propriété intellectuelle en partage*, Dalloz, octobre 2020, p. 53.

emporterait sa circulation¹⁴⁶⁶. Finalement, la chose anthropomorphique serait généralement considérée comme un commun numérique dont l'usage au profit de tous serait accordé en considération des règles spécifiques à leur nature pseudonymisée ou anonymisée¹⁴⁶⁷.

442. En revanche, l'exploitant de la donnée médicale ne détient aucun droit aux fruits à son égard. L'élément immatériel du corps humain du patient est une information factuelle relative à ses conditions physiques, psychiques et biologiques¹⁴⁶⁸. Cette chose incorporelle ne fournit donc aucun bien périodique, pas même à l'aide de l'activité de l'homme. Son traitement à des fins de recherche ou d'innovation dans le domaine de la santé ne permet guère d'obtenir de fruits naturels, industriels ou civils mais uniquement de produire des résultats inhérents à l'analyse de l'homme ou, le cas échéant, de l'informatique. Or, « *si un bien nouveau existait à la suite d'une pure activité humaine, on ne pourrait pas le qualifier de fruits* »¹⁴⁶⁹. Ainsi, les résultats de la recherche ne constituent pas un fruit produit par la donnée médicale mais, possiblement, une œuvre intellectuelle ou une innovation industrielle distincte de celle-ci.

Par ailleurs, le titulaire des droits de propriété intellectuelle sur ces résultats peut récolter les fruits périodiques provenant de leur exploitation. En effet, les bénéfices issus de l'exploitation d'un droit de propriété intellectuelle sont qualifiés de fruits¹⁴⁷⁰. Autrement dit, le profit économique généré grâce au traitement de la donnée médicale extrapatrimoniale ne constitue pas un fruit provenant de l'essence de cette chose anthropomorphique, mais un revenu provenant de l'exploitation des résultats de la recherche. Compte tenu de ce qui précède, il apparaît alors essentiel de distinguer le droit d'usage de la donnée médicale de l'éventuel droit aux fruits des résultats de son traitement. Assurément, « *une restriction [au droit d'usage] supplémentaire existe pour les données personnelles qui retombent dans la catégorie des données de santé, pour lesquelles le principe d'indisponibilité s'accompagne*

¹⁴⁶⁶ CLUZEL-METAYER (L.), *La loi pour une République numérique : l'écosystème de la donnée saisi par le droit*, loc. cit.

¹⁴⁶⁷ En revanche, « on ne saurait pour autant considérer les données personnelles comme un res communis » dans la mesure où « le sens profond des qualificatifs « commun », d'une part, « personnel », d'autre part, qui caractérisent ici l'information s'oppose à une telle inclinaison. ». NONNOU (Enagnon Gildas), *La patrimonialité des données personnelles*, La revue Lexbase Afrique-OHADDA, n°38, 12 novembre 2020.

¹⁴⁶⁸ Cf. Paragraphe 15.

¹⁴⁶⁹ PIEDELIÈVRE (S.), *Fruits*, Répertoire de droit civil, octobre 2014, § 15.

¹⁴⁷⁰ PIEDELIÈVRE (S.), *op. cit.*, § 9.

de l'interdiction de procéder à une cession ou à une exploitation commerciale des données »¹⁴⁷¹. En dépit de son droit d'usage, l'exploitant de la donnée médicale extrapatrimoniale n'en apparaît pas l'usufruitier. Certainement, « le droit de jouissance de l'usufruitier se compose de l'usus (droit d'usage) et du fructus (droit d'en percevoir les fruits) »¹⁴⁷² ; et le fructus constitue « la prérogative essentielle de l'usufruitier, permettant de le distinguer du simple usager »¹⁴⁷³. Néanmoins, l'exercice du droit d'usage peut engendrer des droits qui lui sont supplémentaires¹⁴⁷⁴. Ainsi, le simple utilisateur de la donnée médicale bénéficierait, en quelque sorte, du droit de tirer profit de l'utilisation de cette chose extrapatrimoniale, conformément à l'usage qui lui est légalement concédé.

Pendant que le responsable du traitement use des données médicales du patient et génère des bénéfices à partir de leur réutilisation, qu'en est-il de la compensation économique allouée à la personne à laquelle elles sont intimement rattachées ?

Section 2: La valorisation économique de la participation du patient au traitement de ses données médicales

443. *A priori*, l'absence de conception patrimoniale des éléments immatériels du corps humain du patient ne semble pas dresser un obstacle à la reconnaissance de la composante économique inhérente aux attributs des droits de la personnalité¹⁴⁷⁵. Pour autant, le patient pourrait-il exploiter économiquement la réutilisation de ses données médicales ? Cette perspective supposerait que le patient puisse en devenir l'usufruitier (**Paragraphe 1**). Cependant, tout rapport marchand à la donnée médicale s'avère contraire au statut juridique que nous lui concédons. En effet, son extra-économité partielle et son exclusion du marché s'opposent à ce qu'elle ne devienne l'objet d'un acte juridique conclu à titre onéreux. Mais alors, comment « organiser un retour de la valeur vers ceux qui en sont la source »¹⁴⁷⁶ ? Si

¹⁴⁷¹ BOURCIER (D.), DE FILIPPI (P.), *op. cit.*, p. 448.

¹⁴⁷² MERCIER (V.), : *USUFRUIT . – Prérogatives de l'usufruitier . – Droits de l'usufruitier (usage et jouissance)*, JurisClasseur Civil, Fasc. 10, juillet 2019, § 4.

¹⁴⁷³ MERCIER (V.), *op. cit.*, § 6.

¹⁴⁷⁴ Dans une décision n° 2000-434 DC du 20 juillet 2000, cons. 24, le Conseil Constitutionnel a considéré que « le droit de chasse sur un bien foncier se rattache au droit d'usage de ce bien ».

¹⁴⁷⁵ Cf. Paragraphe 450.

¹⁴⁷⁶ Commission nationale consultative des droits de l'homme, *Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique*, *JORF*, 3 juin 2018, § 32.

le patient ne peut détenir de créance à l'encontre de l'exploitant de sa donnée médicale en contrepartie de sa mise à disposition, le patient pourrait éventuellement détenir une créance à l'encontre de la collectivité. En effet, l'exploitation des données médicales à des fins de recherche et d'innovation en santé ne peut être mise en œuvre qu'en considération d'un motif d'intérêt public. Par conséquent, leur traitement profiterait davantage à la collectivité qu'au responsable de traitement ou au titulaire de droits sur la création intellectuelle qui en résulte (**Paragraphe 2**).

Paragraphe 1 : L'absence d'usufruit sur les données médicales personnelles

444. Compte tenu du statut que nous réservons à la donnée médicale personnelle, le patient ne pourrait en devenir que l'usufruitier. A l'évidence, l'extrapatrimonialité de la chose anthropomorphique personnelle ou anonyme exclut toute possibilité d'en disposer. Si la personne concernée ne peut bénéficier d'un *abusus* sur celle-ci, encore faut-il qu'elle puisse en détenir l'*usus* et le *fructus* pour en concevoir l'usufruit. D'une part, si le patient contrôle l'usage de ses données médicales grâce aux droits qu'il détient sur celles-ci, il semble que l'*usus* soit davantage concédé au responsable de leur traitement (**A**). D'autre part, à défaut d'objet frugifère et à raison de l'exclusion de la donnée médicale du marché, le patient concerné ne peut en récolter les fruits naturels, civils ou industriels (**B**). En conséquence, le patient ne peut finalement posséder l'usufruit des éléments immatériels de son corps humain.

A) Le défaut d'usus

445. La protection et la réservation des données médicales personnelles du patient ne sont pas assurées au moyen d'un droit de propriété sur celles-ci, mais grâce à l'autodétermination informationnelle de la personne concernée¹⁴⁷⁷. Ce principe lui garantit la maîtrise de ses informations confidentielles en dehors de toute conception patrimoniale. Un courant doctrinal considère que cette autodétermination informationnelle représente « *un objectif permettant d'offrir une véritable protection des données personnelles tout en prolongeant une protection construite autour de l'individu* »¹⁴⁷⁸. Vraisemblablement, si les patients avaient la possibilité d'en disposer, ils « *n'auraient plus le droit de contrôler l'exploitation*

¹⁴⁷⁷ Cf. Paragraphe 387.

¹⁴⁷⁸ ANCIAUX (A.), FARCHY (J.), *op. cit.*, p.312.

qui est faite de leurs données, même si ces utilisations [allaient] à l'encontre de leur dignité »¹⁴⁷⁹. Ce droit de contrôle, consacré au premier article de la loi Informatique et Libertés modifiée, est concrétisé par l'ensemble des droits que la personne concernée détient sur ses données à caractère personnel. Le pouvoir que le patient détient sur les informations médicales qui le concernent est donc de nature juridique et correspond aux droits de la personnalité appartenant à tout individu. Pour dire les choses autrement, la chose anthropomorphique à caractère personnel est un objet de droit rattaché au patient qui en contrôle les usages. Toutefois, « *l'impossible aliénation des informations médicales ne saurait interdire, dans son régime de réservation, certaines caractéristiques essentielles de la propriété* »¹⁴⁸⁰. Alors que pour certains auteurs la personne concernée bénéficie effectivement d'un « droit d'*usus* » sur ses données personnelles¹⁴⁸¹, l'autodétermination informationnelle, objectivée par les droits qu'elle détient sur celles-ci, lui est-elle assimilable ?

446. Davantage utilisé en matière successorale, l'*usus* est un droit réel subjectif qu'une personne détient temporairement sur un bien, au plus tard jusqu'à son décès. Il consiste à utiliser et à se servir de la chose conformément à l'usage auquel elle est destinée¹⁴⁸². Si le patient disposait d'un *usus* sur ses données médicales personnelles, il pourrait probablement les utiliser librement pour diverses finalités dans sa vie personnelle comme dans la sphère professionnelle. En apparence, il semble logique que le patient puisse user de ses données médicales personnelles comme bon lui semble. Pourtant, il convient de distinguer leurs usages privés de leurs usages professionnels, même lorsque le traitement est mis en œuvre par la personne concernée. Dans l'hypothèse où elle procède d'un usage domestique, l'utilisation des données personnelles par la personne concernée n'est pas juridiquement encadrée. Certainement, le droit à la protection des données personnelles ne s'applique pas lorsque le traitement est mis en œuvre « *par une personne physique au cours d'activités strictement personnelles ou domestiques* »¹⁴⁸³. Dans le domaine privé, les informations relatives à une personne physique peuvent être utilisées par tout individu, dans le respect de

¹⁴⁷⁹ BOURCIER (D.), DE FILIPPI (P.), *op. cit.*, p. 447.

¹⁴⁸⁰ MOUSSERON (J.-M.), RAYNARD (J.), REVET (T.), *De la propriété comme modèle*, In Mélanges offerts à André Colomer, 1993, p. 281.

¹⁴⁸¹ Voir : MATTATIA (F.), YAÏCHE (M.), *loc. cit.*

¹⁴⁸² Article 589 du code civil.

¹⁴⁸³ Considérant 18 du RGPD.

l'intimité de la vie privée, pour un usage dépourvu de lien avec une activité professionnelle ou commerciale¹⁴⁸⁴. En revanche, au cas où la personne concernée souhaitait utiliser ses propres informations personnelles dans un cadre professionnel, elle aurait la qualité de responsable de traitement et devrait, malgré tout, satisfaire à l'ensemble des obligations édictées par les normes juridiques relatives à la protection de données. En tant que « droit d'usage », l'*usus* se rapporte donc au droit de traiter les données à caractère personnel. Par conséquent, lorsque le patient a la qualité de personne concernée par la réutilisation de ses données médicales personnelles, l'*usus* est légalement exercé par un tiers exploitant. Le cas échéant, le patient dispose-t-il d'un *usus* manifesté par son autodétermination informationnelle sur les données médicales exploitées ?

447. Tandis que les organismes jouissent du droit d'utiliser les données médicales personnelles du patient en vertu des principes énoncés par les lois de police¹⁴⁸⁵, le patient jouit d'une autodétermination informationnelle sur ces informations réutilisées. Cette autodétermination informationnelle résulte des droits qui lui sont octroyés par le RGPD et relève de la catégorie des droits de la personnalité. Comme le soulève Agathe Lepage, l'ensemble des « *droits de la personnalité ont une structure commune qui est celle d'un droit de contrôle* »¹⁴⁸⁶. Cette fonction est corroborée par la lettre du deuxième alinéa du premier article de la loi Informatique et Liberté. En effet, il y est énoncé que « *les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant [...] s'exercent dans le cadre* » du droit à la protection des données. L'emploi de la voie passive signifie que le sujet ne réalise pas l'action mais la subit. Effectivement, l'initiative du traitement et la détermination de sa finalité et de ses moyens reviennent à son responsable. La personne concernée n'intervient qu'*a posteriori* par l'exercice des prérogatives qu'elle peut potentiellement exercer sur ses données médicales personnelles, en fonction de leur nature nominative ou pseudonymisée d'une part¹⁴⁸⁷, et de la base légale du

¹⁴⁸⁴ *Ibid.*

¹⁴⁸⁵ Cf. Paragraphe 439.

¹⁴⁸⁶ LEPAGE (A.), *op. cit.*, § 22.

¹⁴⁸⁷ Lorsque la donnée médicale est nominative, le patient, en tant que titulaire du secret médical, peut s'opposer à leur réutilisation (article 74 de la loi Informatique et Libertés modifiée). Cependant, lorsque la donnée médicale est pseudonymisée, et que les atteintes au respect de la vie privée sont dissipées, le droit de contrôle de son usage est conditionné par la base légale du traitement.

traitement d'autre part¹⁴⁸⁸. Ainsi, les droits du patient sur ses données médicales personnelles lui permettent de relativement maîtriser et de contrôler les usages qui en sont faits par le responsable de traitement. En conséquence, le droit d'usage du responsable de traitement est exercé sous le contrôle de la personne concernée. Il apparaît donc que l'autodétermination informationnelle correspond davantage au droit de maîtriser et de contrôler l'utilisation de ses données personnelles qu'au droit d'en user. Il en résulte que « *le lien entre la personne et ses données nominatives est forgé autour de sa dignité et induit des prérogatives spécifiques, qui encadrent l'activité informatique sans toutefois l'entraver* »¹⁴⁸⁹. Ainsi, l'autodétermination informationnelle ne consiste pas en un droit d'utiliser la chose. Certainement, si l'*usus* comprenait la maîtrise des données médicales personnelles, le responsable de traitement, bénéficiaire d'un droit d'usage, pourrait concurrencer le patient en exerçant des prérogatives sur ses données médicales personnelles. Or, ces prérogatives sont spécifiques aux droits de la personnalité attachés à un individu particulier. Hormis l'*usus* qui leur est légalement concédé, les exploitants des données médicales personnelles ne disposent d'aucun droit subjectif sur ces dernières. L'autodétermination informationnelle ne peut donc être assimilée à un *usus* sur les données médicales personnelles. Assurément, le droit de contrôle de l'usage ne doit pas être confondu avec un droit d'usage.

448. Nous l'avons bien compris, la donnée médicale extrapatrimoniale, lorsqu'elle est à caractère personnel, est rattachée au patient par l'effet de droits extrapatrimoniaux. Certainement, la donnée médicale réifie le corps humain du patient et en devient un élément immatériel. En raison du lien particulièrement intime qui les unit, la réservation de la donnée médicale personnelle par le patient au moyen d'un rapport de propriété se révèle donc inutile. Incontestablement, « *la reconnaissance d'un droit de propriété de l'individu impliquerait en réalité de renoncer largement à la logique de protection* »¹⁴⁹⁰. Toutefois, s'il « *n'est certainement pas souhaitable que l'individu, par l'exercice du droit d'aliénation attaché au*

¹⁴⁸⁸ Tous les droits de la personne concernée n'ont pas toujours vocation à s'appliquer puisque l'exercice de certains de ses droits est conditionné par la base légale du traitement. Pour mémoire, la base légale correspond à l'un des fondements juridiques prévues à l'article 6 du RGPD sur lequel repose la licéité du traitement mis en œuvre. Lorsque la base légale du traitement repose sur le consentement de la personne concernée, celle-ci peut décider de l'emploi de ses données à caractère personnel. En revanche, lorsque le traitement est fondé sur une autre base légale, la personne concernée bénéficie, au plus, du pouvoir de s'opposer au traitement. Le contrôle des usages de ses données personnelles apparaît donc, selon les cas, nuancé et limité.

¹⁴⁸⁹ CORNU (M.), ORSI (F.), ROCHFELD (J.), *loc. cit.*

¹⁴⁹⁰ CE, *Le numérique et les droits fondamentaux*, *op. cit.*, p. 266.

droit de propriété, renonce à toute protection sur ses données personnelles [...] on peut envisager des démembrements du droit de propriété »¹⁴⁹¹. Bien que le patient, en qualité de personne concernée, ne semble pouvoir détenir un *usus* sur ses données médicales personnelles, peut-il jouir d'un *fructus* à leur égard ?

B) Le défaut de fructus

449. Dans une thèse dédiée à la propriété des données de santé, Mathilde Cavalier a signalé que « *dans le cas des données personnelles et des données personnelles de santé, il est évident qu'il existe une asymétrie de prérogatives, en l'espèce le fructus, entre les collecteurs [des données] et les personnes [concernées]* »¹⁴⁹². Compte tenu de ce déséquilibre, l'auteur s'est interrogée de savoir si le patient pouvait « *tirer les fruits de ses données personnelles de santé* »¹⁴⁹³, pour finalement conclure que « *la théorie et les fondements des droits de la personnalité semblent empêcher que cela se produise* »¹⁴⁹⁴.

450. Pourtant, les droits de la personnalité revêtent indissociablement une composante économique en complément de leur aspect moral. En effet, « *le rapport de droit de l'individu sur ses informations est un droit de la personnalité, en dépit même de l'existence d'attributs pécuniaires car ils sont accessoires et ne reposent pas sur la propriété* »¹⁴⁹⁵. En d'autres termes, les éventuels attributs pécuniaires des droits de la personnalité coïncident avec leur nature extrapatrimoniale dans la mesure où ils ne reposent pas sur un droit de propriété mais résultent d'un rapport personnaliste¹⁴⁹⁶. L'extrapatrimonialité de la chose anthropomorphique ne ferait donc pas obstacle à la reconnaissance de son versant économique au seul bénéficiaire du patient concerné. Du fait de cette dualité, maître Cyril Carrière invoque que « *le droit de la personne sur ses informations (nous incluons les informations médicales) devrait s'élaborer sur la base du droit à l'image* »¹⁴⁹⁷. La

¹⁴⁹¹ CE, *Le numérique et les droits fondamentaux*, op. cit., p. 265.

¹⁴⁹² CAVALIER (M.), op. cit., p. 128.

¹⁴⁹³ *Ibid.*

¹⁴⁹⁴ *Ibid.*

¹⁴⁹⁵ CORNU (M.), ORSI (F.), ROCHFELD (J.), loc. cit.

¹⁴⁹⁶ ANTIPPAS (J.), op. cit., p. 36.

¹⁴⁹⁷ CARRIÈRE (C.), *Le droit au secret médical : de la personne à la chose en passant par la propriété*, RDS, 2007, n°20, p. 718 à p. 719.

considération de la dimension économique des droits de la personnalité permettrait donc, à la personne concernée, de tirer profit des utilités économiques de la chose qui lui est ainsi affectée en dépit de toute patrimonialité¹⁴⁹⁸.

Dès lors, le patient devrait disposer du contrôle intégral de ses données médicales personnelles par la maîtrise de l'ensemble de leurs aspects, qu'ils soient moraux ou économiques. D'une certaine manière, l'autodétermination informationnelle de la personne concernée comprendrait également le pouvoir de jouir des utilités économiques des informations qui la concernent. Assurément, « *l'individu ne dispose pas de ses informations mais peut en exploiter l'usage, par le biais d'autorisations expresse* »¹⁴⁹⁹. Si la donnée médicale était frugifère, alors la théorie des droits de la personnalité n'empêcherait pas que le patient puisse en percevoir les fruits. Bien au contraire, eu égard aux droits de la personnalité, les fruits générés par la chose anthropomorphique à caractère personnel ne seraient qu'attribués au patient intéressé. Seulement, par essence, la donnée médicale ne produit aucun fruit naturel ni aucun fruit industriel, tous deux considérés comme des fruits par nature¹⁵⁰⁰. Par ailleurs, le patient pourrait-il percevoir des fruits civils produits par la mise à disposition onéreuse de ses données médicales personnelles au profit d'un responsable de traitement à des fins de recherche et d'innovation dans le domaine de la santé ?

451. Dans un ouvrage consacré au droit des biens, Nadège Reboul-Maupin explique que le droit de jouir de la chose se décline de deux manières : d'une part, par le droit sur les fruits de la chose et, d'autre part, par la réalisation d'actes matériels et juridiques sur la chose¹⁵⁰¹. S'agissant des actes accomplis sur la chose, ils ont principalement vocation à concrétiser le droit de jouissance en permettant la perception de fruits « *obtenus grâce à un contrat dont le capital est l'objet* »¹⁵⁰². Ainsi, la perception des fruits civils, définis comme les « *revenus en argent procurés par une chose* »¹⁵⁰³ au moyen d'un contrat, est objectivée par la réalisation d'actes juridiques sur la chose, tels que la conclusion d'un bail sur une chose entraînant la

¹⁴⁹⁸ LEPAGE (A.), *op. cit.*, § 141 ; REVET (T.), *Le corps humain est-il une chose appropriée ?*, RTD civ., 2017, n° 03, p. 587.

¹⁴⁹⁹ CORNU (M.), ORSI (F.), ROCHFELD (J.), *loc. cit.*

¹⁵⁰⁰ PIEDELIÈVRE (S.), *Fruits, op. cit.*, § 31.

¹⁵⁰¹ REBOUL-MAUPIN (N.), *op. cit.*, p. 571.

¹⁵⁰² GUINCHARD (S.), DEBARD (T.), *op. cit.*, p. 508.

¹⁵⁰³ *Ibid.*

perception de loyers ou encore la conclusion d'un droit d'usage et d'habitation¹⁵⁰⁴. Pour reformuler la question soumise à notre étude, s'il apparaît que l'individu puisse exploiter ses informations personnelles sans qu'il n'y ait ni dépossession, ni disposition¹⁵⁰⁵, peut-il conclure des actes juridiques ayant pour objet sa donnée médicale personnelle afin de dégager des fruits civils ? De la même façon qu'un mannequin peut économiquement concéder l'utilisation de son image en la mettant à disposition d'un photographe pour la création d'une œuvre artistique¹⁵⁰⁶, le patient pourrait-il percevoir une contrepartie financière à la mise à disposition de ses données médicales personnelles ?

452. Théoriquement, la nature extrapatrimoniale de la chose anthropomorphe ne s'oppose pas à ce que le patient puisse recevoir une rémunération en contrepartie de sa mise à la disposition d'un responsable de traitement. En effet, « *le caractère extrapatrimonial, consubstantiel à la notion de droits de la personnalité, ne semble [...] pas remis en question lorsque ceux-ci sont utilisés ou invoqués à des fins économiques* »¹⁵⁰⁷. Toutefois, si l'extrapatrimonialité n'emporte pas l'extracommercialité de la donnée médicale personnelle, nous proposons de l'exclure du marché afin qu'elle ne puisse pénétrer aucun circuit économique¹⁵⁰⁸. Plus largement que l'interdiction de céder les données médicales personnelles à titre onéreux posée à l'article L.1111-8 VII du code de la santé publique, son exclusion du marché interdirait au patient d'exercer le monopole d'exploitation de l'aspect économique de ses droits de la personnalité. Ni le responsable de traitement, ni le patient ne pourraient alors conclure d'opération économique portant sur la donnée médicale personnelle. En conséquence, le patient ne pourrait licitement récolter les fruits civils des éléments immatériels de son corps. Certainement, leur perception nécessite la conclusion d'un acte juridique à titre onéreux. Or, « *une chose peut être soustraite aux rapports marchands sans échapper, de façon générale, au commerce juridique dès lors qu'il est possible d'en disposer à titre gratuit* »¹⁵⁰⁹. De cette manière, les patients seraient

¹⁵⁰⁴ REBOUL-MAUPIN (N.), *op. cit.*, p. 575.

¹⁵⁰⁵ CARRIERE (C.), *loc. cit.*

¹⁵⁰⁶ Civ. 1^{ère}, 11 décembre 2008, n°07-19.494, Bull. civ., I, n° 282 ; JCP G, 2009, n° 07, jur. II. 10025, note G. Loiseau ; Légipresse 2009, III, p. 109, note Th. Roussineau ; CCC, 2009, n° 03, comm. 68, obs. L. Leveneur ; RTD civ., 2009, n° 02, p. 342, obs. T. Revet, supra p. 295, obs. J. Hauser.

¹⁵⁰⁷ ANTIPPAS (J.), *op. cit.*, p. 36.

¹⁵⁰⁸ Cf. Paragraphes 361 s.

¹⁵⁰⁹ LOISEAU (G.), *Typologie des choses hors du commerce, op. cit.*, § 12.

définitivement protégés des dérives suscitées par la potentielle économicité de leur chose anthropomorphique¹⁵¹⁰.

453. Par surcroît, si la donnée médicale personnelle est mise à la disposition de son exploitant par la personne physique ou morale qui en a la garde¹⁵¹¹, c'est parce que l'exploitant est titulaire d'un droit d'usage d'origine légale à son égard¹⁵¹². Le droit de réutiliser les données médicales personnelles à des fins de recherche ou d'innovation dans le domaine de la santé n'est assurément pas conféré par les patients concernés¹⁵¹³. Autrement dit, la permission de traiter les données médicales du patient ne résulte pas d'une volonté contractuelle, *a fortiori* lorsque le traitement poursuit une finalité de recherche et d'innovation dans le domaine de la santé, et quand bien même un acte juridique doit, le cas échéant, en régir la sous-traitance¹⁵¹⁴. Partant, le gardien des données médicales personnelles, qui ne dispose d'aucun droit sur celles-ci, aurait-il l'obligation de les transmettre à l'organisme légalement autorisé à les traiter ? D'ailleurs, les données médicales personnelles pourraient rejoindre le domaine commun informationnel¹⁵¹⁵ afin d'être partagées pour accroître le développement des projets présentant un motif d'intérêt général, en particulier dans le domaine de la santé, dans le respect du droit à la protection des données personnelles.

A l'instar du service public de la donnée¹⁵¹⁶, le domaine commun informationnel aurait vocation à regrouper l'ensemble des données médicales pseudonymisées et anonymisées produites à l'occasion de toute activité sanitaire indépendamment du secteur de prise en charge ou des modalités de financement des actes¹⁵¹⁷. A cet effet, leur regroupement et leur mise à disposition pourrait être gérés et administrés par une entité étatique ou d'intérêt

¹⁵¹⁰ Cf. Paragraphe 466.

¹⁵¹¹ La personne physique ou morale qui met les données médicales personnelles à disposition du responsable de traitement peut être tout titulaire ou dépositaire du secret médical. Il peut s'agir du patient lui-même, d'un établissement de santé, d'un professionnel de santé libéral ou encore de la plateforme nationale des données de santé.

¹⁵¹² Cf. Paragraphe 439.

¹⁵¹³ Cf. Paragraphe 477.

¹⁵¹⁴ Cf. Paragraphe 490.

¹⁵¹⁵ Cf. Paragraphe 376.

¹⁵¹⁶ CLUZEL-METAYER (L.), *La construction d'un service public de la donnée*, Revue française d'administration publique, 2018, n°167, p. 494.

¹⁵¹⁷ Cf. Paragraphe 545.

public¹⁵¹⁸, à l'exemple du Health Data Hub. En raison de ce qui précède, même si la donnée médicale personnelle n'était pas exclue du marché, sa réutilisation pour une finalité secondaire à la prise en charge sanitaire ne pourrait être octroyée par le patient au moyen d'un prêt à usage temporaire concédé à titre onéreux.

454. En tout état de cause, la valorisation financière des données personnelles au profit de la personne concernée aurait été illusoire et la production de fruits civils dérisoire. En effet, la valeur économique d'une donnée à caractère personnel ne correspond qu'à quelques centimes d'euros¹⁵¹⁹ alors que le profit généré par leur exploitation peut en atteindre des centaines de milliers¹⁵²⁰. Il en résulte que « *les initiatives qui ont fleuri jusqu'à présent pour permettre à un individu de valoriser « ses » données lorsque celles-ci sont employées par des tiers montrent leurs limites puisque, le plus souvent, les coûts de transaction sont hors de proportion avec le bénéfice qui serait retiré de l'opération* »¹⁵²¹. Véritablement, si la donnée médicale présente une utilité économique, ce n'est qu'indirectement grâce aux résultats dégagés à l'issue de son traitement, eux-mêmes source de financements et de revenus¹⁵²². Les attributs de la personnalité « *ne sont pas en eux-mêmes dotés d'une valeur pécuniaire* »¹⁵²³. Néanmoins, en tant que « matière première » l'usage que le chercheur ou l'innovateur en fait peut créer de la valeur économique.

L'asymétrie entre le profit généré grâce à l'exploitation des résultats du traitement des données médicales et l'absence de contrepartie octroyée à la personne concernée demeure. Afin de résoudre ce déséquilibre, il conviendrait plus justement de se demander si le patient pourrait obtenir une part du profit généré grâce à leur exploitation.

¹⁵¹⁸ CLUZEL-METAYER (L.), *La construction d'un service public de la donnée*, *op. cit.*, p. 492.

¹⁵¹⁹ *Ibid.*

¹⁵²⁰ *Cf.* Paragraphe 435.

¹⁵²¹ BENABOU (V.-L.), *op. cit.*, p. 66.

¹⁵²² *Cf.* Paragraphes 417 à 437.

¹⁵²³ CARRIERE (C.), *op. cit.*, p. 718.

Paragraphe 2 : Le patient créancier à l'égard de la collectivité

455. En livrant la ressource essentielle à la recherche rétrospective dans le domaine de la santé, le patient contribue manifestement au processus de l'innovation sanitaire. Seulement, cette participation ne peut être reconnue sur le plan de la propriété intellectuelle (A). En effet, si le patient est un maillon de la chaîne de l'innovation en santé, il n'est en aucun cas l'auteur des résultats de la recherche ou le créateur du bien incorporel qui en provient. En conséquence, le patient ne peut profiter de la valorisation économique des résultats du traitement de ses données médicales personnelles. Toutefois, il n'en demeure pas moins que le patient apporte effectivement son concours aux progrès sanitaires à travers les éléments immatériels de son corps humain. Tandis qu'« *il semble [...] légitime de considérer que chaque personne versant sa contribution informationnelle dans un ensemble, parce qu'elle contribue à la création de la valeur économique de ce fonds, est légitime à en demander une juste part* »¹⁵²⁴, il apparaît naturellement juste de récompenser le patient pour cet acte civique d'intérêt général (B).

A) *La participation ignorée à un processus créatif*

« *Le droit positif de la propriété intellectuelle permet-il l'appréhension de l'œuvre créée de manière collaborative ?* »¹⁵²⁵.

456. En fournissant la ressource essentielle à la recherche et à l'innovation en santé, le patient contribue tant au progrès médical et à l'amélioration de la qualité des soins de santé, des médicaments et des dispositifs médicaux, qu'au développement économique du secteur sanitaire. En effet, le patient représente le premier maillon de la chaîne de l'innovation médicale. D'abord, les éléments immatériels de son corps humain sont traités afin, ensuite, de produire des résultats qui seront, finalement, exploitables et valorisables par le titulaire des droits de propriété intellectuelle. C'est ainsi que les résultats du traitement des données médicales du patient peuvent offrir des bénéfices financiers au profit de la personne physique ou morale qui les exploite. En fin de compte, il s'avère que la propriété incorporelle des

¹⁵²⁴ BENABOU (V.-L.), *op. cit.*, p. 66.

¹⁵²⁵ MARTIAL-BRAZ (N.), *Création et économie collaborative : quelle régulation ?*, In ROBIN (A.), *La propriété intellectuelle en partage*, Dalloz, octobre 2020, p. 22.

résultats du traitement des données médicales du patient ne lui revient pas¹⁵²⁶. Certainement, le droit de la propriété intellectuelle a principalement vocation à assurer un retour sur l'investissement engagé par le créateur d'une œuvre littéraire et artistique ou d'une innovation industrielle. Néanmoins, en tant que contributeur au développement de la recherche et de l'innovation dans le domaine de la santé, le patient pourrait-il percevoir un pourcentage des fruits produits grâce à l'exploitation des résultats du traitement de ses données médicales ?

L'utilité économique de la donnée médicale ne provient guère de sa valeur pécuniaire mais de son traitement par un exploitant. Tandis que cette chose anthropomorphique ne peut jamais être l'objet d'une valorisation financière, le responsable de traitement peut tirer profit des biens incorporels créés à partir de son exploitation¹⁵²⁷. Autrement dit, la donnée médicale comporte une utilité économique indirecte étant donné que cette ressource essentielle permet d'élaborer des choses nouvelles et de nature patrimoniale. S'il apparaît équitable et légitime de partager les fruits issus des biens incorporels procréés à partir de l'exploitation des éléments immatériels du corps humain du patient, il convient de déterminer dans quelle hypothèse ce dernier pourrait-il détenir des droits patrimoniaux sur ceux-ci. En d'autres termes, le patient pourrait-il jouir d'un droit aux fruits sur les bénéfices produits par l'œuvre ou l'innovation donnant prise au droit de la propriété intellectuelle¹⁵²⁸ ?

457. Le patient pourrait posséder des droits patrimoniaux sur les résultats du traitement de ses données médicales s'il avait participé à la création de l'œuvre ou de l'innovation. Cette solution semble *a priori* envisageable dans la mesure où le bien incorporel, procréé à partir des résultats de la recherche, résulte fréquemment d'une création commune. Le cas échéant, le patient contribue-t-il à l'œuvre plurale par la seule fourniture de la matière première essentielle ?

¹⁵²⁶ Sur l'absence de partage de la valeur de l'économie numérique, voir : BENABOU (V.-L.) et ROCHFELD (J.), *A qui profite le clic ? : le partage de la valeur à l'ère numérique*, Odile Jacob, 2015.

¹⁵²⁷ Cf. Paragraphes 417 à 437.

¹⁵²⁸ Cf. Paragraphe 442.

En premier lieu, l'œuvre de collaboration est définie comme « *l'œuvre à la création de laquelle ont concouru plusieurs personnes physiques* »¹⁵²⁹. Le concours à la création exige que la personne physique, pour être qualifiée d'auteur, ait activement participé à la mise en forme de l'œuvre et que sa contribution soit originale. Seulement, l'apport de données médicales personnelles ne peut être assimilé à un apport créatif et original. En effet, la donnée médicale ne peut être qualifiée d'œuvre de l'esprit¹⁵³⁰. De surcroît, l'œuvre de collaboration suppose une concertation préalable de l'ensemble des auteurs¹⁵³¹. André Lucas signale que cette « *condition n'est pas remplie si les rôles sont répartis et la partie artistique expressément réservée à l'un des contributeurs* »¹⁵³². Dans le cas du traitement des données médicales à des fins de recherche et d'innovation dans le domaine de la santé, le patient ne fournit aucune œuvre artistique et ne participe pas, de façon concertée, à l'analyse scientifique des données conduisant aux conclusions originales en réponse à la problématique posée. Par conséquent, le patient est exclu de la propriété commune des coauteurs de l'œuvre de collaboration.

En deuxième lieu, l'œuvre collective consiste en une « *œuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom* »¹⁵³³ et qui « *est investie des droits de l'auteur* »¹⁵³⁴. Si le patient avait pu être qualifié de contributeur, par la fourniture de ses données médicales, au nouveau bien incorporel créé collectivement, aucune rémunération ni aucun bénéfice n'auraient donc pu lui être octroyés. À l'identique, le patient ne devient pas l'inventeur d'une création industrielle par le simple apport de la matière première. Il en résulte que le patient ne peut jamais détenir aucun droit de propriété intellectuelle sur la création résultant du traitement de ses données médicales personnelles¹⁵³⁵.

¹⁵²⁹ Article L.113-2 alinéa 1 du code de la propriété intellectuelle.

¹⁵³⁰ Cf. Paragraphes 397 à 401.

¹⁵³¹ Civ. 1^{ère}, 18 octobre 1994, n° 92-17.770, Bull. civ., I., n° 298 ; RIDA, 1995, n° 04, p. 305, note A. Latreille.

¹⁵³² LUCAS (A.), *Synthèse - Objet du droit d'auteur. Titulaires du droit d'auteur*, JurisClasseur Propriété Littéraire et Artistique, 01 avril 2021, § 16.

¹⁵³³ Article L.113-2 alinéa 3 du code de la propriété intellectuelle.

¹⁵³⁴ Article L.113-5 du code de la propriété intellectuelle.

¹⁵³⁵ Sauf, évidemment, à ce qu'il prenne effectivement part aux travaux de recherche dans le domaine de la santé en raison de ses qualités professionnelles ou que le titulaire des droits de propriété intellectuelle sur la création incorporelle ne lui cède les droits patrimoniaux.

Certainement, il convient de distinguer les outils ayant permis la production de l'œuvre de la création qui en résulte¹⁵³⁶. Bien que les rapports entre une création intellectuelle et son support matériel ou les moyens techniques de son élaboration puissent être ambigus¹⁵³⁷, le bien incorporel créé à partir de la chose d'autrui demeure, indépendamment, l'élément principal de la création. En conséquence, le propriétaire du bien incorporel ne détient aucun droit privatif sur la chose d'autrui. Réciproquement, le propriétaire du support ou de l'outil ayant permis la production de l'œuvre ne détient aucun droit intellectuel sur celle-ci. Dès lors, en tant que matière première et outil technique, les éléments immatériels du corps humain du patient ne font nullement partie de la création intellectuelle. Tandis que le patient jouit d'une autodétermination informationnelle sur ses données médicales personnelles, il ne bénéficie d'aucun droit patrimonial sur les biens incorporels créés à partir de leur exploitation originelle.

458. En 2015, Arnaud Anciaux et Joëlle Farchy révélaient que l'internaute était inconsciemment au travail par la production de données personnelles recueillies à l'occasion de sa navigation sur l'Internet¹⁵³⁸. Ces auteurs ont remarqué que l'internaute contribuait gratuitement à la création de marchés, au développement de produits ou encore à la fabrication de prestations¹⁵³⁹. Ces nouveaux modes de mise au travail des particuliers, utilisateurs de services rendus, en faisaient les collaborateurs bénévoles des entreprises et les contributeurs à des œuvres incorporelles¹⁵⁴⁰. De la même façon, le patient qui fournit des données médicales à l'occasion de sa prise en charge sanitaire contribue gratuitement et involontairement au développement de nouveaux biens incorporels et innovants dans le domaine de la santé. Seulement, le droit de la propriété intellectuelle ne permet pas d'appréhender toutes les situations de contribution plurale, ni de prendre en considération l'ensemble des intervenants dans les différentes étapes d'élaboration de la création intellectuelle¹⁵⁴¹.

¹⁵³⁶ Civ. 1^{ère}, 1^{er} décembre 2011, n° 09-15.819, Bull. civ., I, n° 208 ; D., 2011, n° 44, p. 2995 ; RTD civ., 2012, n° 01, p. 131, obs. T. Revet ; RTD com., 2012, n° 01, p. 110, obs. F. Pollaud-Dulian.

¹⁵³⁷ VIVANT (M.), BRUGUIERE (J.-M.), *op. cit.*, p. 453 à p. 455.

¹⁵³⁸ ANCIAUX (A.), FARCHY (J.), *op. cit.*, p. 315.

¹⁵³⁹ *Ibid.*

¹⁵⁴⁰ *Ibid.*

¹⁵⁴¹ *Cf. supra.*

A l'occasion d'un colloque portant sur la propriété intellectuelle en partage, les participants se sont questionnés sur la manière dont cette spécialité juridique pouvait être repensée à l'aune de nouveaux usages dont font l'objet les créations incorporelles¹⁵⁴². Nathalie Martial-Braz s'est alors interrogée sur les modifications engendrées par l'implication des particuliers dans le processus créatif à l'heure du développement de l'économie collaborative¹⁵⁴³. L'auteur expose que « *le propre de l'économie collaborative c'est à la fois de générer de nouvelles formes de création qu'il convient d'encadrer, faute pour ces dernières de pouvoir être appréhendées par le prisme des qualifications traditionnelles, mais également de modifier les méthodes de création impliquant de nouveaux régimes plus adaptés* »¹⁵⁴⁴. Alors qu'il apparaît nécessaire de revisiter les règles relatives aux propriétés intellectuelles, nous doutons que le patient puisse bénéficier de cette nouvelle conception. Nonobstant sa contribution à la recherche et à l'innovation en santé à travers la réutilisation de ses données médicales personnelles, ce dernier ne semble pas associé au processus collaborativement créatif. En revanche, si la titularité des droits de propriété intellectuelle doit légitimement être attribués aux auteurs et aux inventeurs, l'ensemble des participants à la création, qu'ils soient directs, indirects, conscients ou involontaires, devraient profiter d'un droit aux bénéfices engendrés par la valorisation des résultats du traitement des données médicales à des fins de recherche ou d'innovation en santé. Il peut donc être intéressant de redéfinir les contours des nouvelles méthodes créatives afin de rétablir une équité économique entre l'ensemble des maillons de la chaîne de création.

459. Compte tenu de ce qui précède, la révision du droit de la propriété intellectuelle interviendrait possiblement comme une solution à la valorisation économique de l'exploitation de la donnée médicale au profit du patient. Cependant, ce dénouement potentiel présente certains écueils. D'une part, les données traitées étant pseudonymisées, le détenteur de la table de correspondance des pseudonymes, soumis au secret professionnel médical, devrait intervenir en tant qu'intermédiaire dans la distribution des bénéfices alloués aux personnes concernées. D'autre part, il suffirait, pour les exploitants des données médicales, de ne traiter que des jeux de données anonymisées pour échapper au partage des bénéfices entre les différents participants à la création intellectuelle. La donnée médicale n'étant plus

¹⁵⁴² ROBIN (A.), *La propriété intellectuelle en partage*, Dalloz, octobre 2020, p. 3.

¹⁵⁴³ MARTIAL-BRAZ (N.), *Création et économie collaborative : quelle régulation ?*, op. cit., p. 20.

¹⁵⁴⁴ MARTIAL-BRAZ (N.), *Création et économie collaborative : quelle régulation ?*, op. cit., p. 22.

affectée à une personne physique identifiable, la personne concernée ne pourrait être considérée comme un participant à l'œuvre intellectuelle ou à la création industrielle. Vraisemblablement, cette solution nébuleuse serait complexe à mettre en œuvre et l'impériosité de son application pourrait être contournée. De surcroît, une telle solution bouleverserait la finalité et les fondements théoriques de la réservation privative des créations intellectuelles. En effet, le droit de la propriété intellectuelle aspire à protéger les créations intellectuelles de la contrefaçon et du plagiat ainsi qu'à les valoriser afin d'en couvrir le développement. De cette manière, le progrès et l'innovation dans le secteur de la santé sont encouragés par le droit de la propriété intellectuelle, qui octroie un monopole d'exploitation au créateur.

460. En l'espèce, la protection de la création intellectuelle et sa valorisation économique ne représentent pas la finalité du traitement des données médicales mais en sont les conséquences. Certainement, le responsable de traitement a l'interdiction d'exploiter la chose anthropomorphique du patient à des fins économiques ou commerciales. Lorsque l'exploitant de la donnée médicale conçoit leur réutilisation pour une finalité de recherche ou d'innovation dans le secteur de la santé, il doit impérativement poursuivre un motif d'intérêt public dans le domaine de la santé publique¹⁵⁴⁵. Lorsqu'il est étranger à la prise en charge sanitaire du patient, le traitement de ses données médicales ne peut donc être mis en œuvre que dans l'intérêt général¹⁵⁴⁶. Incidemment, les résultats de la recherche pourront engendrer un bien incorporel qui pourra supposément donner prise au droit de la propriété intellectuelle. Dans cette hypothèse, les divers usages de ce bien incorporel profiteront à la collectivité tandis que son promoteur en financera le déploiement et participera au développement économique du secteur de la santé. L'unique bénéficiaire de la recherche ou de l'innovation dans le domaine de la santé, et du bien incorporel qui l'objective, siège donc au sein de la collectivité. Dès lors, n'appartiendrait-il pas à la collectivité d'offrir une récompense pécuniaire au patient pour cette participation citoyenne ? Comme l'indique Gérard Raymond, partager ses données médicales « *à son équipe soignante, c'est mieux être soigné ; les partager pour tous, c'est permettre que l'ensemble de nos concitoyens le soient aussi* »¹⁵⁴⁷.

¹⁵⁴⁵ Articles 9.2 i) du RGPD et 66.I de la loi Informatique et Libertés modifiée.

¹⁵⁴⁶ Cf. Paragraphes 526 et 613 s.

¹⁵⁴⁷ Gérard Raymond, président de France Assos Santé.

B) La récompense nationale pour la participation à un acte civique d'intérêt général

461. En sus de la valorisation de la création intellectuelle à l'échelle de son propriétaire, l'exploitation des données médicales du patient entraîne, par ricochet, de la richesse en profusion. En effet, la réutilisation des données médicales concourt directement à la recherche dans le domaine de la santé, puis indirectement à l'innovation, à son accès sur le marché ainsi qu'à la relance de la croissance économique. Selon le Gouvernement français, « *l'augmentation des données disponibles et leur échange, sont autant d'éléments de transformations du secteur [de la] santé* »¹⁵⁴⁸ et « *cette transformation [...] est en pleine accélération, avec une croissance attendue entre 2019 et 2023 de l'ordre de 160 % du marché de l'e-santé au sens large, pour un marché d'une valeur totale de 90 Mds\$ en 2019 et évalué à 235 Mds\$ en 2023* »¹⁵⁴⁹. En somme, la réutilisation des données médicales du patient contribue à « *favoriser l'émergence en France de solutions innovantes armées de propositions de valeurs médico-économiques fortes pour conquérir un marché en pleine croissance au niveau mondial* »¹⁵⁵⁰. Force est de constater l'iniquité entre le profit économique généré grâce aux résultats du traitement de la chose anthropomorphe et l'absence totale de compensation accordée au patient concerné. Pourtant, le patient se trouve au premier rang de la chaîne du progrès sanitaire. Sans la réutilisation des éléments immatériels de son corps humain, les capacités de recherche et de développement en santé seraient atrophiées et l'attractivité de la France en ce domaine paralysée. Alors, bien que le patient, en tant que membre de la société, soit observé comme l'ultime bénéficiaire de la recherche présentant un motif d'intérêt public dans le domaine de la santé – et de l'innovation incorporelle qui en résulte –, apparaît-il équitable de le priver de toute récompense financière pour sa participation à l'innovation sanitaire ? Tandis que l'exploitation de ses données médicales engendre des milliards d'euros, ce déséquilibre nous semble-t-il naturellement juste ? Nous serions d'avis que non.

¹⁵⁴⁸ Ministère de l'économie, des finances et de la relance, *Présentation de la stratégie d'accélération « Santé numérique »*, Disponible en ligne sur le site [www.entreprises.gouv.fr]. Consulté le 10 septembre 2021.

¹⁵⁴⁹ *Ibid.*

¹⁵⁵⁰ *Ibid.*

462. Du latin *aequitas*¹⁵⁵¹, l'équité est définie comme le principe du respect absolu de l'appréciation juste de ce qui est dû à chacun¹⁵⁵² ; ou comme la « *qualité consistant à attribuer à chacun ce qui lui est dû par référence aux principes de la justice naturelle* »¹⁵⁵³. Plus qu'une simple notion morale, l'équité judiciaire édifie « *un retour à la loi naturelle, dans le silence, l'obscurité ou l'insuffisance des lois positives* »¹⁵⁵⁴. Aux yeux de Jean-Étienne-Marie Portalis, « *c'est cette équité qui est le vrai supplément de la législation, et sans laquelle le ministère du juge, dans le plus grand nombre des cas, deviendrait impossible* »¹⁵⁵⁵. Synonyme de justice, l'équité serait davantage un concept « *ordonné autour du droit* »¹⁵⁵⁶ qu'une moralité philosophique. En effet, « *l'équité ferait partie intégrante du droit comme qualité de celui-ci* »¹⁵⁵⁷. Par conséquent, « *la première qualité de toute règle de droit serait d'être juste* »¹⁵⁵⁸. Par ailleurs, « *si le droit est muet ou comporte des lacunes, on peut se tourner vers l'équité qui est alors à côté du droit comme palliatif* »¹⁵⁵⁹. Ainsi que l'avait suggéré Aristote, « *la nature de l'équitable : c'est d'être un correctif de la loi* »¹⁵⁶⁰. L'équité apparaît donc comme un rectificatif du droit positif afin de rétablir le juste et de lutter contre tout déséquilibre¹⁵⁶¹. Si le droit est intrinsèquement lié à l'équité, alors l'équité, *praeter legem*, pourrait influencer la norme juridique vers le juste. Par suite, la règle de droit pourrait remédier à ce qui se présente naturellement injuste. L'équité pousse donc le théoricien du droit à considérer, pécuniairement, la contribution du patient à un motif d'intérêt public dans le domaine de la santé.

¹⁵⁵¹ Qui signifie esprit de justice, égalité, juste proportion.

¹⁵⁵² Lexicographie du mot « équité » défini par le CNRTL. Disponible en ligne sur le site [ww.cnrtl.fr]. Consulté le 09 septembre 2021.

¹⁵⁵³ Définition du mot « équité » du dictionnaire Larousse.

¹⁵⁵⁴ PORTALIS (J.-E.-M.), *Exposé des motifs du titre préliminaire du Code civil (1804)*.

¹⁵⁵⁵ *Ibid.*

¹⁵⁵⁶ SOREL (J.-M.), *Équité*, Répertoire de droit international, juillet 2017, § 1.

¹⁵⁵⁷ SOREL (J.-M.), *op. cit.*, § 9.

¹⁵⁵⁸ *Ibid.*

¹⁵⁵⁹ *Ibid.*

¹⁵⁶⁰ Voir : ARISTOTE, *Sur la justice, Éthique à Nicomaque*, Flammarion, 2008, Livre V : La vertu de Justice, Chapitre 14 : L'équité et l'équitable.

¹⁵⁶¹ ALBIGES (C.), *Équité*, Répertoire de droit civil, octobre 2017, actu. janvier 2019, § 36 ; CARBONNIER (J.), *op. cit.*, p. 31 à p. 32.

463. Il ne fait aucun doute que le patient intervient comme un acteur de l'innovation en santé en faveur de la collectivité. Aussi bien qu'il a été proposé de rémunérer les services autour de la donnée médicale¹⁵⁶², cette participation du patient pourrait être reconnue comme un acte civique à valoriser. Au même titre que l'on « *se pose tout naturellement la question de la « récompense » pour celui qui « apporte » des données à un ensemble, source d'une valeur économique notamment produite par cette mise en commun* »¹⁵⁶³, la valorisation de l'acte civique du patient – par son concours à la recherche et à l'innovation en santé – pourrait donc reposer sur une récompense exonérée de toute imposition. En effet, la récompense est définie comme une « *compensation* »¹⁵⁶⁴, elle-même entendue comme le « *fait de compenser, de réaliser ou de rétablir l'équilibre entre deux choses complémentaires ou antagonistes* »¹⁵⁶⁵. Finalement, la récompense serait l'une des manifestations de l'équité. Le législateur pourrait alors consacrer une récompense indemnitaire au bénéfice du patient de façon à pallier le déséquilibre relatif à la richesse économique gravitant autour de l'exploitation de ses données médicales. Effectivement, l'indemnité est l'expression financière de la compensation, *ergo* de la récompense. Et cette indemnité, intervenant au titre de l'équité, ne viserait pas à rétribuer la mise à disposition de la donnée médicale en considération de sa valeur économique potentielle¹⁵⁶⁶, mais à récompenser un acte citoyen sans que la proportion indemnisée ne soit égale à la richesse produite, l'équité étant assurément distincte de l'égalité. Partant, la cause de cette récompense siègerait dans le comportement du patient acquitté par l'exercice de ses droits de la personnalité, lesquels présentent une composante économique en dépit de leur extrapatrimonialité¹⁵⁶⁷. Dans cette hypothèse, la donnée médicale ne serait pas l'objet du contrat mais le prétexte de la

¹⁵⁶² Dialoguer pour agir, AI for Health, Présidence de l'Assemblée Nationale, Assemblée Nationale, *Numérique et santé pour tous : quelles actions pour la santé publique de demain ?*, Table ronde n°6 : Souveraineté et enjeux de dépendance, conférence du 13 juillet 2021. Replay disponible en ligne sur le site [www.aiforhealth.fr]. Consulté le 09 septembre 2021.

¹⁵⁶³ BENABOU (V.-L.), *op. cit.*, p. 65.

¹⁵⁶⁴ Lexicographie du mot « récompense » défini par le CNRTL. Disponible en ligne sur le site [ww.cnrtl.fr]. Consulté le 10 septembre 2021.

¹⁵⁶⁵ Lexicographie du mot « compensation » défini par le CNRTL. Disponible en ligne sur le site [ww.cnrtl.fr]. Consulté le 10 septembre 2021.

¹⁵⁶⁶ Cf. Paragraphes 381 et 450.

¹⁵⁶⁷ Cf. Paragraphe 450.

prestation¹⁵⁶⁸. L'extrapatrimonialité de la donnée médicale ne serait donc nullement remise en cause.

464. La récompense de l'accomplissement d'actes civiques par l'allocation d'indemnités n'est pas étrangère à notre système juridique. A titre d'exemple, le service civique, qui a pour objet de « *renforcer la cohésion nationale et la mixité sociale et offre à toute personne volontaire l'opportunité de servir les valeurs de la République et de s'engager en faveur d'un projet collectif en effectuant une mission d'intérêt général* »¹⁵⁶⁹, est gratifié au moyen d'une indemnité¹⁵⁷⁰ versée au citoyen engagé. Pareillement, les « *Français méritants qui se sont illustrés par leur engagement pour la société* »¹⁵⁷¹ en réalisant des actions de citoyenneté et de solidarité auprès de la collectivité sont récompensés, au titre des Prodiges de la République, par un chèque de 500 euros à reverser à l'association locale de leur choix¹⁵⁷². Par ailleurs, l'implication des citoyens dans le système de santé et l'exercice de la démocratie sanitaire prêtent à récompense. En effet, la citoyenneté sanitaire, qui reflète « *une capacité à prendre part (participation) à une expression et une action qui dépassent son propre intérêt personnel de patient* »¹⁵⁷³, donne régulièrement lieu à indemnisation, voire à rémunération¹⁵⁷⁴. Effectivement, l'on peut « *noter une tendance plutôt significative à l'existence de cette indemnisation dans le domaine de la santé* »¹⁵⁷⁵.

Toutefois, à l'occasion d'une étude relative à la participation des usagers-citoyens au système de santé, des questionnements ont été soulevés au sujet de « *l'indemnisation du travail effectué lors de la participation* » à la citoyenneté sanitaire¹⁵⁷⁶, « *et non sur le remboursement des frais qui semble ne pas faire controverse et constitue même souvent un*

¹⁵⁶⁸ MALLET-POUJOL (N.), *Droit à et droit sur l'information de santé*, In *Le droit des données de santé*, op. cit. p. 84.

¹⁵⁶⁹ Article L.120-1 du code du service national.

¹⁵⁷⁰ Voir : articles L.120-18 à L.120-24 du code du service national.

¹⁵⁷¹ MINISTERE DE L'INTERIEUR, *Dossier de presse : les prodiges de la République*, 27 mai 2021.

¹⁵⁷² Site internet du Gouvernement, *Les Prodiges de la République à l'honneur*, 15 décembre 2020. Disponible en ligne sur le site [www.gouvernement.fr]. Consulté le 11 septembre 2021.

¹⁵⁷³ PLANETE PUBLIQUE, *Pour un débat citoyen sur la santé plus actif*, Rapport d'étude commandé par le Ministère de la santé, de la jeunesse et des sports, 7 juillet 2011.

¹⁵⁷⁴ *Ibid.*

¹⁵⁷⁵ *Ibid.*

¹⁵⁷⁶ *Ibid.*

prérequis à la participation »¹⁵⁷⁷. Pour les mêmes raisons que l'extrapatrimonialité de la donnée médicale devrait être consacrée, « *indemniser la participation est perçu par certains comme faisant courir le risque de la marchandisation de l'expertise citoyenne : des personnes s'engageraient uniquement dans un but lucratif* »¹⁵⁷⁸.

En revanche, récompenser le patient pour l'accomplissement d'un acte civique relatif à l'innovation dans le domaine de la santé préviendrait des dérives mercantiles relatives à l'économicité de l'exploitation de la donnée médicale. D'abord, s'il était admis que les choses anthropomorphiques pseudonymisées et anonymisées tombaient automatiquement dans le domaine commun informationnel¹⁵⁷⁹, elles seraient systématiquement réutilisées pour des projets d'intérêt public dans le domaine de la santé. Le concours aux recherches rétrospectives présentant un motif d'intérêt général dans le domaine de la santé publique ne serait donc pas influencé par une quelconque marchandisation de cet acte civique, fossoyeuse de discrimination. Certainement, cette participation deviendrait systématique et concernerait unanimement l'intégralité des patients pris en charge par un professionnel de santé. L'ensemble des citoyens serait donc également récompensé pour cet acte de citoyenneté, que nous pourrions, en outre, considérer comme un devoir de concours aux motifs d'intérêt public dans le domaine de la santé¹⁵⁸⁰. D'une certaine façon, la récompense nationale pour la participation à un acte d'intérêt général serait désintéressée. Nous retrouverions alors de l'égalité dans la mise en œuvre de l'équité. Ensuite, si chaque citoyen percevait indistinctement une récompense financière en contrepartie de cet acte citoyen, la dignité humaine serait davantage préservée contre toute instrumentalisation de son corps humain par la vente de données médicales¹⁵⁸¹.

Dans l'hypothèse où le Système national des données de santé concrétiserait le domaine commun informationnel, tout élément immatériel du corps humain du patient serait mis à disposition par le Health Data Hub¹⁵⁸². Tandis qu'il paraît « *légitime que le producteur*

¹⁵⁷⁷ *Ibid.*

¹⁵⁷⁸ *Ibid.*

¹⁵⁷⁹ *Cf.* Paragraphe 376.

¹⁵⁸⁰ *Cf.* Paragraphes 533 s.

¹⁵⁸¹ *Cf.* Paragraphes 362 et 371.

¹⁵⁸² *Cf.* Paragraphe 453.

de donnée reçoive une rétribution [par le Health Data Hub] dès lors qu'il consent des efforts techniques pour les mettre à disposition et pour améliorer leur qualité »¹⁵⁸³, il semble équitable que le patient qui en est la source soit récompensé par une prestation indemnitaire versée par ce groupement d'intérêt public, ou par tout autre organisme étatique chargé de la gouvernance de ce nouveau domaine public. Compte tenu de ce qui précède, le droit pourrait, dans l'expression de sa justice, corriger symboliquement l'iniquité résultant de la valorisation économique de la chose anthropomorphique du patient.

¹⁵⁸³ CUGGIA (M.), POLTON (D.), WAINRIB (G.), COMBES (S.), *op. cit.*, p. 18.

Conclusion du chapitre

465. Dans le domaine de la santé, le traitement des données médicales du patient poursuit différents objectifs. Evidemment, il a vocation à répondre à une problématique scientifique, objectivée par une finalité déterminée, explicite et légitime, afin de créer et d'innover. Seulement, toute activité professionnelle est coûteuse. Même si l'exploitant de la donnée médicale du patient désire sincèrement œuvrer au bénéfice de la collectivité en contribuant à l'amélioration de la qualité des prises en charge sanitaire, au progrès de la santé collective ou encore à l'optimisation du système de santé, ce dernier doit également pouvoir jouir d'un intérêt économique vital à la pérennisation de son activité. Le traitement des données médicales du patient génère incidemment du profit et contribue vertueusement à la croissance économique. Les résultats de leur traitement sont généralement valorisables et représentent, le cas échéant, une source de revenus et de financement. Selon les secteurs d'activités, il existe cependant un décalage conséquent entre le simple retour sur le capital investi pour mettre en œuvre le traitement des données médicales et la fortune qui en résulte effectivement.

Conscients de la richesse produite à partir du traitement des données médicales du patient, les acteurs chargés de la mission de préfiguration du Health Data Hub ont considéré qu'il était « *essentiel de prévoir un juste partage de la valeur qui résulterait de leur utilisation* »¹⁵⁸⁴. Seulement, les experts chargés de cette mission ne visaient que les producteurs des données médicales sans considérer le patient qui en est pourtant la source originelle. S'il semble légitime de distribuer la valeur dégagée par le traitement des données médicales du patient au professionnel de santé qui les a produites, n'apparaît-il pas tout aussi légitime d'en partager une fraction avec la personne de laquelle elles émanent ? Sans patient, il n'existerait aucun producteur de données médicales ni, *a fortiori*, aucun traitement reposant sur celles-ci. Cette absence totale de considération portée au patient donne le malheureux sentiment que l'ensemble du profit résultant du traitement de ses données médicales est produit à partir d'informations collectées dans un contexte de maladie ; et cette incommodité pourrait engendrer une certaine défiance de la collectivité.

¹⁵⁸⁴ *Ibid.*

Au nom de l'éthique et de l'équité, il a donc été fondamental de réfléchir à un dispositif qui permettrait de valoriser la participation du patient à l'innovation sanitaire et à la santé publique. Le mécanisme de la récompense allouée en contrepartie d'un acte civique nous a semblé concordant avec le statut juridique et les régimes applicables que nous appliquons à la chose anthropomorphique pseudonymisée et anonymisée. Il appartient désormais aux économistes de modéliser la fraction indemnitaire ou forfaitaire pouvant être accordée à l'intégralité des patients – dans la mesure où leurs données médicales alimenteraient systématiquement le domaine commun informationnel –, puis au législateur d'employer cette potentialité.

Conclusion du titre

« Au rang des communs figure incontestablement l'information : information non-appropriable parce que « collective » ou information non-appropriable parce que « individuelle ». Des lois de police règlent la manière de jouir des informations, choses communes, tandis qu'une « police » du droit de la personnalité est accordée à l'individu sur ses données personnelles. »¹⁵⁸⁵.

466. Objectivement, les données médicales présentent « un fort potentiel de valorisation économique »¹⁵⁸⁶. En dépit de cette réalité économique, nous défendons l'extrapatrimonialité de la donnée médicale, qu'elle soit à caractère personnel ou qu'elle ait été anonymisée. Compte tenu de la révolution numérique et du développement de l'intelligence artificielle, les éléments immatériels du corps humain du patient ont vocation à circuler davantage entre les mains d'une somme d'exploitants attachés à de multiples filières. Face aux nombreuses réutilisations de ces informations singulièrement intimes, et aux potentialités économiques qui lui sont intrinsèques, il est apparu nécessaire d'offrir aux personnes concernées une meilleure protection de leur chose anthropomorphique. A cet effet, nous pensons que l'accroissement de cette protection peut être assurée par la consécration de leur extrapatrimonialité et, conjointement, de leur intégration dans le domaine commun informationnel.

D'une part, la consécration de l'extrapatrimonialité de la donnée médicale empêcherait toute concrétisation future de la doctrine favorable à la conception propriétaire des données à caractère personnel, dont les données médicales forment une sous-catégorie. Tandis que certains rapportent que « le droit de propriété [...] paraît être une réponse naturelle à la question de l'identification du lien existant entre la personne et ses données »¹⁵⁸⁷, nous pensons, au contraire, que la donnée à caractère personnel ne peut être intimement et définitivement affectée qu'à la seule personne concernée, en dehors de toute

¹⁵⁸⁵ CORNU (M.), ORSI (F.), ROCHFELD (J.), *loc. cit.*

¹⁵⁸⁶ *Ibid.*

¹⁵⁸⁷ DESTREGUIL (M.), *Plaidoyer en faveur d'une approche propriétaire des données personnelles*, Revue Juridique Personnes et Famille, mars 2019, n° 03.

réserve privative. Ainsi, le patient ne pourrait hypothéquer sa dignité humaine¹⁵⁸⁸ et nul ne pourrait disposer des éléments immatériels de son corps humain.

D'autre part, si l'intégralité des données médicales pseudonymisées et anonymes intégraient le domaine commun informationnel, personne ne trouverait plus aucun intérêt ni à les approprier, ni à les vendre. À jamais soustraite de tout rapport marchand, le patient serait préservé contre toute dérives mercantiles liées à la réutilisation de sa chose anthropomorphique. De surcroît, si l'ensemble des producteurs des données médicales devaient les y verser, leur mise à disposition au profit tout exploitant serait administrée par un guichet unique dans le respect des normes de police administrative qui les gouvernent et, le cas échéant, conformément au droit à la protection des données personnelles. Conséquemment, leur sécurisation, la traçabilité de leurs accès et l'exercice des droits de la personne concernée seraient considérablement améliorés.

467. En outre, l'extrapatrimonialité et l'intégration de la donnée médicale au sein du domaine commun informationnel favoriserait sa réutilisation en faveur de tout projet présentant un motif d'intérêt public dans le domaine de la santé. En effet, la simplicité du recours à un guichet unique, la structuration et la mise en qualité des données minimisées à la finalité du traitement projeté et le principe de gratuité de la réutilisation des données¹⁵⁸⁹ encourageraient l'exploitation de cet élément immatériel émanant du patient. En conséquence, le profit généré grâce à la valorisation du traitement de la chose anthropomorphique et la croissance économique du marché idoine seraient subséquentement amplifiés. A l'évidence, la non-appropriation ainsi que la libération de l'information encourage l'activité économique¹⁵⁹⁰. Par ailleurs, les producteurs des données médicales ainsi que les patients concernés pourraient être financièrement récompensés pour leurs engagements et leurs efforts respectifs achevés au bénéfice de la collectivité¹⁵⁹¹. Finalement, « *cette récusation de tout droit de propriété sur l'information invite à revivifier le concept d'usage d'une chose hors commerce parce que non appropriable ou indisponible* »¹⁵⁹². De la

¹⁵⁸⁸ MALLET-POUJOL (N.), *op. cit.*, p. 333.

¹⁵⁸⁹ A moins que les conditions de l'exception de redevance ne soient réunies.

¹⁵⁹⁰ CLUZEL-METAYER (L.), *La construction d'un service public de la donnée, op. cit.*, p. 497.

¹⁵⁹¹ Cf. Paragraphes 430 et 463.

¹⁵⁹² MALLET-POUJOL (N.), *op. cit.*, p. 334.

même façon, « *penser cet usage en termes de droit à l'information et de droit de la personnalité contribuerait à renforcer un « certain humanisme juridique »* »¹⁵⁹³. Sans conteste, les aspects économiques, juridiques, humains et éthiques relatifs à la réutilisation de la chose anthropomorphique sont conjugables indépendamment de toute patrimonialité.

468. Dès lors que les conditions juridiques encadrant la réutilisation de la « chose anthropomorphique commune » sont effectivement réunies, sa réutilisation par un tiers exploitant est-elle réellement permise ? La réponse à ce questionnement requiert maintenant de déterminer les contours de l'autodétermination informationnelle du patient lorsque ses données médicales personnelles sont concrètement réutilisées au bénéfice de l'intérêt public dans le domaine de la santé.

¹⁵⁹³ *Ibid.*

TITRE 2 :

LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AUX FINS D'INTERET PUBLIC DANS LE DOMAINE DE LA SANTE : LA RECHERCHE, L'INNOVATION ET LA SANTE PUBLIQUE

« On peut comprendre que la notion d'intérêt général, c'est-à-dire d'un intérêt neutre et impartial censé exprimer celui du peuple tout entier [...] semble, au fond, constituer le nœud conceptuel qui est l'objet même de l'État moderne et de son droit, son nouvel horizon et sa nouvelle légitimité. »¹⁵⁹⁴.

469. Les données médicales, produites à l'occasion d'une prise en charge sanitaire, présentent des intérêts généraux supérieurs aux intérêts particuliers du patient qui en est à la source. En effet, la réunion d'informations relatives aux conditions physiques, psychiques et biologiques de plusieurs personnes physiques permettent d'observer des phénomènes sanitaires. Par conséquent, l'agrégat des éléments immatériels des corps humains d'une pluralité de patients offre des perspectives pour l'intérêt général dans le domaine de la santé. Si le traitement des données médicales d'un patient pris isolément favorise l'amélioration de sa santé individuelle, le traitement des données médicales des membres de la société concourt au développement de la santé publique, à une meilleure connaissance de la santé collective de la population et, *in fine*, à son amélioration. A l'évidence, si les données médicales constituent l'outil indispensable à la prise en charge sanitaire du patient, comment améliorer les connaissances médicales et la santé de la population sans le traitement des données médicales de ses membres ? Seulement, *« ériger les données en matériau collectif revient à faire peu de cas du lien avec la personne qui en est à l'origine : mérite-t-elle d'être soumise, sur ses données, à ces finalités collectives sans pouvoir donner son consentement aux utilisations qui en relèvent ? »¹⁵⁹⁵.*

¹⁵⁹⁴ CRETOIS (P.), ROZA (S.), *De l'intérêt général : Introduction*, In CRETOIS (P.), ROZA (S.), *De l'intérêt général*, Astérian, 2017, n°17, p. 5.

¹⁵⁹⁵ BENABOU (V.-L.), ROCHFELD (J.), *À qui profite le clic ? Le partage de la valeur à l'heure numérique*, Odile Jacob, 2015, p. 63.

Il est primordial de garder à l'esprit la nature de la chose anthropomorphique ainsi que le contexte de sa production¹⁵⁹⁶. Plus qu'une donnée à caractère personnel, il s'agit de la réification d'un état de santé dépendant de la physiologie du corps humain du patient. Cette information, nécessairement collectée à l'occasion de l'étude médicale de son (dys)fonctionnement, touche intimement à la dignité de son hôte. Néanmoins, il convient de rompre avec l'opposition systémique entre le respect de la vie privée et de l'intégrité du corps humain du patient d'une part, et l'ouverture de ses données médicales au profit de l'intérêt général d'autre part. A l'inverse, il conviendrait de conjuguer public avec privé, et ouverture avec protection et confidentialité¹⁵⁹⁷. Certainement, la réutilisation des données médicales des individus constitue un enjeu de santé publique majeur. Tant la recherche et l'innovation dans le domaine de la santé (**Chapitre 1**) que la maîtrise des risques et de la sécurité sanitaires (**Chapitre 2**) constituent des ambitions au cœur de la politique de la santé publique contemporaine et numérique. Or, ces deux disciplines se fondent essentiellement sur l'exploitation des données médicales des membres de la société. La santé publique correspond donc à une notion multidisciplinaire fondée sur le traitement de données sanitaires dont, infailliblement, les données médicales des patients. Fort heureusement, le droit à la protection des données personnelles autorise autant qu'il encadre les traitements de ces données sensibles lorsqu'ils sont nécessaires pour des motifs d'intérêt général dans le domaine de la santé.

¹⁵⁹⁶ Cf. Paragraphes 16 et 466.

¹⁵⁹⁷ PECHILLON (E.), *L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ?*, L'information psychiatrique, vol. 91, 2015, n°08, p. 645 à p. 649.

Chapitre 1 : La requalification des données médicales en données de recherche

470. Les recherches rétrospectives dans le domaine de la santé sont réalisées à partir de l'exploitation de données déjà existantes, collectées à l'occasion d'un traitement antérieur poursuivant une finalité initiale. C'est ainsi que les données médicales originellement produites pour satisfaire à la prise en charge sanitaire du patient peuvent être secondairement réutilisées à des fins de recherche scientifique pour l'intérêt public de la santé collective. La réutilisation ultérieure des éléments immatériels du corps humain du patient pour un nouvel objectif implique donc un changement de la finalité pour laquelle ils ont été originellement recueillis (**Section préliminaire**).

471. Une telle modification de la finalité du traitement des données médicales impacte l'autodétermination informationnelle du patient concerné. Alors que toute personne concernée devrait pouvoir décider de l'usage des informations qui la concernent¹⁵⁹⁸, le patient ne pourrait empêcher la réutilisation de ses choses anthropomorphiques dès lors que leur exploitation participe à la protection de la santé publique (**Section 2**). En effet, les données médicales, requalifiées en *données de recherche* pseudonymisées, constituent la ressource essentielle au développement de la recherche dans le domaine de la santé et, subséquemment, au progrès de l'innovation sanitaire.

472. Tandis que l'autodétermination informationnelle du patient concerné par l'utilisation de ses données de recherche se trouve circonscrite, il conserve néanmoins certaines prérogatives à leur égard (**Section 1**). Selon toute apparence, il jouit des droits d'y accéder, de les rectifier, de les effacer et de limiter leur exploitation.

¹⁵⁹⁸ Article 1 alinéa 2 de la loi Informatique et Libertés modifiée.

Section préliminaire : Le changement de la finalité du traitement des données médicales produites à l'occasion du soin

« *L'irruption dans les pratiques médicales des technologies du Big Data décuple les possibilités de recherche dans le domaine de la santé, au prix d'une requalification systématique des données de soins en données de recherche.* »¹⁵⁹⁹.

473. En France, des quantités exponentielles de données médicales sont produites chaque jour à l'occasion de toute prise en charge sanitaire. Grâce à l'application des technologies de l'information et de la communication, cette masse de données peut être facilement analysée au bénéfice du patient dans le cadre de sa prise en charge médicale, mais également dans l'intérêt public de la collectivité. En effet, l'utilité des données médicales dépasse aujourd'hui celle des seules prises en charge cliniques¹⁶⁰⁰. C'est ainsi qu'une nouvelle forme de recherche n'impliquant pas la personne humaine, se déroulant à distance des personnes physiques à partir de leurs données médicales, a émergé. Plus précisément, le code de la santé publique les définit comme « *les recherches ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation dans le domaine de la santé conduites exclusivement à partir de l'exploitation de données à caractère personnel* »¹⁶⁰¹. Il s'agit de recherches rétrospectives fondées sur l'examen de données médicales déjà existantes provenant des dossiers médicaux des patients ou des bases et entrepôts de données de santé¹⁶⁰². Ces recherches dans le domaine de la santé couvrent un large éventail d'activités. Leur qualification couvre tant l'épidémiologie que l'évaluation des activités de soins et de la pertinence thérapeutique, le développement des logiciels algorithmiques ou d'intelligence artificielle dans le domaine de la santé¹⁶⁰³, ou les études de suivi *post-marketing* des dispositifs médicaux. Cette vaste catégorie de recherche s'oppose aux recherches impliquant la personne humaine qui sont pratiquées sur l'être humain afin de produire des données spécifiquement dans l'intention de

¹⁵⁹⁹ MAMZER BRUNEEL (M.-F.), HERVE (C.), *La requalification des données de soins en données de recherche : enjeux éthiques et blocages normatifs*, Ethics, Medicine and Public Health, 2017, n°3, p. 83.

¹⁶⁰⁰ MAMZER BRUNEEL (M.-F.), HERVE (C.), *op. cit.*, p. 84.

¹⁶⁰¹ L'article R.1121-1 II 3° du code de la santé publique

¹⁶⁰² INSERM, *La recherche clinique*, 07 juin 2021. Disponible en ligne sur le site [www.inserm.fr]. Consulté le 19 septembre 2021.

¹⁶⁰³ BENSAMOUN (A.), *Rapport de la CNIL sur l'intelligence artificielle : une réflexion éthique*, Revue pratique de la prospective et de l'innovation, 2018, n° 01, p. 33 à p. 37.

développer les connaissances biologiques ou médicales¹⁶⁰⁴. Les recherches, les études et les évaluations dans le domaine de la santé reposent donc sur la réutilisation des données médicales du patient produites à l'occasion de sa prise en charge sanitaire. La requalification des données issues du soin en données de recherche modifie conséquemment la finalité initiale pour laquelle les données médicales ont été produites et collectées¹⁶⁰⁵.

474. Pourtant, le RGPD pose un principe de limitation des finalités du traitement selon lequel les données personnelles doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* »¹⁶⁰⁶. Préalablement à un traitement de données personnelles, le responsable de traitement doit alors déterminer un objectif à atteindre qui soit précis, justifié, raisonnable et énoncé de manière compréhensible et suffisamment claire. Cette spécification des finalités est doublement décisive pour la protection des données personnelles. D'abord, elle permet de délimiter le périmètre de leur exploitation. En effet, les données personnelles ne peuvent être traitées que pour les finalités pour lesquelles elles ont été pertinemment et adéquatement collectées et dont la personne concernée a été informée. La limitation des finalités du traitement vise donc à prévenir tout détournement des informations personnelles de la personne concernée. Dans l'hypothèse d'un mésusage des données collectées, le responsable de traitement encourt une peine pouvant s'élever jusqu'à 300 000 euros d'amende et 5 ans d'emprisonnement¹⁶⁰⁷. Ensuite, la spécification de la finalité sert à déterminer l'ensemble des autres principes relatifs au traitement des données personnelles édictés par le RGPD. C'est à partir de la finalité que découlent, entre autres, la minimisation des données collectées, leur durée de conservation, la liste des personnes autorisées à y accéder, ou encore la base légale sur laquelle le traitement établit sa licéité. En somme, la limitation des finalités du traitement contribue à la transparence, à la sécurité juridique ainsi qu'à la prévisibilité du traitement des données personnelles. De cette façon, les limites à la manière dont les responsables du traitement peuvent les utiliser sont cristallisées et les personnes concernées en ressortent confiantes et protégées. Certainement, le principe de la limitation des finalités est positionné

¹⁶⁰⁴ Article L.1121-1 du code de la santé publique.

¹⁶⁰⁵ Cf. Paragraphe 46.

¹⁶⁰⁶ Article 5.1 b) du RGPD.

¹⁶⁰⁷ Le détournement de finalité est puni à l'article 226-21 du code pénal.

« au cœur de la confiance que les personnes peuvent avoir dans les services de la société numérique »¹⁶⁰⁸.

475. Une fois que les finalités de la collecte des données personnelles ont été suffisamment déterminées, le responsable de traitement peut ensuite mettre en œuvre tout traitement ultérieur compatible avec ces dernières. Avant tout, il est utile de préciser que la collecte des données constitue la première opération de traitement des données personnelles. Ainsi, tout traitement consécutif à la collecte doit être considéré comme un traitement ultérieur devant donc répondre à l'exigence de compatibilité¹⁶⁰⁹. Le responsable de traitement peut donc mettre en œuvre toute opération de traitement ultérieure à la collecte des données, qu'elle soit effectuée dans le cadre de la finalité initiale ou pour une finalité différente dès lors qu'elle est compatible avec l'originale. Autrement dit, le responsable de traitement peut « effectuer des opérations de traitements au-delà de la collecte des données initiale, dès lors que ces traitements sont compatibles avec la finalité initiale, c'est-à-dire qu'ils présentent notamment un lien suffisant avec la finalité initiale de la collecte »¹⁶¹⁰. Force est d'observer que le principe de la limitation des finalités est également conçu pour offrir une certaine flexibilité au responsable du traitement, tout en garantissant une certaine prévisibilité des traitements ultérieurs¹⁶¹¹.

Il en résulte que les données médicales du patient, collectées aux fins de sa prise en charge sanitaire, peuvent faire l'objet de traitements ultérieurs lorsqu'ils s'inscrivent dans la continuité de cette finalité originale. A titre d'exemple, les éléments immatériels du corps humain collectés pour la prise en charge sanitaire du patient peuvent consécutivement alimenter ses dossiers médicaux, être échangés avec d'autres professionnels afin d'assurer la coordination des soins, être analysés par un algorithme d'aide au diagnostic ou examinés à distance dans le cadre de la télésanté. Ces différents traitements convergent vers la même finalité – la prise en charge médicale – : ils sont alors réputés compatibles. En revanche, lorsque le traitement ultérieur des données personnelles répond à une finalité différente de

¹⁶⁰⁸ Conseil d'Etat, *Le numérique et les droits fondamentaux*, op. cit., p. 19.

¹⁶⁰⁹ Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 02 avril 2013, p. 21.

¹⁶¹⁰ GAULLIER (F.), *Le principe de finalité dans le RGPD : beaucoup d'ancien et un peu de nouveau*, Communication Commerce électronique, avril 2018, n° 4, § 21.

¹⁶¹¹ Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, op. cit., p. 38.

celle ayant justifié leur collecte, leur compatibilité doit alors être démontrée¹⁶¹². Ainsi, les données médicales du patient peuvent être utilisées à d'autres fins que sa prise en charge sanitaire à condition que cette autre finalité soit compatible avec l'initiale. A cet effet, un test de compatibilité substantielle doit être réalisé.

476. L'analyse substantielle de la compatibilité entre les finalités initiales et les finalités ultérieures repose sur l'évaluation de cinq critères. « *Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement* »¹⁶¹³, le responsable de traitement doit, en premier lieu, tenir compte de tout lien convergeant entre les différentes finalités¹⁶¹⁴. En deuxième lieu, il lui appartient d'étudier le « *contexte dans lequel les données à caractère personnel ont été collectées* »¹⁶¹⁵ et de considérer « *les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données* »¹⁶¹⁶. En troisième lieu, le responsable de traitement doit examiner « *la nature des données à caractère personnel* »¹⁶¹⁷. En quatrième lieu, il lui revient de vérifier « *les conséquences pour les personnes concernées du traitement ultérieur* »¹⁶¹⁸. En cinquième lieu, le responsable de traitement doit garantir « *l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur* »¹⁶¹⁹.

477. Toutefois, le RGPD annonce que « *le traitement ultérieur [...] à des fins de recherche scientifique [...] devrait être considéré comme une opération de traitement licite compatible* »¹⁶²⁰. Une présomption de compatibilité entre la finalité initiale ayant légitimé la collecte des données personnelles et leur réutilisation aux fins de recherche scientifique semble donc exister ; et cette extension des finalités profite aux recherches rétrospectives dans le domaine de la santé. Certainement, « *par fins de recherche scientifique, il convient*

¹⁶¹² Considérant 50 du RGPD.

¹⁶¹³ *Ibid.*

¹⁶¹⁴ *Ibid.*

¹⁶¹⁵ *Ibid.*

¹⁶¹⁶ *Ibid.*

¹⁶¹⁷ *Ibid.*

¹⁶¹⁸ *Ibid.*

¹⁶¹⁹ *Ibid.*

¹⁶²⁰ *Ibid.*

également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique »¹⁶²¹. Apparemment, la réutilisation des données médicales du patient à des fins de recherche n'impliquant pas la personne humaine paraît donc compatible avec leur collecte lors de sa prise en charge sanitaire.

478. Le RGPD précise que tout traitement ultérieur à des fins de recherche scientifique n'est pas incompatible avec toute finalité initiale à condition que « *des garanties appropriées pour les droits et libertés de la personne concernée* »¹⁶²² soient instituées par le responsable de traitement. De surcroît, la loi Informatique et Libertés modifiée ajoute que le traitement ultérieur ne doit pas être « *utilisé pour prendre des décisions à l'égard des personnes concernées* »¹⁶²³. Cette présomption de compatibilité ne devrait pas être considérée comme une permission générale de changement de finalité pour la recherche dans le domaine de la santé. En effet, cette présomption ne joue qu'à la condition que les exigences susvisées soient appliquées au traitement à des fins de recherche scientifique.

A cet égard, le responsable de la recherche doit d'abord instaurer des mesures techniques et organisationnelles pour garantir la séparation fonctionnelle entre les données personnelles et les personnes concernées¹⁶²⁴. S'il n'est pas possible de procéder à leur anonymisation, celles-ci devront tout au moins être pseudonymisées. Le cas échéant, la clé de réidentification entre les données nominatives et pseudonymisées doit être conservée par les professionnels dépositaires du secret professionnel médical habilités à accéder aux éléments immatériels du corps humain du patient¹⁶²⁵. Egalement, des fonctions telles que le cryptage et le hachage devraient être appliquées de façon à empêcher la réidentification des données pseudonymisées par les tiers exploitants. Ainsi, le traitement des données de recherche ne pourrait occasionner aucune conséquence individuelle à l'égard des patients concernés et le secret professionnel médical serait effectivement préservé. Au demeurant, il importe de préciser que la pseudonymisation s'avère « *compatible avec la préservation de la confidentialité des données, tout en rendant compte des possibilités techniques existantes de*

¹⁶²¹ Considérant 159 du RGPD.

¹⁶²² Article 89.1 du RGPD.

¹⁶²³ Article 4 alinéa 2 de la loi Informatique et Libertés modifiée.

¹⁶²⁴ Article 89.1 du RGPD.

¹⁶²⁵ Cf. Paragraphe 255.

ré-identification des personnes sources »¹⁶²⁶ via la table de correspondance des pseudonymes. En effet, cette clé de réidentification n'est détenue que par les professionnels ayant effectivement participé à la prise en charge sanitaire du patient.

Ensuite, les mesures techniques et organisationnelles doivent permettre d'« *assurer le respect du principe de minimisation des données* »¹⁶²⁷. La liste des catégories de patients inclus dans la recherche n'impliquant pas la personne humaine et l'inventaire exhaustif des données médicales sélectionnées doivent être scientifiquement justifiés au sein du protocole de recherche. Ce document permet « *de préjuger de la pertinence des données traitées au regard de la finalité du traitement* »¹⁶²⁸ et de cibler les données médicales à extraire de leur base initiale afin d'intégrer un jeu de données de recherche pseudonymisées.

En outre, lorsque le patient concerné réside sur le territoire français¹⁶²⁹, des « *dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé* »¹⁶³⁰ établissent des garanties supplémentaires aux dispositions de droit commun du RGPD. Ces mesures législatives visent à encadrer l'ensemble des traitements à des fins de recherche scientifique et à renforcer la protection des données sensibles exploitées.

479. Compte tenu de ce qui précède, la mise en place de garanties techniques, organisationnelles et juridiques dans la mise en œuvre du traitement à des fins de recherche scientifique semble donc se substituer à l'évaluation préalable de compatibilité substantielle entre les différentes finalités. Comme l'indique Maître Florence Gaullier, « *si le traitement ultérieur concerné respecte les exigences de l'article 89.1 précité, la probabilité qu'il puisse passer le test de compatibilité devrait s'avérer élevée* »¹⁶³¹. Les cinq critères de compatibilité énoncés par le RGPD apparaissent *de facto* réunis lorsque les données médicales sont requalifiées en données de recherche. Premièrement, l'objectif initial qui réside dans la prise

¹⁶²⁶ MAMZER BRUNEEL (M.-F.), HERVE (C.), *op. cit.*, p. 87.

¹⁶²⁷ Article 89.1 du RGPD.

¹⁶²⁸ MAMZER BRUNEEL (M.-F.), HERVE (C.), *op. cit.*, p. 86.

¹⁶²⁹ Article 3.I de la loi Informatique et Libertés modifiée.

¹⁶³⁰ Sous-section 2 de la Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

¹⁶³¹ GAULLIER (F.), *op. cit.*, § 27.

en charge sanitaire du patient et le but du traitement ultérieur qui consiste à innover dans l'intérêt public de la santé sont intrinsèquement liés. Deuxièmement, c'est grâce aux progrès médicaux que les patients peuvent individuellement bénéficier de soins innovants et fondés sur les données acquises de la science¹⁶³². Troisièmement, cette réutilisation des données médicales à des fins de recherche scientifique est une pratique habituelle à laquelle les patients peuvent raisonnablement s'attendre. Quatrièmement, le traitement à des fins de recherche scientifique est réalisé en toute transparence dans la mesure où il suppose l'information individuelle préalable des personnes concernées¹⁶³³. Cinquièmement, le responsable de traitement doit respecter des mesures telles que l'autorisation de l'autorité de contrôle¹⁶³⁴, la pseudonymisation des données nominatives, ou encore la réalisation d'une analyse d'impact sur la vie privée et la protection des données¹⁶³⁵. En l'espèce, la présomption de compatibilité posée par le RGPD ne conçoit plus une supposition mais devient une certitude. Si le G29 suggère que l'évaluation de compatibilité soit effectuée préalablement à chaque traitement ultérieur en considération de ses spécificités¹⁶³⁶, sa réalisation ne peut être exigée pour les traitements ultérieurs à des fins de recherche scientifique. En l'absence de disposition juridique contraignante, ce test de compatibilité effectué à la lumière des cinq critères d'évaluation¹⁶³⁷ ne peut qu'être recommandé.

480. Dès l'instant où l'ensemble des garanties de l'article 89.1 du RGPD sont effectivement respectées, les données médicales peuvent donc être requalifiées en données de recherche et subséquemment exploitées pour toute étude dans le domaine de la santé. Ce nouveau traitement, poursuivant une nouvelle finalité, doit néanmoins satisfaire aux exigences de licéité édictées par le droit à la protection des données avant sa mise en œuvre. Quand bien même les différentes finalités du traitement des données médicales sont présumées compatibles, l'appréciation de la conformité de toute recherche n'impliquant pas la personne humaine au droit positif en vigueur doit être examinée pour chaque nouveau

¹⁶³² Voir: arrêt Mercier 1936 ; article R.4127-32 du code de la santé publique.

¹⁶³³ Cf. Paragraphe 487.

¹⁶³⁴ Sauf si le traitement est conforme à une méthodologie de référence ou s'il est réalisé par les seuls professionnels dépositaires du secret médical ayant assuré la prise en charge sanitaire du patient pour les besoins de leur activité médicale ou paramédicale.

¹⁶³⁵ Article 35 du RGPD.

¹⁶³⁶ Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, *op. cit.*, p. 33.

¹⁶³⁷ Cf. Paragraphe 476.

projet. Simplement, la requalification des données médicales en données de recherche favorise le développement de l'innovation dans le domaine de la santé sans qu'il n'y ait besoin de procéder à une collecte spécifique de données médicales auprès des personnes physiques. A défaut, seule la catégorie des recherches impliquant la personne humaine règnerait.

481. Eu égard à la présomption de compatibilité des traitements ultérieurs à des fins de recherche scientifique, les données médicales du patient se trouvent systématiquement requalifiées en données de recherche. En 2017, Marie-France Mamzer Bruneel et Christian Hervé avertissaient que « *l'installation progressive de cette porosité entre le soin et la recherche pourrait rapidement aboutir à la disparition complète de toute frontière entre ces deux pratiques, le soin alimentant quotidiennement la recherche* »¹⁶³⁸. Il faut alors comprendre que le patient qui consent à sa prise en charge sanitaire se voit tacitement contraint de produire des données de recherche et, consécutivement, de participer aux études présentant un motif d'intérêt public dans le domaine de la santé. Pourtant, lorsqu'il est malade, le patient n'a pas d'autre choix que de se faire soigner. Dès lors, la systématisation de la requalification des données médicales ne constituerait-elle pas un abus de vulnérabilité ? Les relations entre les patients concernés et les exploitants des données de recherche est-elle suffisamment équilibrée pour considérer que cette finalité ultérieure est compatible avec la prise en charge sanitaire ?

Avant d'étudier spécifiquement les droits du patient sur ses données de recherche, il convient de préciser que le volume des données de recherche ainsi disponible décuple les capacités des chercheurs et accroît le développement de l'innovation en santé. Certainement, les données médicales « *sont le matériau de recherche de base pour les scientifiques* »¹⁶³⁹. Leur exploitation représente donc « *une véritable source d'avancées scientifiques et de nouvelles connaissances tout en permettant de créer de la valeur grâce à l'innovation* »¹⁶⁴⁰. Inévitablement, « *le progrès de la connaissance au service de la santé et de la société passe par l'accès, l'utilisation et le partage de ces données dans le respect de la protection des*

¹⁶³⁸ MAMZER BRUNEEL (M.-F.), HERVE (C.), *op. cit.*, p. 87.

¹⁶³⁹ LESAULNIER (F.), *Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données*, Médecine & Droit, 2019, n°158, p. 103.

¹⁶⁴⁰ VAYR (J.), *Les données de santé : un enjeu pour le futur*, LPA, septembre 2016, n°120, p. 4.

personnes ». ¹⁶⁴¹ La requalification des données médicales en données de recherche présente incontestablement des enjeux considérables pour l'intérêt public dans le domaine de la santé. *In fine*, cette nécessité au bénéfice du plus grand nombre pourrait proportionnellement contrebalancer les intérêts en présence dès lors que la réutilisation des données médicales personnelles est protégée au moyen de garanties appropriées.

482. Toutefois, bien que ces recherches n'impliquent pas la personne humaine, l'éloignement entre le patient concerné et ses données de recherche existe-t-il réellement ? Il ne fait aucun doute que cette donnée requalifiée n'est jamais véritablement distanciée du patient qui en est la source. Evidemment, la donnée de recherche n'est autre que la chose anthropomorphique du patient. En tant qu'élément de réification de la condition physiologique du patient, elle se situe au point de tangence entre les attributs de la personnalité et les attributs du corps humain ¹⁶⁴². Elle touche donc directement et imprescriptiblement à la dignité de son hôte. La généralisation de la requalification des données médicales et ses « *conséquences sur la personne humaine et les rapports qu'elle entretient avec son corps et la société mériteraient d'être pensées, dans une approche d'éthique anticipative, compte tenu des attendus de nos sociétés dans lesquelles la multiplication des fragilités pousse les patients et leurs familles à réclamer plus d'humanité* » ¹⁶⁴³. L'édification d'un statut particulier à la donnée médicale apparaît, là encore, comme une solution satisfaisante. En premier lieu, la qualification d'une « chose anthropomorphique » permettrait de considérer l'humanité inhérente à cette catégorie de données singulièrement intimes et de lui attacher un régime juridique respectueux de ses caractéristiques ¹⁶⁴⁴. En second lieu, la donnée médicale systématiquement requalifiée en données de recherche deviendrait une chose anthropomorphique commune et tomberait automatiquement dans un unique domaine commun informationnel. La centralisation de ces éléments empreints d'humanité et l'instauration d'une gouvernance *ad hoc* garantiraient leur intégrité, leur confidentialité, leur sécurisation, leur contrôle et leur traçabilité.

¹⁶⁴¹ LESAULNIER (F.), *loc. cit.*

¹⁶⁴² Cf. Paragraphe 356.

¹⁶⁴³ MAMZER BRUNEEL (M.-F.), HERVE (C.), *op. cit.*, p. 87.

¹⁶⁴⁴ Cf. Chapitre 1 du Titre 1 de la Partie 2 de la présente thèse.

Section 1 : Les prérogatives du patient à l'égard de ses données de recherche utilisées pour un motif d'intérêt public dans le domaine de la santé

483. Eu égard à l'introduction de la notion de transparence dans le droit à la protection des données personnelles, le responsable de traitement doit absolument respecter ses obligations d'information et d'instruction des droits exercés par les personnes concernées.

En premier lieu, le patient doit être scrupuleusement informé de la requalification de ses données médicales en données de recherche d'une part, et de chaque opération de traitement subséquente d'autre part (**Paragraphe 1**). Concrètement, le patient doit, le cas échéant, être informé de l'intégration de ses données médicales dans une base de mégadonnées disponibles pour la recherche et l'innovation en santé, ainsi que de leur implémentation dans un jeu de données de recherche spécifique à un projet ponctuel et déterminé.

En deuxième lieu, le principe de transparence exige que le patient soit informé des droits qu'il détient sur ses données de recherche ainsi que de leurs modalités pratiques d'exercice. Qu'elles soient implémentées dans le système national des données de santé, dans un entrepôt de données de santé ou simplement extraites de ses dossiers médicaux pour un projet de recherche spécifique, les prérogatives qui lui sont effectivement reconnues vis-à-vis de ses données de recherche apparaissent atténuées en raison des caractéristiques qui lui sont inhérentes et du contexte de leur traitement (**Paragraphe 2**).

Paragraphe 1 : Le droit à l'information relative à l'utilisation des données de recherche

484. En vertu des dispositions spécifiques de l'article 69 de la loi Informatique et Libertés modifiée, le patient concerné par le traitement des données concernant sa santé doit, théoriquement, en être informé individuellement (**A**). Partant, il incombe légalement au responsable de l'exploitation des données de recherche d'organiser l'information individuelle de chaque patient intéressé. Seulement, ce principe est assorti d'exceptions. En effet, lorsque l'obligation d'information individuelle ne fait pas l'objet d'une dérogation juridique, les modalités de sa diffusion peuvent également connaître des aménagements (**B**).

A) Le principe de l'information individuelle et spécifique complémentaire à l'information générale

485. Préalablement à la mise en œuvre de toute exploitation de données à caractère personnel, les personnes concernées doivent être informées des caractéristiques essentielles du traitement envisagé ainsi que de l'existence de leurs droits¹⁶⁴⁵. Les principes de loyauté¹⁶⁴⁶ et de transparence¹⁶⁴⁷ à l'égard des personnes concernées résonnent directement dans le droit à l'information. En effet, ce droit capital de la protection des données oblige les responsables de traitement à fournir un certain nombre d'informations à propos de chaque traitement de données personnelles correspondant à une finalité déterminée. Ainsi, les personnes sont averties que les informations qui les concernent feront l'objet d'un traitement spécifique à une finalité définie. Consécutivement, elles devraient pouvoir garder le contrôle et la maîtrise de leurs usages. Pour cela, les informations doivent lui être délivrées de façon concise, en des termes clairs et simples les rendant compréhensibles et aisément accessibles dans un format lisible¹⁶⁴⁸. Il appartient donc au responsable de traitement d'employer tous les moyens permettant de garantir la bonne information des individus. Si l'information du patient concerné par le traitement de ses données médicales aux fins de sa prise en charge sanitaire ne pose pas de difficulté lorsque cette chose anthropomorphique est directement recueillie auprès de celui-ci¹⁶⁴⁹, quelles sont les modalités de délivrance de l'information relative à leur requalification en données de recherche et à leur réutilisation pour une finalité secondaire ? S'agissant de traitements portant sur des données sensibles dans le domaine de la santé, le législateur français a introduit des conditions relatives au droit à l'information supplémentaires à celles prescrites par le RGPD. La détermination des procédés d'information des patients concernés par la réutilisation de leurs données médicales à des fins de recherche scientifique implique donc la combinaison des dispositions nationales et européennes.

¹⁶⁴⁵ CE, 24 août 2011, n°336382, *HSBC Private Bank (Suisse) SA*, Rec. Lebon T., p. 939 ; RJEP, 2012, n° 699, comm. 40, J. Boucher ; Dr. Fisc., 2018, n° 45, comm. 443, E. Crépey.

¹⁶⁴⁶ Article 5.1 a) du RGPD.

¹⁶⁴⁷ Article 12 du RGPD.

¹⁶⁴⁸ Article 12 du RGPD.

¹⁶⁴⁹ Cf. Paragraphe 466.

486. Les données médicales personnelles sont recueillies et produites par l'ensemble des professionnels participant à la prise en charge sanitaire du patient¹⁶⁵⁰. A cet instant, le patient doit recevoir une information lui expliquant que le traitement de ses données médicales est notamment indispensable à la constitution et à l'alimentation de ses dossiers médicaux et, plus particulièrement, à l'élaboration des diagnostics médicaux, à la dispensation, à la continuité et à la coordination de ses soins, ainsi qu'à l'administration de ses thérapeutiques. Cette première information porte sur des traitements s'inscrivant directement dans la lignée de la finalité initiale, explicite et déterminée qu'est la prise en charge sanitaire. En complément, le responsable de traitement doit, le cas échéant, alerter le patient concerné du fait que ses données personnelles pourront éventuellement être traitées pour une finalité ultérieure différente. Au moment de la spécification de la finalité initiale afférente à la prise en charge sanitaire du patient, l'établissement ou le professionnel de santé responsable de traitement a conscience que les données médicales ainsi collectées seront très certainement requalifiées en données de recherche. Effectivement, les données médicales représentent la ressource essentielle aux recherches, aux études et aux évaluations dans le domaine de la santé. Alors, en considération d'une approche formelle de l'évaluation de la compatibilité des finalités¹⁶⁵¹, le responsable de traitement peut généralement informer les patients concernés que leurs données médicales seront possiblement réutilisées à des fins de recherche scientifique présentant un motif d'intérêt public dans le domaine de la santé. L'information générale concernant cette possibilité est délivrée au moment de la collecte des données médicales auprès du patient à l'occasion de sa prise en charge sanitaire¹⁶⁵². Au demeurant, si cette éventualité venait à se concrétiser, une information spécifique à cette nouvelle finalité de recherche devrait être délivrée à tout patient concerné.

487. En effet, « lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité »¹⁶⁵³. En application de l'article 69 de la loi Informatique et Libertés modifiée, le patient concerné par l'utilisation effective

¹⁶⁵⁰ Cf. Paragraphes 50 à 53.

¹⁶⁵¹ Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, op. cit., p. 21.

¹⁶⁵² Article 13.1 du RGPD.

¹⁶⁵³ Article 14.4 du RGPD.

de ses données de recherche bénéficie d'un droit d'information devant être préalablement délivrée individuellement, à moins qu'il n'ait entendu faire usage du droit d'être laissé dans l'ignorance d'un diagnostic ou d'un pronostic. L'emploi de l'adverbe « individuellement » signifie que l'information doit être remise séparément à chaque personne concernée. En effet, le terme individuel s'oppose à la collectivité et désigne ce « *qui est conçu pour une seule personne* »¹⁶⁵⁴. En conséquence, la CNIL considère qu'avant toute exploitation des données de recherche, la notice d'information individuelle doit être remise en main propre au patient concerné ou envoyée par courrier postal à sa dernière adresse connue¹⁶⁵⁵.

488. Cette exigence, dans le mode de transmission de l'information relative au traitement des données de recherche, paraît surprenante. En effet, l'article 69 de la loi Informatique et Libertés modifiée précise que les patients concernés doivent être « *individuellement informés conformément aux dispositions du règlement (UE) 2016/679 du 27 avril 2016* ». Seulement, aucune disposition du RGPD ne consacre formellement un mode individuel d'information. A l'inverse, ce règlement européen exige que toute personne concernée soit effectivement informée de chacune des finalités du traitement de ses données personnelles ; et tout procédé d'information peut être utilisé pour y parvenir. Autrement dit, le mode de délivrance de l'information est libre, l'essentiel étant que son support puisse être adapté au contexte de la collecte des données et à la forme du traitement. Effectivement, l'article 12 du RGPD dispose que « *le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 [...] en ce qui concerne le traitement à la personne concernée* ». Le législateur européen se soucie davantage des caractéristiques de l'information que des modalités de sa délivrance. Il importe uniquement que l'information soit donnée « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant* »¹⁶⁵⁶. A cet égard, elle peut être accompagnée « *d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu* »¹⁶⁵⁷. A la lumière du RGPD, il est donc important qu'une information

¹⁶⁵⁴ Définition du dictionnaire Larousse. Disponible en ligne sur le site [www.larousse.fr]. Consulté le 21 septembre 2021.

¹⁶⁵⁵ CNIL, *Recherche médicale : quel est le cadre légal ?* 10 décembre 2018. Disponible en ligne sur le site [www.cnil.fr]. Consulté le 21 septembre 2021.

¹⁶⁵⁶ Article 12.1 du RGPD.

¹⁶⁵⁷ Article 12.7 du RGPD.

intelligible et transparente soit portée à la connaissance de la personne concernée, cela de quelle que manière que ce soit. Cependant, en précisant qu'elle devait être fournie individuellement, le législateur national semble avoir introduit une modalité particulière de délivrance de l'information portant sur la réutilisation des données relatives à la santé. L'information délivrée collectivement ne devrait donc être qu'une exception au principe de l'information individuelle. Il importe alors de distinguer l'information collective de l'information générale et l'information individuelle de l'information spécifique. Véritablement, une information à caractère général peut être délivrée individuellement tandis qu'une information spécifique à une finalité déterminée peut être délivrée collectivement.

489. Cette information individuelle, concernant l'exploitation des données de recherche pour une finalité déterminée, doit être fournie au patient préalablement à la mise en œuvre du traitement¹⁶⁵⁸. En effet, lorsque des données personnelles sont traitées pour une finalité différente de celle pour laquelle elles ont été collectées, « *le G29 précise que l'information doit avoir lieu dans un délai préalable raisonnable* »¹⁶⁵⁹. Cependant, ni le législateur, ni la jurisprudence, ni la doctrine juridique ne renseignent d'unité temporelle permettant de mesurer cette échéance.

Concrètement, « *la définition d'une période raisonnable dépendra des circonstances particulières* »¹⁶⁶⁰ du traitement et son responsable doit être « *en mesure de démontrer que les délais raisonnables déterminés pour la communication de ces informations sont justifiés eu égard aux circonstances et que les délais dans l'ensemble sont équitables pour les personnes concernées* »¹⁶⁶¹. Véritablement, l'instauration d'un espacement entre la délivrance de l'information et la réutilisation effective des données personnelles tend à « *permettre à la personne d'exercer ses droits avant la mise en œuvre du traitement ultérieur* »¹⁶⁶² dont, en particulier, son éventuel droit d'opposition. Dès lors, l'intervalle entre la fourniture de l'information et la réutilisation des données personnelles

¹⁶⁵⁸ Conformément à l'article 14.4 du RGPD.

¹⁶⁵⁹ GAULLIER (F.), *op. cit.*, § 29.

¹⁶⁶⁰ Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, 29 novembre 2017, actu. 11 avril 2018, p. 29

¹⁶⁶¹ Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, WP260 rev.01, adoptées le 29 novembre 2017, version révisée et adoptée le 11 avril 2018, p. 29

¹⁶⁶² GAULLIER (F.), *loc. cit.*

pourrait réciproquement être calquée sur le délai d'un mois pendant lequel le responsable de traitement doit répondre à la demande d'exercice des droits formulée par la personne concernée¹⁶⁶³. D'une part, ce délai apparaît suffisant pour que le patient bénéficie de la bonne compréhension de la finalité de recherche poursuivie, en mesure les enjeux, et prenne le temps nécessaire à la réflexion. D'autre part, ce laps de temps semble raisonnablement pondéré pour ne pas emboliser les exigences méthodologiques de la recherche et décourager les porteurs de projets présentant un motif d'intérêt public dans le domaine de la santé. Ainsi, l'exploitant des données de recherche du patient devrait l'en informer individuellement au moment où il a l'intention de les utiliser pour une finalité particulière. Par suite, le traitement pourrait concrètement débiter au terme d'un délai d'un mois à compter de la remise de l'information. Pour des raisons pratiques et pragmatiques, il semblerait opportun d'opter pour la théorie de l'émission dans la mesure où l'information individuelle peut toutefois être délivrée sous différentes formes qui ne rendent pas toujours compte de la date effective de sa réception.

490. S'il incombe à l'exploitant des données de recherche d'informer individuellement les patients concernés avant la mise en œuvre du traitement, comment peut-il adresser une notice d'information à des personnes physiques dont il ignore l'identité ?

Il est intéressant de rappeler que l'exploitant des données de recherche n'est autorisé à accéder qu'à des données médicales pseudonymisées et strictement minimisées à ce qui est nécessaire à la finalité scientifique justifiée dans le protocole de recherche¹⁶⁶⁴. En effet, seuls les professionnels ayant participé à la prise en charge médicale du patient, et soumis à une obligation de secret professionnel, ont connaissance de l'état civil et des coordonnées du patient. Ils sont ainsi les seuls à pouvoir « *conserver le lien entre l'identité codée des personnes concernées par la recherche et leurs nom(s) et prénom(s)* »¹⁶⁶⁵. Par conséquent, nous déduisons que le détenteur de la table de correspondance des pseudonymes est l'unique protagoniste à pouvoir individuellement informer les patients concernés par l'utilisation de leurs données de recherche. Pourtant, le professionnel ayant produit les données médicales du patient à l'occasion de sa prise en charge sanitaire n'intervient pas en qualité de

¹⁶⁶³ Article 12.3 du RGPD.

¹⁶⁶⁴ Cf. Paragraphe 440.

¹⁶⁶⁵ CNIL, Délibération n° 2018-155 du 3 mai 2018, *loc. cit.*

responsable du traitement à des fins de recherche lorsqu'il n'en est pas le promoteur. En effet, le détenteur des données médicales nominatives intervient en qualité de sous-traitant de ce traitement. En transmettant les données médicales pseudonymisées indispensables à la recherche, il agit au nom et pour le compte du promoteur du projet qui assume la responsabilité du traitement. Alors, comment l'obligation d'information individuelle et préalable peut-elle incomber au gardien des données médicales nominatives ?

Lorsque le responsable de la recherche fait appel à un sous-traitant, en l'occurrence l'établissement ou le professionnel de santé détenteur des données médicales nominatives, un acte juridique littéral régissant le traitement et répartissant les droits et les obligations des parties doit être conclu¹⁶⁶⁶. Notamment, il appartient au sous-traitant d'aider le responsable de traitement à respecter l'effectivité des droits de la personne concernée¹⁶⁶⁷. A cet effet, le contrat de sous-traitance peut prévoir que l'obligation d'information relative au traitement réalisé par le responsable de traitement soit acquittée par le sous-traitant¹⁶⁶⁸. En revanche, « *la formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données* »¹⁶⁶⁹. Si la délivrance de l'information individuelle des patients concernés repose contractuellement sur le gardien de la table de correspondance, la responsabilité juridique de cette obligation légale revient tout de même au promoteur responsable du traitement. En définitive, la fourniture de l'information individuelle nécessite toujours l'intervention d'un intermédiaire dépositaire du secret professionnel médical entre les patients concernés et les exploitants de leurs données de recherche¹⁶⁷⁰. Identiquement, lorsque les données de recherche utilisées par le promoteur d'une étude dans le domaine de la santé proviennent du SNDS ou d'un entrepôt de données de santé, le responsable de traitement doit requérir l'aide du responsable de la base de données et déterminer « *l'action à réaliser en fonction de sa capacité à contacter les personnes concernées* »¹⁶⁷¹.

¹⁶⁶⁶ Article 28.3 du RGPD.

¹⁶⁶⁷ Article 28.3 e) du RGPD.

¹⁶⁶⁸ CNIL, *Règlement européen sur la protection des données personnelles : Guide du sous-traitant*, septembre 2017, p. 15.

¹⁶⁶⁹ CNIL, *Règlement européen sur la protection des données personnelles : Guide du sous-traitant*, septembre 2017, p. 15.

¹⁶⁷⁰ Sauf à ce que la recherche n'impliquant pas la personne humaine soit effectuée par les professionnels de santé ayant généré les données médicales du patient à l'occasion de sa prise en charge sanitaire.

¹⁶⁷¹ Health Data Hub, *Guide pédagogique - note d'information aux personnes*, p. 5.

491. L'information relative à l'intégration des données médicales au sein d'une base de données destinée à leur réutilisation ultérieure à des fins de recherche doit être réalisée avec l'aide du professionnel de santé fournisseur de la chose anthropomorphe. Le responsable d'un entrepôt de données de santé qui souhaite y inclure les informations médicales contenues dans les dossiers médicaux du patient doit, au préalable, l'en informer individuellement¹⁶⁷² avec, le cas échéant, l'aide de son sous-traitant. De même, la Caisse nationale de l'assurance maladie (CNAM), en tant que responsable du SNDS, doit réaliser « une information individuelle, par voie papier ou électronique, relative à la mise en œuvre du système national des données de santé permettant de porter directement à la connaissance des personnes les principales caractéristiques de ce dispositif »¹⁶⁷³. Cette information individuelle relative à l'intégration des données médicales au sein d'un entrepôt de données de santé ou du SNDS doit être distinguée de l'information individuelle préalable devant être délivrée pour chaque recherche n'impliquant pas la personne humaine réalisée à partir des données intégrées dans ces bases.

492. Le professionnel sous-traitant doit donc, au nom et pour le compte du responsable de traitement, informer individuellement chaque patient inclus dans le protocole de recherche. Cependant, lorsque le patient concerné est un majeur protégé par une mesure de tutelle, d'habilitation familiale ou par un mandat de protection future, l'information relative au traitement de ses données de recherche doit être adressée à la personne physique ou morale en charge de sa représentation dès lors qu'il n'est pas en état de prendre seul une décision personnelle éclairée¹⁶⁷⁴. Quand le patient concerné par le traitement est un mineur, cette même information doit être délivrée aux titulaires de l'exercice de l'autorité parentale, ou à l'un d'entre eux s'il apparaît impossible d'en informer l'autre¹⁶⁷⁵.

493. Néanmoins, il convient de noter qu'en matière de traitement de données personnelles réalisé à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, le mineur

¹⁶⁷² CNIL, *Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?*, 28 novembre 2019.

¹⁶⁷³ Article R.1461-9 I du code de la santé publique.

¹⁶⁷⁴ Article 70 alinéa 1 de la loi Informatique et Libertés modifiée.

¹⁶⁷⁵ Article 70 alinéa 2 de la loi Informatique et Libertés modifiée.

âgé de quinze ans et plus est autorisé à exercer seul ses droits. En effet, le législateur dispose que « *le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale aient accès aux données le concernant recueillies au cours de la recherche, de l'étude ou de l'évaluation. Le mineur reçoit alors l'information et exerce seul ses droits* »¹⁶⁷⁶. Le législateur poursuit que « *le mineur âgé de quinze ans ou plus peut s'opposer à ce que les titulaires de l'exercice de l'autorité parentale soient informés du traitement de données si le fait d'y participer conduit à révéler une information sur une action de prévention, un dépistage, un diagnostic, un traitement ou une intervention pour laquelle le mineur s'est expressément opposé à la consultation des titulaires de l'autorité parentale, en application des articles L. 1111-5 et L. 1111-5-1 du code de la santé publique, ou si les liens de famille sont rompus et que le mineur bénéficie à titre personnel [...] d'une couverture maladie universelle* »¹⁶⁷⁷.

Alors que l'exercice du droit pour le mineur d'obtenir des soins confidentiels et d'en conserver le secret n'est soumis à aucune limite d'âge, les représentants légaux d'un mineur de moins de quinze ans doivent systématiquement être informés de sa participation à une recherche n'impliquant pas la personne humaine, quand bien même cette information conduirait à leur révéler qu'un acte médical a été dispensé à leur insu. Il est important de préciser que l'inclusion d'un sujet de recherche dans une étude rétrospective intervient postérieurement à sa prise en charge médicale. En effet, une étude rétrospective dans le domaine de la santé est fondée sur la réutilisation des données médicales collectées au cours des soins, le cas échéant prodigués dans le secret. Alors que la confidentialité des données collectées à l'occasion de la prise en charge sanitaire d'un mineur lui est assurée à un moment déterminé, l'opposition du secret peut néanmoins être levée dès lors que la recherche, l'étude ou l'évaluation requiert la réutilisation des données médicales du mineur de moins de quinze ans. D'une part, cette révélation briserait le secret dû au mineur et la confiance de la relation médicale. D'autre part, cette divulgation pourrait dégrader les rapports entre le mineur et ses représentants légaux. Dès lors, il apparaît absolument indispensable d'uniformiser le corpus normatif régissant les conditions du droit d'opposition du mineur à l'information de ses représentants légaux ainsi que de leur accès aux données médicales ou de recherche le concernant.

¹⁶⁷⁶ Article 70 alinéa 3 de la loi Informatique et Libertés modifiée.

¹⁶⁷⁷ Article 70 alinéa 4 de la loi Informatique et Libertés modifiée.

494. Quel que soit le destinataire du droit à l'information, les mentions qu'elle comporte doivent toujours correspondre au champ défini au quatrième alinéa de l'article 14 du RGPD. Le législateur européen a périmétré le contenu de l'information relative au traitement des données personnelles selon qu'elles aient été collectées auprès de la personne concernée¹⁶⁷⁸ ou à partir d'une autre source. Les recherches n'impliquant pas la personne humaine consistent en l'analyse rétrospective de données déjà recueillies à l'occasion d'une finalité initiale compatible. Par nature, ces recherches rétrospectives sont donc effectuées à partir de données médicales collectées auprès d'une autre source que la personne concernée. En effet, il peut s'agir de données médicales conservées au sein des dossiers médicaux du patient ou d'un entrepôt de données de santé dédié à la recherche. Il peut également être question de données de recherche notamment collectées à l'occasion d'une recherche impliquant la personne humaine ou d'une étude prospective de cohorte.

Lorsque les données personnelles n'ont pas été collectées auprès de la personne concernée, et dans l'hypothèse d'une réutilisation pour une finalité autre que celle ayant justifié leur recueil, l'information de la personne concernée doit contenir des explications au sujet de cette nouvelle finalité ainsi que « *toute autre information pertinente visée au paragraphe 2* »¹⁶⁷⁹ de l'article 14 du RGPD. Dans la formulation de la notice d'information, le responsable de traitement et le sous-traitant doivent alors renseigner les finalités déterminées du traitement ultérieur des données médicales, la durée pendant laquelle elles seront conservées¹⁶⁸⁰, les intérêts légitimes poursuivis par l'exploitant lorsqu'ils fondent la base légale du traitement¹⁶⁸¹, l'existence des droits effectifs de la personne concernée¹⁶⁸², le droit de retirer le consentement à tout moment lorsqu'il fonde ou autorise le traitement des données personnelles¹⁶⁸³, le droit d'introduire une réclamation auprès d'une autorité de

¹⁶⁷⁸ Dans ce cas le contenu de l'information doit être conforme aux dispositions de l'article 13 du RGPD.

¹⁶⁷⁹ Article 14.4 du RGPD.

¹⁶⁸⁰ Article 14.2 a) du RGPD.

¹⁶⁸¹ Article 14.2 b) du RGPD.

¹⁶⁸² Article 14.2 c) du RGPD.

¹⁶⁸³ Article 14.2 d) du RGPD.

contrôle¹⁶⁸⁴, la source d'où proviennent les données à caractère personnel¹⁶⁸⁵ et l'éventuelle existence d'une prise de décision automatisée¹⁶⁸⁶. En cas de traitement ultérieur pour une finalité différente de celle pour laquelle les données personnelles ont été obtenues, le législateur européen n'a pas estimé nécessaire de fournir les informations visées au premier paragraphe de l'article 14 du RGPD. Si le champ des informations du deuxième paragraphe permet de « *garantir un traitement équitable et transparent à l'égard de la personne concernée* »¹⁶⁸⁷, ces informations ne permettent pas d'identifier le responsable de traitement¹⁶⁸⁸, de connaître les coordonnées du délégué à la protection des données¹⁶⁸⁹, de déterminer les catégories de données personnelles concernées¹⁶⁹⁰, d'entrevoir leurs destinataires¹⁶⁹¹, ni d'apprécier le fait qu'elles feront l'objet d'un transfert vers un pays tiers à l'Union européenne¹⁶⁹². Pourtant, cet ensemble d'informations s'avère indispensable pour circonscrire le contexte du traitement des données personnelles, essentiel pour gagner la confiance des patients concernés par le traitement de leurs informations intimes, et fondamental pour l'exercice de leur autodétermination informationnelle. Si l'information dispensée au patient doit être conforme aux dispositions de l'article 14 du RGPD, aucune norme juridique n'interdit la fourniture d'informations supplémentaires à celles énumérées au deuxième paragraphe de l'article susvisé. Au demeurant, le législateur national devrait préciser, au sein des dispositions particulières aux recherches n'impliquant pas la personne humaine de la loi Informatique et Libertés modifiée¹⁶⁹³, que le contenu de l'information préalable délivrée individuellement à la personne concernée par la réutilisation de ses données médicales devrait être conforme aux deux premiers paragraphes de l'article 14 du RGPD.

¹⁶⁸⁴ Article 14.2 e) du RGPD.

¹⁶⁸⁵ Article 14.2 f) du RGPD.

¹⁶⁸⁶ Article 14.2 g) du RGPD.

¹⁶⁸⁷ Article 14.2 du RGPD.

¹⁶⁸⁸ Article 14.1 a) du RGPD.

¹⁶⁸⁹ Article 14.1 b) du RGPD.

¹⁶⁹⁰ Article 14.1 d) du RGPD.

¹⁶⁹¹ Article 14.1 e) du RGPD.

¹⁶⁹² Article 14.1 f) du RGPD.

¹⁶⁹³ Sous-section 2 de la Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

Assurément, l'information constitue la clé de la protection des données personnelles et équivaut au premier des droits de la personne concernée. Une information complète, loyale et transparente représente une condition *sine qua non* à la maîtrise des usages de ses données personnelles, *a fortiori* lorsqu'elles ne sont pas directement collectées auprès de la personne concernée. Certainement, sans cette information, personne ne pourrait jamais supposer que les informations qui le concernent font l'objet d'une exploitation pour une finalité inconnue. En dépit de cette impérieuse nécessité, le droit à l'information est accompagné de tempéraments juridiques et de difficultés pratiques.

B) La dissipation de l'information individuelle relative à l'utilisation des données de recherche

495. Ainsi que l'explique Frédérique Lesaulnier, « *l'exigence d'une information individuelle et spécifique à chaque projet issu de ces données [...] est difficilement compatible avec les projets reposant sur une réutilisation secondaire renouvelée et réitérée de données* »¹⁶⁹⁴. En raison de ces difficultés pratiques, des tempéraments à cette obligation d'information individuelle peuvent être envisagés. Pourtant, l'absence d'information des patients concernés préalablement à un traitement de données à des fins de recherche n'impliquant pas la personne humaine constitue une infraction pénalement sanctionnée à l'article 226-19-1 du code pénal.

496. Quand les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, la délivrance d'une information individuelle peut s'avérer insurmontable pour des raisons tenant au nombre important de personnes concernées, à la méconnaissance de leurs coordonnées ou encore à l'ancienneté des informations réutilisées¹⁶⁹⁵. Compte de tenu des circonstances dans lesquelles les données personnelles ont été recueillies, le législateur européen a exceptionnellement admis que l'information ne puisse pas être adressée à la personne concernée par le traitement des informations qui la concernent. Quoi qu'il advienne, l'application de cette dérogation à l'obligation d'information doit être inhérente « *au fait que les données à caractère personnel ont été collectées autrement qu'auprès de la personne*

¹⁶⁹⁴ LESAULNIER (F.), *op. cit.*, p. 108.

¹⁶⁹⁵ Considérant 62 du RGPD.

concernée »¹⁶⁹⁶ d'une part, et conforme à l'une des situations décrites à l'article 14.5 du RGPD d'autre part.

Dans le domaine des recherches n'impliquant pas la personne humaine, la réunion des conditions de cette exception doit être vérifiée par la CNIL. Cette autorité de contrôle a compétence pour statuer sur les demandes de dérogation à l'obligation d'information adressées par les promoteurs responsables d'un projet de recherche. Quand le responsable de la recherche ne se trouve pas en capacité d'informer individuellement les personnes concernées, notamment lorsqu'il n'est pas responsable de la base de données de recherche qu'il utilise, et que la délivrance de l'information individuelle repose contractuellement sur le sous-traitant détenteur de la table de correspondance des pseudonymes, la demande de dérogation à l'obligation de l'information individuelle ainsi que la justification des conditions de cette exception doivent toujours être fournies par le promoteur de la recherche dans le domaine de la santé. Dans le cas où le porteur du projet de recherche ne peut satisfaire à son obligation d'information individuelle, il lui appartient donc de détailler, au sein du protocole de recherche : le motif réglementaire invoqué au soutien de sa demande, la mise en balance entre le motif allégué et les conséquences engendrées par l'absence d'information pour la personne concernée, ainsi que les mesures compensatoires adoptées pour protéger les droits, les libertés et les intérêts légitimes des individus¹⁶⁹⁷.

497. Dans l'hypothèse où la fourniture de l'information individuelle préalable à la mise en œuvre du projet de recherche se révèle impossible pour le promoteur¹⁶⁹⁸, il lui appartient de « démontrer quels facteurs l'empêchent effectivement de communiquer les informations en question à la personne concernée »¹⁶⁹⁹. Sans aucun doute, cette impossibilité doit être certaine et absolue pour lui-même, ou pour le sous-traitant dépositaire de la clé de réidentification des données de recherche pseudonymisées. Dès l'instant où il existe une quelconque possibilité d'informer individuellement les personnes concernées, ou lorsque l'un des facteurs ayant généré l'impossibilité disparaît, le responsable de traitement doit alors

¹⁶⁹⁶ Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, op. cit., p. 35 à p. 36.

¹⁶⁹⁷ Health Data Hub, *Guide pédagogique - note d'information aux personnes*, p. 9.

¹⁶⁹⁸ Article 14.5 b) du RGPD.

¹⁶⁹⁹ Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, op. cit., p. 34.

immédiatement communiquer l'information aux patients intéressés¹⁷⁰⁰. Cette impossibilité sans réserve concerne notamment les situations dans lesquelles ni le responsable de traitement, ni le sous-traitant ne disposent, d'aucune manière que ce soit, ni de l'identité, ni des coordonnées des personnes concernées.

498. Lorsque la délivrance de l'information individuelle apparaît possible mais qu'elle exigerait des efforts disproportionnés pour le responsable de traitement – ou pour son sous-traitant –, la CNIL peut aussi l'autoriser à s'affranchir de cette obligation¹⁷⁰¹. Le promoteur de la recherche doit alors démontrer en quoi les moyens employés pour informer individuellement les patients concernés apparaissent manifestement excessifs. En outre, il lui incombe de justifier que « *les effets sur la personne concernée dans le cas où celle-ci ne recevrait pas ces informations* »¹⁷⁰² seront compensés par la mise en place de mesures adéquates.

La première des mesures compensatoires à introduire consiste dans la diffusion collective de la notice d'information au public. Dans ses lignes directrices, le G29 suggère, par exemple, de publier les informations sur le site internet du responsable de traitement ou de son sous-traitant, de les afficher dans leurs locaux, ou encore de les communiquer par voie de presse¹⁷⁰³. En complément de cette diffusion publique de l'information, le responsable de traitement doit, selon les circonstances du traitement, réaliser une analyse d'impact relative à la protection des données, procéder à la pseudonymisation des données à caractère personnel, limiter le nombre d'informations collectées et réduire leur période de conservation¹⁷⁰⁴. Cette situation dérogatoire trouve particulièrement à s'appliquer aux traitements à des fins de recherche scientifique dans le domaine de la santé¹⁷⁰⁵, sous réserve de l'instauration des garanties appropriées décrites à l'article 89.1 du RGPD.

¹⁷⁰⁰ Groupe de travail «Article 29», *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, *op. cit.*, p. 34.

¹⁷⁰¹ Article 14.5 b) du RGPD.

¹⁷⁰² Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, *op. cit.*, p. 36.

¹⁷⁰³ Groupe de travail « Article 29 », *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, *op. cit.*, p. 36 à p. 37.

¹⁷⁰⁴ *Ibid.*

¹⁷⁰⁵ Groupe de travail «Article 29», *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, *op. cit.*, p. 35.

Vraisemblablement, les mesures compensatoires à l'absence d'information¹⁷⁰⁶ correspondent aux garanties appropriées aux traitements à des fins de recherche scientifique dans le domaine de la santé¹⁷⁰⁷. Paradoxalement, ces deux catégories de garanties poursuivent une finalité commune : la protection des droits et des libertés des personnes concernées en dépit des dérogations à l'exercice effectif de leurs droits sur leurs données personnelles.

499. Cette exception à l'obligation d'information individuelle concerne davantage les recherches rétrospectives réalisées à partir de données implémentées au sein d'un entrepôt de données de santé ou du système national des données de santé. D'abord, parce que ces bases tendent à regrouper des données massives pour la recherche. Ainsi, les promoteurs de recherches rétrospectives peuvent disposer d'un gigantesque volume de données dont l'analyse peut être effectuée à l'aide de puissants outils de traitement informatique¹⁷⁰⁸. En pratique, lorsque le responsable de la recherche accède à des données rattachées à plusieurs centaines de personnes concernées, la communication individuelle d'une notice d'information à chaque patient concerné par une étude de grande ampleur engagerait nécessairement des efforts disproportionnés. Ensuite, parce qu'il peut exister des difficultés à réidentifier les personnes concernées, particulièrement lorsque les données de recherche sont extraites du SNDS. En effet, ce système « *ne contient ni les noms et prénoms des personnes, ni leur numéro d'inscription au répertoire national d'identification des personnes physiques, ni leur adresse* »¹⁷⁰⁹. Afin de garantir la confidentialité des informations relatives à la santé des personnes concernées, l'intégralité des données personnelles relatives à une personne concernée sont alors pseudonymisées *via* « *un code non significatif obtenu par un procédé cryptographique irréversible du numéro d'inscription au Répertoire national d'identification des personnes physiques* » (NIR)¹⁷¹⁰. La fourniture d'une information individuelle préalable à l'utilisation des données du SNDS pour un projet de recherche spécifique exigerait de réattribuer la correspondance entre le pseudonyme et le NIR d'une part, puis de rechercher l'identité et les coordonnées de la personne concernée à partir de son NIR d'autre part. La mission de pseudonymisation des données personnelles incluses dans le

¹⁷⁰⁶ Article 14.5 b) du RGPD.

¹⁷⁰⁷ Cf. Paragraphe 478.

¹⁷⁰⁸ MAMZER BRUNEEL (M.-F.), HERVE (C.), *op. cit.*, p. 85.

¹⁷⁰⁹ Article L.1461-4 du code de la santé publique.

¹⁷¹⁰ Article R.1461-7 II a) du code de la santé publique.

SNDS étant dévolue à la CNAM, cet organisme serait le seul compétent pour corréler le pseudonyme et le NIR. En conséquence, tout utilisateur des données de recherche collectées dans le SNDS devrait prendre contact avec la CNAM afin d'organiser la fourniture de l'information individuelle et préalable des personnes concernées. S'il appartient à la CNAM d'informer individuellement les affiliés à l'Assurance maladie obligatoire de l'intégration de leurs données médicales au sein du SNDS, les efforts devant être employés pour informer individuellement chaque affilié de toute réutilisation spécifique des éléments immatériels de son corps humain peuvent toutefois apparaître excessifs. Partant, les utilisateurs des données du SNDS à des fins de recherche présentant un motif d'intérêt public dans le domaine de la santé peuvent être tentés de systématiquement solliciter une demande de dérogation à leur obligation d'information individuelle auprès de la CNIL.

Lorsque la délivrance de l'information se révèle impossible ou engage ainsi des efforts disproportionnés, « *la Commission rappelle qu'il appartiendra à chaque responsable de traitement souhaitant réaliser un traitement de données du SNDS de mettre en œuvre des mesures appropriées afin de rendre l'information publiquement disponible, laquelle ne pourra se limiter à l'inscription de son traitement au sein du portail de transparence de la Plateforme des données de santé* »¹⁷¹¹. Si l'information préalable ne peut être délivrée individuellement, l'information collective communiquée publiquement demeure toujours réalisable.

500. Dans l'hypothèse où ces exceptions à l'obligation d'information individuelle préalable sont appliquées, le traitement à des fins de recherche dans le domaine de la santé devient inéligible à la méthodologie de référence MR-004 adoptée et homologuée par la CNIL¹⁷¹². La conformité de la recherche à une méthodologie de référence présente plusieurs avantages. En effet, elle simplifie les formalités dans le domaine de la recherche et de l'innovation en santé afin de favoriser la compétitivité, elle instaure un cadre protecteur pour les patients concernés et elle permet de bénéficier d'un aménagement de l'information individuelle des personnes concernées par la recherche n'impliquant pas la personne humaine. Tandis que le responsable de traitement ne peut déroger à son obligation

¹⁷¹¹ CNIL, Délibération n° 2020-106 du 29 octobre 2020 portant avis sur un projet de décret relatif au système national des données de santé (demande d'avis n° 20011090), *JORF* n°0150, 30 juin 2021, texte n° 110.

¹⁷¹² CNIL, Délibération n° 2018-155 du 3 mai 2018, *loc. cit.*

d'information individuelle dans le cadre de la MR-004, la CNIL accommode les modalités de délivrance de l'information individuelle préalable.

Effectivement, il est prévu que « *des données [...] recueillies non spécifiquement pour la recherche peuvent faire l'objet d'une réutilisation sans qu'il soit procédé à une nouvelle information individuelle des personnes concernées [...] lorsque l'information délivrée lors de la collecte des données [...] prévoit la possibilité de réutiliser les données [...] et renvoie à un dispositif spécifique d'information auquel les personnes concernées pourront se reporter préalablement à la mise en œuvre de chaque nouveau traitement de données* »¹⁷¹³. Autrement dit, les données médicales du patient, produites à l'occasion de sa prise en charge sanitaire, peuvent être réutilisées conformément au cadre institué par la MR-004 sans qu'il ne soit nécessaire d'en informer individuellement les patients concernés. Cette exception est autorisée à la double condition que l'information délivrée à l'occasion de la collecte initiale des données médicales à des fins de prise en charge ait précisé que ces éléments immatériels pourront éventuellement faire l'objet d'une réutilisation pour un traitement ultérieur à des fins de recherche d'une part, et ait indiqué le procédé collectif d'information auquel les personnes concernées pourront se reporter avant la mise en œuvre de chaque nouveau traitement d'autre part.

Très concrètement, pour que cet aménagement puisse être institué, l'information relative à la possible réutilisation des éléments immatériels du corps humain du patient à des fins de recherche doit être anticipée par l'établissement ou le professionnel de santé l'ayant médicalement pris en charge. En effet, l'article 71 de la loi Informatique et Libertés modifiée dispose qu'une « *information relative aux dispositions de la présente sous-section doit être assurée notamment dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement mentionné au présent titre* ». De plus, cette information initiale délivrée lors de la prise en charge sanitaire du patient peut renvoyer au dispositif d'un site internet ou à la rubrique d'un journal dans lequel le responsable de traitement à des fins de prise en charge sanitaire communiquerait, au nom et pour le compte du responsable de la

¹⁷¹³ CNIL, Délibération n° 2018-155 du 3 mai 2018, *loc. cit.*

recherche, l'ensemble des projets présentant un motif d'intérêt public impliquant la réutilisation des données médicales des patients.

Lorsque l'information communiquée lors de la collecte initiale des données médicales satisfait à ces deux dispositions particulières, l'information collective préalable à la mise en œuvre d'une recherche rétrospective conforme à la MR-004 peut se substituer à la délivrance d'une information individuelle préalable. Finalement, l'aménagement de l'information individuelle revient à la mesure compensatoire consistant à rendre les informations publiques lorsqu'« *il est fait application de l'exception [à l'obligation d'information] prévue à l'article 14, paragraphe 5, point b) du RGPD* »¹⁷¹⁴. Pourtant, la lettre de la MR-004 explicite que la recherche rétrospective n'entre pas dans le champ d'application de cette méthodologie lorsqu'« *il est fait application de l'exception [à l'obligation d'information] prévue à l'article 14, paragraphe 5, point b) du RGPD* »¹⁷¹⁵. Paradoxalement, la mesure compensatoire à l'absence d'information des personnes concernées prévue par le RGPD¹⁷¹⁶ et l'aménagement de l'information individuelle permis par la MR-004 résident conjointement dans la diffusion d'une information disponible publiquement. Par conséquent, l'aménagement de l'information individuelle s'apparente à une dérogation à l'information individuelle. Qu'il s'agisse d'une dérogation ou d'un aménagement de l'information individuelle préalable à l'utilisation effective des données de recherche du patient, la dissipation de ce droit capital pour la protection des données personnelles semble partiellement corrigée par la diffusion d'une information collective préalable à la mise en œuvre de tout projet de recherche n'impliquant pas la personne humaine.

501. Seulement, la communication d'une information collective préalablement au traitement des données de recherche ne garantit pas qu'elle parvienne effectivement au patient concerné. Comment le patient concerné par la réutilisation de ses données médicales pourrait appréhender leur traitement ultérieur pour une finalité différente de celle ayant légitimé leur collecte initiale *a fortiori* lorsque, requalifiées en données de recherche, elles sont fournies à un tiers exploitant ?

¹⁷¹⁴ CNIL, Délibération n° 2018-155 du 3 mai 2018, *loc. cit.* ; Cf. Paragraphe 498.

¹⁷¹⁵ *Ibid.*

¹⁷¹⁶ Article 14.5 b) du RGPD.

En raison de la réfaction du droit à l'information au profit des promoteurs de recherche, l'appréciation de la réutilisation des données médicales à des fins de recherche contraint le patient à effectuer une veille d'*informations collectives* auprès de chaque structure de santé au sein de laquelle il a été pris en charge médicalement. Réciproquement, cette inspection hasardeuse n'exigerait-elle pas des efforts disproportionnés pour la personne concernée ? De surcroît, si le patient concerné réussit à accéder à une notice d'information collective présentant les caractéristiques du projet de recherche, comment savoir si les données médicales qui le concernent ont été sélectionnées à cet effet ? Pour obtenir la réponse à cette question, la personne – possiblement – concernée est tenue d'exercer son droit d'accès afin « *d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données* »¹⁷¹⁷. Tandis que l'allègement d'une information communiquée collectivement simplifie les démarches préalables à la recherche au bénéfice de son promoteur, les manœuvres requises pour atteindre cette notice d'information collective alourdissent l'exercice des droits des personnes concernées. Pourtant, n'appartient-il pas au responsable de traitement de le faciliter¹⁷¹⁸ ? Réellement, le troncage du premier des droits du patient concerné par la réutilisation de ses données médicales personnelles tend à compromettre l'effectivité de l'ensemble des autres droits qu'il détient à l'égard des éléments immatériels de son corps humain. A l'évidence, si le patient concerné n'est pas informé de l'exploitation de ses données de recherche, il n'exercera jamais aucun droit sur celles-ci.

Paragraphe 2 : L'atténuation des droits du patient sur ses données de recherche

502. Que les données de recherche du patient soient réunies dans une base de données massives pour la recherche (**A**) ou utilisées pour une étude déterminée (**B**), les droits que le patient détient effectivement sur celles-ci se trouvent fortement nuancés. A l'exception du droit d'y accéder, l'exercice des droits de modification, de suppression et de limitation pourraient entraver la réalisation des recherches n'impliquant pas la personne humaine. Afin de préserver la qualité ainsi que l'intégrité des données de recherche et de favoriser la production des résultats de leur analyse, le législateur européen concède des dérogations aux

¹⁷¹⁷ Article 15.1 du RGPD.

¹⁷¹⁸ Article 12.2 du RGPD.

droits généralement réservés aux personnes concernées¹⁷¹⁹. Tandis que le producteur d'une base de données de recherche¹⁷²⁰ ne jouit d'aucun droit sur la chose anthropomorphique d'autrui¹⁷²¹, les principaux intéressés voient leurs prérogatives affaiblies lorsque leur exploitation profite à l'intérêt public dans le domaine de la santé.

A) Les droits du patient sur ses données médicales intégrées dans une base de données massives pour la recherche

503. Après que le patient ait eu connaissance de l'intégration de ses données médicales dans une base de données massives vouée à la recherche, il peut demander à exercer les droits qu'il détient effectivement sur celles-ci. A cet effet, le patient concerné doit s'adresser à l'entité dont les coordonnées ont été communiquées *via* la notice d'information. Hormis la maîtrise de l'usage des éléments immatériels de son corps humain¹⁷²², le patient peut accéder à ses données de recherche ainsi requalifiées et en demander la rectification, l'effacement et la limitation.

504. D'abord, l'exercice du droit d'accès permet de connaître l'étendue des éléments immatériels du corps humain mis à la disposition de toute recherche alors qu'ils ont été produits à l'occasion de la prise en charge sanitaire du patient. En conséquence, le droit d'accès permet au patient d'obtenir la confirmation de la requalification de ses données médicales en données de recherche. Dans les situations où le droit d'opposition demeure applicable¹⁷²³, l'exercice du droit d'accès contribue également à déterminer le champ d'opposition à cette requalification. En effet, le patient peut refuser que certains des éléments immatériels de son corps humain soient réutilisés à des fins de recherche tout en acceptant que d'autres puissent être mis à la disposition de tout projet concourant à un intérêt public dans le domaine de la santé.

¹⁷¹⁹ Article 89.2 du RGPD ; Considérant 156 du RGPD.

¹⁷²⁰ Qu'il s'agisse des bases du système national des données de santé, des entrepôts de données de santé ou des jeux de données de recherche constitués pour un projet de recherche ponctuel et déterminé.

¹⁷²¹ Cf. Paragraphe 439.

¹⁷²² Cf. Section 2 du Chapitre 1 du Titre 2 de la Partie 2 de la présente thèse.

¹⁷²³ Cf. Paragraphe 1 de la Section 2 du Chapitre 1 du Titre 2 de la Partie 2 de la présente thèse.

En outre, lorsque les données médicales du patient sont incluses dans le SNDS, l'exercice du droit d'accès peut lui permettre de connaître les éventuels appariements, dans le catalogue centralisé, de ses données médicales extraites de la base principale¹⁷²⁴. Ce catalogue, hébergé par le Health Data Hub, comprend des bases de données contenant les informations intégrées dans la base principale et appariées en raison d'un intérêt scientifique correspondant à une thématique déterminée. A titre d'exemple, le catalogue du SNDS comporte une base relative aux « *données du Système National des Données de Santé pour les patients avec un diagnostic hospitalier de Covid-19* »¹⁷²⁵. La corrélation des différentes informations médicales et médico-administratives du patient tend ainsi à inférer de nouvelles données relatives à sa santé. Alors, le droit d'accès de la personne concernée à l'intégralité de ses données de recherche, y compris celles « *consolidées et appariées qui lui sont rattachées dans le catalogue* » du SNDS¹⁷²⁶, participe directement au droit à l'information médicale¹⁷²⁷.

505. Ensuite, le patient concerné par l'intégration de ses données médicales dans une base de données massives pour la recherche bénéficie du droit de les faire rectifier¹⁷²⁸. En premier lieu, le droit de rectification implique la correction des informations inexacts. Cette situation pourrait, à titre d'exemple, résulter d'une erreur dans l'alimentation de la base de données de recherche à la suite de la retranscription des données médicales du patient. En d'autres termes, l'inexactitude des données de recherche doit être appréciée en comparaison avec les données médicales telles qu'issues des dossiers médicaux du patient concerné suite à leur production lors de la dispensation des actes de prévention, de diagnostic ou de soins. Certainement, la correction des données de recherche du patient ne doit pas conduire à la modification de ses données médicales¹⁷²⁹. En second lieu, le droit de rectification emporte « *le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y*

¹⁷²⁴ Article R1461-2 I du code de la santé publique : « *Le système national des données de santé comprend une base principale couvrant l'ensemble de la population et un ensemble de bases de données ne couvrant pas l'ensemble de la population dénommé " catalogue " ».*

¹⁷²⁵ La présentation du catalogue est disponible en ligne sur le site [www.health-data-hub.fr]. Consulté le 29 septembre 2021.

¹⁷²⁶ CNIL, Délibération n°2020-106 du 29 octobre 2020, *loc. cit.*

¹⁷²⁷ Cf. Paragraphe 189.

¹⁷²⁸ Dans les conditions définies à l'article 16 du RGPD.

¹⁷²⁹ Cf. Paragraphes 398 et 512.

compris en fournissant une déclaration complémentaire »¹⁷³⁰. Si le patient découvrait qu'il manquait, au sein de la base de données massives pour la recherche, des éléments immatériels de son corps humain connexes à ceux qui y sont intégrés, pourrait-il les compléter en fournissant une copie de ses dossiers médicaux ?

En tant que bénéficiaire du secret médical, le patient est libre de communiquer sa chose anthropomorphique au destinataire de son choix¹⁷³¹. Toutefois, si le patient venait à compléter un entrepôt de données de santé, ou le SNDS, par la fourniture de ses données médicales, le responsable de la base devrait veiller à la confidentialité de ces informations hautement sensibles. Dans l'hypothèse où cette situation venait à se produire, ce complément de données devrait donc être pseudonymisé conformément à la procédure appliquée aux autres éléments de la base¹⁷³². Si cette possibilité apparaît stupéfiante, elle pourrait plausiblement devenir un devoir pour toute personne dont il émane des données médicales¹⁷³³. En effet, la vocation de toute chose anthropomorphique consisterait à devenir une donnée de recherche afin d'être implémentée dans le domaine commun informationnel¹⁷³⁴.

506. Après, le patient concerné par l'intégration de ses données médicales dans une base dédiée à la recherche a le droit de réclamer leur effacement. L'exercice de ce droit suppose que les critères définis à l'article 17 du RGPD soient réunis. Premièrement, le patient concerné a le droit d'obtenir la suppression de ses données de recherche lorsqu'elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées¹⁷³⁵. Ce motif d'effacement renvoie au principe de limitation de la durée de conservation des données. En principe, dès l'instant où la finalité du traitement est accomplie, les données personnelles doivent être effacées ou anonymisées. Par exception, l'intérêt scientifique peut toutefois justifier que certaines données soient conservées pour des durées plus longues pour autant que soient mises en œuvre les mesures appropriées requises à l'article 89 du RGPD afin de

¹⁷³⁰ Article 16 du RGPD.

¹⁷³¹ Cf. paragraphes 300 et 558.

¹⁷³² Cf. Paragraphe 499.

¹⁷³³ Cf. Paragraphe 533.

¹⁷³⁴ Cf. Paragraphe 466.

¹⁷³⁵ Article 17.1 a) du RGPD.

garantir les droits et les libertés de la personne concernée¹⁷³⁶. Les données médicales pseudonymisées incluses dans le SNDS peuvent donc être « *conservées pour une durée maximale de vingt ans* »¹⁷³⁷ à compter de leur intégration, tandis que celles insérées dans un entrepôt de données de santé « *peuvent être conservées 20 ans maximum à compter de leur collecte dans le cadre des soins ou des recherches* »¹⁷³⁸. Bien que la période de conservation des données médicales puisse être allongée lorsqu'elles sont intégrées dans une base de mégadonnées pour la recherche, ces délais demeurent sensiblement équivalents à la durée réglementaire de conservation des dossiers médicaux¹⁷³⁹. Au terme des délais susvisés, le patient concerné devrait alors pouvoir en demander l'effacement.

Pourtant, si l'effacement des données médicales incluses dans une base de données massives pour la recherche peut être demandé à l'issue de la durée de leur traitement¹⁷⁴⁰, les données intégrées dans le SNDS sont, à l'expiration de leur délai de conservation, versées indéfiniment dans le service public des archives¹⁷⁴¹ pourvu qu'elles présentent une utilité d'intérêt scientifique¹⁷⁴². De la même façon, les données médicales du patient produites par les établissements publics de santé et les établissements privés habilités à assurer le service public hospitalier peuvent, à l'expiration du délai de conservation des dossiers médicaux¹⁷⁴³, devenir des archives publiques en raison de leur intérêt scientifique¹⁷⁴⁴. Les archives publiques étant imprescriptibles¹⁷⁴⁵, les patients concernés par un traitement de leurs données médicales à des fins archivistiques dans l'intérêt public de la science ne peuvent en demander la suppression. L'opposabilité du droit à l'oubli du patient concerné doit donc profiter à la collectivité. En ce sens, les dispositions du RGPD annoncent que le droit à l'effacement ne

¹⁷³⁶ Article 5.1 e) du RGPD.

¹⁷³⁷ Article L.1461-1 IV 4° du code de la santé publique.

¹⁷³⁸ CNIL, Délibération n° 2021-118 du 7 octobre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé, *JORF* n°249, 24 octobre 2021, texte n° 44.

¹⁷³⁹ Cf. Paragraphe 151.

¹⁷⁴⁰ Mais cet effacement n'est qu'illusoire dans la mesure où les données médicales du patient sont d'une part intégrées dans le SNDS et, d'autre part, versées dans le service public des archives, voire dans le domaine commun informationnel.

¹⁷⁴¹ Article R.1461-4 II du code de la santé publique.

¹⁷⁴² Articles L.212-3 et L.212-4 du code du patrimoine.

¹⁷⁴³ Article R.1112-7 du code de la santé publique.

¹⁷⁴⁴ Cf. Paragraphe 156.

¹⁷⁴⁵ Article L.212-1 du code du patrimoine.

s'applique pas dans la mesure où le traitement des données est nécessaire à des fins archivistiques dans l'intérêt public ou à des fins de recherche scientifique et que son exercice est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement¹⁷⁴⁶.

Après leur requalification en archives publiques, les données incluses dans le SNDS et les données médicales issues des dossiers médicaux constitués par les structures participant au service public hospitalier pourraient ainsi tomber dans le domaine commun informationnel. Leur mise à disposition pour toute recherche rétrospective poursuivant un motif d'intérêt public dans le domaine de la santé pourrait être autorisée à condition qu'elles aient été anonymisées ou, à tout le moins, pseudonymisées. Par conséquent, il ne serait plus nécessaire d'attendre l'expiration d'un délai de vingt-cinq ans après la date de décès du patient concerné ni, dans le cas où cette date est inconnue, le terme d'un délai de cent-vingt ans à compter de sa date de naissance¹⁷⁴⁷ pour pouvoir exploiter ces archives publiques. L'absence d'identification des données médicales archivées définitivement serait un moyen permettant de préserver le caractère secret des informations relatives à la santé et, ainsi, d'autoriser leur réutilisation. Certainement, la confidentialité de ces données intimes doit perdurer après la mort de l'intéressé¹⁷⁴⁸, quel que soit le délai entre la date du décès et la révélation du secret.

Deuxièmement, l'effacement des données de recherche peut être demandé lorsque le patient concerné s'est opposé à ce qu'elles alimentent une base de données massives pour la recherche¹⁷⁴⁹, ou lorsqu'il a retiré son consentement sur lequel reposait le fondement juridique de ce traitement¹⁷⁵⁰. Seulement, l'opposition à la requalification des données médicales en données de recherche ainsi que l'opposition à leur réutilisation pour un projet d'intérêt public dans le domaine de la santé apparaissent fortement circonscrites¹⁷⁵¹. Par

¹⁷⁴⁶ Article 17.3 d) du RGPD.

¹⁷⁴⁷ Article L.213-3 I 2° du code du patrimoine.

¹⁷⁴⁸ CA, Paris, 27 mai 1997, *aff. du Docteur Gubler*, JurisData n° 1997-990005 : JCP G, 1997, jur. II, 22894, note E. Derieux ; LPA, 1997, n° 82, p. 26, note E. Derieux et F. Gras

¹⁷⁴⁹ Article 17.1 b) du RGPD.

¹⁷⁵⁰ Article 17.1 c) du RGPD.

¹⁷⁵¹ Cf. Paragraphe 1 de la Section 2 du Chapitre 1 du Titre 2 de la Partie 2 de la présente thèse.

surcroît, le consentement du patient concerné ne fonde que très rarement la licéité¹⁷⁵² ou l'autorisation¹⁷⁵³ du traitement des données médicales à des fins de recherche. En effet, le consentement constitue résiduellement le régime juridique de la construction des entrepôts de données de santé lorsqu'ils ne présentent pas un caractère d'intérêt public dans le domaine de la santé. Certainement, lorsqu'ils ne reposent pas sur le consentement des personnes concernées, les traitements des données de santé, en dehors de ceux nécessaires à la prise en charge sanitaire du patient¹⁷⁵⁴, « ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent »¹⁷⁵⁵. Il en ressort que l'effectivité du droit à l'effacement des données médicales des bases de données massives pour la recherche ne peut intervenir que de façon marginale. Assurément, le RGPD affirme que « la conservation ultérieure des données à caractère personnel devrait être licite lorsqu'elle est nécessaire [...] pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, [ou] à des fins de recherche »¹⁷⁵⁶.

507. Finalement, le patient concerné peut demander la limitation du traitement de ses données de recherche pendant la durée permettant au responsable du traitement de vérifier l'exactitude des informations dont il a demandé la rectification¹⁷⁵⁷ ou, lorsqu'il s'est opposé au traitement, pendant la vérification de la prédominance des motifs légitimes poursuivis par le responsable du traitement par rapport aux siens¹⁷⁵⁸.

Cependant, le gel temporaire de l'utilisation des données personnelles de la personne concernée n'empêche pas leur traitement « pour des motifs importants d'intérêt public de l'Union ou d'un État membre »¹⁷⁵⁹. A cet égard, l'intégration des données médicales dans une base de données consacrée à la recherche peut revêtir un motif important pour l'intérêt public, et la particularité des données médicales relatives aux patients ayant contracté le virus de la

¹⁷⁵² Article 6.1 a) du RGPD.

¹⁷⁵³ Article 9.2 a) du RGPD.

¹⁷⁵⁴ Cf. les cinq exceptions de l'article 65 de la loi Informatique et Libertés modifiée.

¹⁷⁵⁵ Article 66 I de la loi Informatique et Libertés modifiée.

¹⁷⁵⁶ Considérant 65 du RGPD.

¹⁷⁵⁷ Article 18.1 a) du RGPD.

¹⁷⁵⁸ Article 18.1 d) du RGPD.

¹⁷⁵⁹ Article 18.2 du RGPD.

Covid-19 en est la parfaite illustration. Afin de faciliter leur utilisation pour l'amélioration des connaissances sur ce nouveau virus, une base de données concernant la santé des patients qui en ont été atteints a été constituée et intégrée dans la base principale du SNDS¹⁷⁶⁰. Assurément, « *la capacité à mobiliser les données de santé est un enjeu essentiel dans la lutte contre l'épidémie de COVID-19* »¹⁷⁶¹ et cette catégorie de données médicales doit demeurer à disposition de toute recherche, évaluation ou étude pour des motifs importants d'intérêt public dans le domaine de la santé. Dans une telle hypothèse, le droit à la limitation du traitement des données médicales s'avérerait inefficace. Une fois encore, l'un des droits dont le patient concerné peut théoriquement se prévaloir peut, en pratique, se trouver inexistant.

508. Alors que les droits du patient concerné par le regroupement de ses données de recherche dans une base de mégadonnées se révèlent manifestement limités, comment les exercer lorsque les données qu'elle contient sont obligatoirement pseudonymisées ?

La notice d'information délivrée à la personne concernée doit détailler les modalités d'exercice de ses droits et indiquer les coordonnées du délégué à la protection des données à qui s'adresser. Les données médicales et de recherche étant couvertes par le secret professionnel médical, le délégué à la protection des données doit, après réception de la demande d'exercice des droits du patient concerné, la relayer au professionnel habilité à y répondre. Il doit néanmoins s'assurer de sa bonne instruction dans le respect des délais réglementaires impartis¹⁷⁶². Il en advient que le professionnel qui accède à la requête du patient concerné doit être dépositaire du secret professionnel médical et détenir la clé de correspondance entre l'identité du patient et son pseudonyme.

Ce processus ne pose apparemment aucune difficulté lorsque les données médicales sont intégrées dans un entrepôt de données de santé pour la recherche. Deux hypothèses sont alors envisageables. En premier lieu, le responsable du traitement aux fins de constitution

¹⁷⁶⁰ Article 5 du décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », *JORF* n°0150, 30 juin 2021, texte n° 63.

¹⁷⁶¹ Direction générale de la santé, lettre adressée le 26 mai 2020 à la direction de la Plateforme nationale des données de santé, référencée D.20-009467. Disponible en ligne sur le site [www.health-data-hub.fr]. Consulté le 30 septembre 2021.

¹⁷⁶² Article 12.3 et 12.4 du RGPD.

d'un entrepôt de données de santé peut être l'établissement ou le professionnel de santé producteur et gardien des données médicales du patient. Le cas échéant, le responsable de traitement fournira directement, au patient concerné, les informations sur les mesures prises à la suite de la demande formulée. En second lieu, le responsable de l'entrepôt de données de santé peut devoir collecter des données médicales auprès de l'établissement ou du professionnel de santé les ayant produites au cours de la prise en charge sanitaire du patient. Dans ces conditions, un contrat de sous-traitance organisant le traitement et attribuant les droits et les obligations des parties doit être conclu¹⁷⁶³. Cet acte juridique doit notamment prévoir que la pseudonymisation des données médicales doit être effectuée au niveau du détenteur des données médicales nominatives. Les identifiants pseudonymisés sont ensuite transmis au responsable de l'entrepôt de données de santé avec les données médicales alors requalifiées en données de recherche. Par conséquent, le professionnel détenteur des données médicales nominatives, intervenant en qualité de sous-traitant, doit être contractuellement chargé de l'exercice des droits reconnus au patient concerné. De cette façon, la confidentialité des données médicales à caractère secret se trouve préservée.

509. En revanche, l'exercice des droits reconnus au patient concerné apparaît davantage alambiqué lorsque ses données médicales sont incluses dans le SNDS. Au préalable, il semble essentiel de rappeler « *qu'un des principes fondamentaux de la sécurité du SNDS repose sur la pseudonymisation de ses données et un strict cloisonnement entre les données identifiantes et les données pseudonymisées, excluant par principe qu'une même entité ait accès simultanément aux NIR et aux données du SNDS* »¹⁷⁶⁴. Dès lors, seule une entité soumise au secret professionnel médical devrait pouvoir reconstituer la correspondance entre l'identité du patient concerné et ses données médicales. Avant que le décret du 29 juin 2021 relatif au SNDS n'entre en vigueur¹⁷⁶⁵, le patient concerné par l'inclusion de ses données médicales au sein de ce système devait exercer les droits qui lui étaient effectivement reconnus « *auprès du directeur de l'organisme gestionnaire du régime d'assurance maladie obligatoire auquel* »¹⁷⁶⁶ il était rattaché. Seulement, depuis le 1^{er} juillet 2021, la personne concernée doit

¹⁷⁶³ Article 28.3 du RGPD.

¹⁷⁶⁴ CNIL, Délibération n° 2020-106 du 29 octobre 2020, *loc. cit.*

¹⁷⁶⁵ Décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », *JORF* n°0150, 30 juin 2021, texte n° 63.

¹⁷⁶⁶ Article 1 du décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », *JORF* n°0301, 28 décembre 2016.

désormais adresser sa demande, « *en justifiant de son identité par tout moyen, au directeur de la Plateforme ou au directeur de l'organisme gestionnaire d'assurance maladie obligatoire dont elle relève* »¹⁷⁶⁷. Il s'ensuit que « *dans la stricte limite de ce qui est nécessaire pour l'exercice des droits [...] la Plateforme des données de santé ou son sous-traitant est autorisée à traiter les données à caractère personnel adéquates et pertinentes, parmi lesquelles le numéro d'inscription des personnes au Répertoire national d'identification des personnes physiques* »¹⁷⁶⁸. Il s'ensuit que le Health Data Hub est réglementairement habilité à lever la pseudonymisation des données médicales intégrées dans le SNDS afin d'identifier les informations relatives au demandeur et d'instruire sa requête. En conséquence, le Health Data Hub peut, à la fois, disposer de l'identité du patient concerné, de son pseudonyme et de ses données médicales.

Tandis que l'instruction des demandes d'exercice des droits par ce groupement d'intérêt public contribue à accélérer le traitement des requêtes formulées par les personnes concernées, cette solution bouleverse le principe de la stricte confidentialité visant à empêcher l'identification directe de la personne associée à son pseudonyme. Ainsi que le suggère la CNIL, « *la gestion des demandes d'exercice des droits devrait intervenir au niveau des organismes gestionnaires du régime d'assurance maladie obligatoire* »¹⁷⁶⁹ comme tel était le cas auparavant. Concrètement, « *ces organismes sont dépositaires du secret permettant d'effectuer le premier niveau de pseudonymisation du NIR, et sont susceptibles de constituer un « guichet unique » efficace pour toutes les demandes d'exercice des droits d'une personne* »¹⁷⁷⁰. La CNAM et le Health Data Hub, en tant que responsables conjoints du SNDS, « *ne recevraient alors qu'un pseudonyme dérivé du NIR [transmis par la caisse primaire d'assurance maladie du patient concerné] leur permettant de sélectionner les données correspondant au demandeur et d'effectuer les opérations nécessaires au bon exercice de ses droits* »¹⁷⁷¹. De surcroît, cette procédure faciliterait les modalités d'exercice des droits de la personne concernée. Assurément, « *ce schéma permettrait à la personne concernée, grâce à une seule demande, d'exercer ses droits pour l'ensemble des bases du «*

¹⁷⁶⁷ Article R.1461-9 IV du code de la santé publique.

¹⁷⁶⁸ Article R.1461-9 IV du code de la santé publique.

¹⁷⁶⁹ CNIL, Délibération n° 2020-106 du 29 octobre 2020, *loc. cit.*

¹⁷⁷⁰ CNIL, Délibération n° 2020-106 du 29 octobre 2020, *loc. cit.*

¹⁷⁷¹ *Ibid.*

SNDS centralisé », permettant ainsi de se conformer à la fois aux principes de sécurité du SNDS et aux dispositions du RGPD »¹⁷⁷². Cependant, cette recommandation préconisée par la CNIL suite à la saisine du ministre des solidarités et de la santé concernant le projet de décret relatif au SNDS n'a pas été retenue par le pouvoir exécutif. Compte tenu des risques inhérents à la réidentification des données du SNDS à l'occasion de l'exercice des droits de la personne concernée, la sécurité juridique de ce traitement ne semble pas suffisamment garantie. Alors qu'une « protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées »¹⁷⁷³, les modalités de leur exercice peuvent paradoxalement mettre en péril la protection des données personnelles.

B) Les droits du patient sur ses données de recherche utilisées pour un projet déterminé

510. Le porteur d'un projet de recherche rétrospective peut recueillir les données médicales nécessaires à ce traitement auprès de trois catégories d'entités différentes. En premier lieu, le promoteur de la recherche peut collecter les éléments nécessaires à la recherche auprès d'un établissement ou d'un professionnel de santé assurant la conservation des dossiers médicaux des patients qu'ils ont pris en charge. En deuxième lieu, il peut recourir à un entrepôt de données de santé constitué par le producteur d'une telle base de données. En troisième lieu, il peut solliciter l'accès aux données incluses au sein du Système national des données de santé. Ces détenteurs de données de recherche, intervenant en qualité de sous-traitant du promoteur de la recherche, sont tenus de constituer un jeu de données pseudonymisées et pertinemment utiles à la réalisation de la finalité de l'étude. Après avoir été formalisé au sein d'un jeu de données spécifique à une recherche déterminée, il appartient aux sous-traitants de le transmettre au responsable du projet. Les données de la recherche sont alors analysées par les « chercheurs » conformément au protocole scientifique validé avant la mise en œuvre de leur traitement. Dans ces conditions, quels sont les droits attribués au patient lorsque ses données de recherche sont utilisées pour une étude déterminée ? Vraisemblablement, les droits reconnus au patient concerné par l'utilisation de ses données de recherche pour un

¹⁷⁷² *Ibid.*

¹⁷⁷³ Considérant 11 du RGPD.

projet spécifique apparaissent notablement identiques aux droits qui lui sont reconnus lorsque ses données médicales sont intégrées dans une base de mégadonnées pour la recherche.

511. Dans le respect de l'article 15 du RGPD, le patient concerné peut évidemment accéder à ses données de recherche échantillonnées pour l'étude dont il est question. Bien que les catégories de données de recherche traitées soient détaillées au sein de la notice d'information¹⁷⁷⁴, cet accès permet de préciser avec exactitude quels éléments immatériels de son corps humain ont été retenus pour la recherche. Ainsi, le droit d'accès participe fondamentalement au principe de transparence. C'est pourquoi le responsable de la recherche doit veiller à ne collecter que les données médicales décrites dans l'information communiquée aux patients sélectionnés. A défaut, l'absence de conformité entre les catégories de données dont le traitement a été annoncé et celles effectivement traitées pourrait susciter de la méfiance à l'égard du responsable de la recherche et, plus globalement, à l'encontre du système de santé. Par conséquent, le sous-traitant chargé de fournir les données de recherche au promoteur doit rigoureusement veiller à honorer la nature et la liste des données à caractère personnel décrites dans le protocole de recherche, après avoir vérifié les justifications scientifiques du recours à celles-ci¹⁷⁷⁵. Aussi, le gardien des données médicales du patient doit scrupuleusement s'assurer de la cohérence entre les données détaillées au sein du protocole de recherche et celles inscrites dans la notice d'information.

512. Suite à l'exercice du droit d'accès à ses données de recherche, le patient peut théoriquement en réclamer la rectification. Le patient qui constaterait l'inexactitude de ses données de recherche, en comparaison avec ses données médicales, devrait s'adresser au sous-traitant ayant transmis ses choses anthropomorphiques au promoteur de la recherche¹⁷⁷⁶. Certainement, l'entité qui détient les données médicales du patient est soumise à une double obligation d'exactitude¹⁷⁷⁷ et d'intégrité¹⁷⁷⁸ des données personnelles traitées. Il lui incombe alors de communiquer un jeu de données de recherche composé d'éléments intègres, qualitatifs et dépourvus de biais. La qualité de la recherche rétrospective dépend assurément

¹⁷⁷⁴ Article 14.1 d) du RGPD.

¹⁷⁷⁵ CNIL, Délibération n° 2018-155 du 3 mai 2018, *loc.cit.*

¹⁷⁷⁶ Cf. Paragraphe 510.

¹⁷⁷⁷ Article 5.1 d) du RGPD.

¹⁷⁷⁸ Article 5.1 f) du RGPD.

de la qualité des données traitées. C'est pourquoi les personnes responsables du contrôle de la qualité de la recherche sont chargées de se rendre chez le sous-traitant ayant fourni le jeu de données de recherche¹⁷⁷⁹ afin de « *contrôler et d'évaluer la qualité et l'authenticité des données collectées, et notamment par la comparaison des données enregistrées avec le contenu des documents sources* »¹⁷⁸⁰. Compte tenu des enjeux liés à la véracité des données de recherche, le patient qui, au cours du contrôle des usages de sa chose anthropomorphe, s'apercevrait d'une telle inexactitude devrait en alerter les acteurs du traitement. En agissant ainsi, le patient concourrait activement à la probité de la recherche menée à partir des éléments immatériels de son corps humain.

En revanche, le patient ne devrait pouvoir compléter ses données de recherche. En effet, seules les données pertinemment adéquates et limitées aux objectifs décrits dans le protocole de recherche peuvent être licitement traitées. Le principe de minimisation des données personnelles se trouve donc renforcé lorsque les éléments immatériels du corps humain du patient sont traités pour une finalité de recherche, d'étude ou d'évaluation dans le domaine de la santé. Le patient concerné ne peut donc ingérer dans la sélection des éléments nécessaires à la réalisation de la recherche n'impliquant pas la personne humaine.

513. A l'inverse, lorsque le patient remarque que des données supplémentaires aux catégories déclarées dans la notice d'information sont traitées, il jouit du droit d'en demander l'effacement. En effet, le législateur européen déclare que lorsque les données à caractère personnel ont fait l'objet d'un traitement illicite, le responsable du traitement a l'obligation de les effacer dans les meilleurs délais¹⁷⁸¹. Au préalable, il conviendrait toutefois de s'assurer du respect du principe de minimisation des données de recherche traitées. Si le traitement de ces données supplémentaires n'était pas justifié au sein du protocole de recherche, leur suppression du jeu de données de recherche devrait intervenir immédiatement. *A contrario*, lorsque leur traitement s'avère scientifiquement motivé, mais que leur sélection n'apparaît pas au sein de la notice d'information délivrée au patient concerné, il appartient au

¹⁷⁷⁹ L'établissement, le professionnel de santé, l'organisme ou l'entité détenant et transmettant les données utilisées dans le cadre de la recherche n'impliquant pas la personne humaine.

¹⁷⁸⁰ CNIL, Délibération n° 2018-155 du 3 mai 2018, *loc. cit.*

¹⁷⁸¹ Article 17.1 d) du RGPD.

responsable de la recherche de lui fournir un complément d'information conformément à l'article 15 du RGPD.

En outre, l'effacement des données de recherche peut également être sollicité au terme des délais de conservation définis par le promoteur de la recherche en application du principe de limitation¹⁷⁸². Bien que les données médicales, requalifiées en données de recherche, ont vocation à alimenter le domaine commun informationnel, le promoteur d'une recherche poursuivant un objectif déterminé ne peut indéfiniment les conserver. De surcroît, même lorsque le traitement pour une finalité de recherche scientifique est présumé compatible avec la finalité initiale ayant légitimé la collecte des données personnelles¹⁷⁸³, le promoteur d'une nouvelle recherche n'impliquant pas la personne humaine doit, d'une part, conclure un nouvel acte juridique le liant au fournisseur du jeu de données de recherche¹⁷⁸⁴ et, d'autre part, accomplir les formalités préalables à leur traitement auprès de l'autorité de contrôle compétente.

514. Par ailleurs, le patient concerné par l'utilisation de ses données de recherche pour un projet déterminé peut incertainement exercer son droit à l'effacement à la suite de l'exercice de son éventuel droit d'opposition à leur traitement¹⁷⁸⁵. Dans l'hypothèse où le patient peut effectivement s'opposer à l'utilisation de ses données de recherche¹⁷⁸⁶, leur effacement peut être envisagé lorsqu' « *il n'existe pas de motif légitime impérieux pour le traitement* »¹⁷⁸⁷. Seulement, quand le droit d'opposition est exercé postérieurement au démarrage du traitement, « *le droit à l'effacement des données est susceptible d'entrer en contradiction avec les exigences méthodologiques d'une recherche* »¹⁷⁸⁸. La pertinence et la fiabilité des résultats de la recherche semblent alors représenter des motifs légitimes et impérieux en

¹⁷⁸² Article 5.1 e) du RGPD.

¹⁷⁸³ Cf. Paragraphe 477.

¹⁷⁸⁴ L'acte juridique de sous-traitance des données personnelles prévoit le sort qui leur est réservé au terme de la durée de leur traitement pour une finalité spécifique. Si le responsable de la recherche souhaite les réutiliser pour une finalité ultérieure compatible, il convient alors de conclure un nouveau contrat déterminant la nouvelle finalité poursuivie, les nouveaux délais de conservation de ces données personnelles ainsi que leur devenir.

¹⁷⁸⁵ Cf. Section 2 du Chapitre 1 du Titre 2 de la Partie 2 de la présente thèse.

¹⁷⁸⁶ Cf. Section 2 du Chapitre 1 du Titre 2 de la Partie 2 de la présente thèse.

¹⁷⁸⁷ Article 17.1 c) du RGPD.

¹⁷⁸⁸ LESAULNIER (F.), *op cit.*, p. 108.

faveur de leur sauvegarde, *a fortiori* lorsque la recherche rétrospective poursuit une finalité d'intérêt public dans le domaine de la santé.

Identiquement, si l'éventuel droit d'opposition était exercé avant la mise en œuvre de la recherche, le droit à l'effacement des données du jeu constitué pour la recherche ne pourrait être exercé. Certainement, la suppression des données personnelles ne peut être réclamée quand le traitement est nécessaire « *pour des motifs d'intérêt public dans le domaine de la santé publique* »¹⁷⁸⁹ ou lorsque son exercice peut compromettre la réalisation des objectifs de la recherche scientifique¹⁷⁹⁰. L'un et l'autre de ces deux obstacles au droit à l'effacement des données personnelles s'opposent *de facto* au patient concerné par la réutilisation des éléments immatériels de son corps humain à des fins de recherche. En effet, le traitement de ses données de recherche participe à un motif d'intérêt public dans le domaine de la santé d'une part et leur effacement compromettrait la réalisation des objectifs de la recherche d'autre part^Mani que les intérêts dont la collectivité bénéficierait suite au traitement de la chose anthropomorphe à des fins de recherche dans le domaine de la santé prévalent sur les droits individuels des patients concernés.

515. Pareillement, le droit à limitation du traitement paraît contraire aux motifs importants d'intérêt public poursuivis par le responsable de la recherche¹⁷⁹¹. Le gel de l'utilisation de la chose anthropomorphe d'une personne concernée pourrait mettre en péril la validation des résultats de la recherche n'impliquant pas la personne humaine alors même qu'elle concourt à une finalité d'intérêt public dans le domaine de la santé. En effet, la limitation de l'utilisation des éléments immatériels du corps humain d'un seul individu peut conduire à la suspension de la recherche rétrospective fondée sur l'utilisation d'un ensemble de données de recherche. Finalement, l'exercice du droit à la limitation du traitement des données médicales contreviendrait à la poursuite de l'étude scientifique et, subséquemment, à l'amélioration de la santé publique¹⁷⁹². C'est pourquoi l'exercice de ce droit peut connaître des restrictions inhérentes à la nature ainsi qu'à la finalité du traitement des données de recherche du patient.

¹⁷⁸⁹ Article 17.3 c) du RGPD.

¹⁷⁹⁰ Article 17.3 d) du RGPD.

¹⁷⁹¹ Article 18.2 du RGPD.

¹⁷⁹² Cf. Paragraphe 625.

516. Même si les droits du patient concerné par l'utilisation de ses données de recherche pour un projet spécifique se trouvent fortement limités, il apparaît essentiel qu'il puisse effectivement exécuter les prérogatives qui lui sont réellement reconnues. A cet effet, deux dénouements sont envisageables.

Afin de simplifier l'exercice des droits conférés au patient concerné¹⁷⁹³, celui-ci peut adresser sa demande au promoteur de la recherche rétrospective. Dans ces conditions, il incombe à ce dernier de transmettre la demande formulée par le patient concerné et les documents justifiant de son identité au sous-traitant autorisé à accéder aux données de recherche nominatives. En effet, le sous-traitant est contractuellement tenu d'aider le responsable de traitement « à *s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits* »¹⁷⁹⁴, *a fortiori* lorsque les données présentent un caractère secret. En fin de compte, les suites données à la demande d'exercice des droits du patient concerné lui seront directement apportées par le sous-traitant intermédiaire du responsable de traitement.

Autrement, les modalités d'exercice des droits du patient concerné, définies au sein de la notice d'information, peuvent s'accomplir auprès du sous-traitant habilité à reconstituer la correspondance entre leur identité et les données de recherche pseudonymisées. Seulement, cette option semble fastidieuse pour les patients concernés par l'utilisation de leurs données de recherche. Bien qu'ils soient informés de la source d'où proviennent leurs choses anthropomorphiques¹⁷⁹⁵, il serait particulièrement épineux, pour le patient concerné, de contacter l'organisme les ayant mises à disposition, à plus forte raison lorsqu'elles sont extraites d'une base de mégadonnées pour la recherche.

Quelle que soit l'option préférée, il appartient au promoteur de la recherche de concevoir, en concertation avec le sous-traitant lui ayant communiqué le jeu de données de recherche, une procédure de réponse aux demandes d'exercice des droits des patients concernés qui soit peu contraignante et suffisamment accessible à chaque intéressé. A défaut,

¹⁷⁹³ Article 12.2 du RGPD

¹⁷⁹⁴ Article 28.3 e) du RGPD.

¹⁷⁹⁵ Article 14.2 f) du RGPD.

des modalités d'exercice trop complexes à appliquer peuvent entraîner une renonciation des personnes concernées à l'exécution de leurs droits dont, soulignons-le, l'existence est atténuée au profit de la collectivité. Eu égard à la restriction des droits octroyés au patient concerné par l'utilisation de ses données de recherche, l'exercice des prérogatives qu'il détient effectivement sur sa chose anthropomorphique devrait lui être garanti.

517. Si les modalités d'exercice du droit d'opposition à l'utilisation des données de recherche devraient poursuivre ces mêmes exigences d'aisance, cette maîtrise de leur usage semble remise en cause lorsque le traitement poursuit une finalité d'intérêt public dans le domaine de la santé. L'autodétermination informationnelle du patient vis-à-vis de ses données de recherche serait alors unanimement affaiblie en raison de la finalité poursuivie.

Section 2 : La réduction de l'autodétermination informationnelle du patient au profit de l'indispensable exploitation des données de recherche

« Construire une politique publique suppose de parvenir à démontrer l'existence d'un intérêt général supérieur permettant de revenir sur des principes juridiques de nature inférieure ou égale. »¹⁷⁹⁶.

518. A l'instar de la réduction des droits du patient sur ses données de recherche, le législateur européen concède la diminution du droit d'opposition à la réutilisation des données médicales lorsqu'elle présente une finalité de recherche scientifique. Ainsi, lorsque les données de recherche du patient sont utilisées pour un projet poursuivant un motif d'intérêt public dans le domaine de la santé, le droit d'opposition lui devient réciproquement opposable (**Paragraphe 1**).

519. Compte tenu de l'inefficience du droit d'opposition, le principe de transparence exigerait que l'impossibilité d'empêcher l'utilisation de ses données de recherche pour un projet d'intérêt public dans le domaine de la santé soit honnêtement affirmée. A cet égard, un devoir de concours à la recherche et à l'innovation au bénéfice de la santé publique pourrait être instauré à la charge de la Nation (**Paragraphe 2**). L'encadrement légal de cette

¹⁷⁹⁶ PECHILLON (E.), *L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ?*, L'information psychiatrique, vol. 91, 2015, n°8, p. 648.

contrainte permettrait de consolider les capacités des recherches n'impliquant pas la personne humaine – lesquelles sont indispensables à la protection de la santé publique – tout en assurant la poursuite d'un motif d'intérêt public et en garantissant le respect du droit à la protection des données personnelles. Si le patient avait l'assurance que ses données de recherche étaient exploitées de façon confidentielle dans le respect du secret professionnel médical et pour un objectif de protection de la santé publique, pourquoi souhaiterait-il contrevenir aux progrès médicaux ?

Paragraphe 1 : L'opposabilité du droit d'opposition au patient concerné par l'utilisation de ses données de recherche

520. En pratique, l'ensemble des différentes notices d'information relatives à l'utilisation des données de recherche énoncent l'existence du droit de s'y opposer et précisent les modalités de son exercice (**A**). Pourtant, le droit d'opposition à l'exploitation des données de recherche pour un motif d'intérêt public dans le domaine de la santé est assorti de limitations normatives consacrées tant à l'échelle européenne qu'au niveau national (**B**). Ces différentes restrictions tiennent au fait que le développement de l'innovation dans le domaine de la santé dépend de l'utilisation des données de recherche des citoyens qui composent notre société. Les intérêts pour la santé de la collectivité semblent alors prévaloir sur l'autodétermination informationnelle revenant individuellement aux personnes concernées.

A) Le principe d'un supposé droit d'opposition à l'utilisation des données de recherche

521. Le droit d'opposition à la requalification des données médicales en données de recherche et, subséquemment, à leur utilisation pour un projet présentant un motif d'intérêt public pour la santé est consacré par les responsables de leur traitement. En théorie, toute personne concernée peut, à tout moment, s'opposer à un traitement de ses données personnelles fondé sur l'exécution d'une mission d'intérêt public dont le responsable de traitement est investi ou sur les intérêts légitimes qu'il poursuit¹⁷⁹⁷. A moins qu'elle ne repose extraordinairement sur le consentement du patient concerné, la réutilisation des éléments immatériels de son corps humain à des fins de recherche rétrospective est majoritairement

¹⁷⁹⁷ Article 21.1 du RGPD.

fondée sur l'un ou l'autre de ces deux fondements juridiques. En pratique, le choix entre ces deux bases légales est opéré en considération du statut juridique du responsable de traitement et de son secteur d'activités¹⁷⁹⁸. A titre d'exemple, quand le traitement des données de recherche est mis en œuvre par un établissement public de santé, sa licéité repose sur la mission de recherche et d'innovation en santé dont il est légalement investi¹⁷⁹⁹. En revanche, lorsque ce même traitement est réalisé par un organisme de droit privé, sa base légale ne peut que s'appuyer sur les intérêts qu'il poursuit légitimement à condition qu'aucune atteinte importante ne soit portée aux droits et intérêts des patients concernés. En apparence, « *lorsque les recherches sont, en raison de leur qualification réglementaire, soumises à un régime d'opposition, 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* »¹⁸⁰⁰.

522. Dès l'instant où le fondement juridique du traitement permet de concéder l'existence du droit de s'y opposer, les notices d'information délivrées aux patients concernés par l'utilisation de leurs données de recherche explicitent clairement et distinctement¹⁸⁰¹ son existence ainsi que les modalités de son exercice. Qu'il s'agisse de l'intégration de ses données médicales dans une base volumineuse dédiée à l'innovation ou de leur utilisation pour un projet spécifique, le patient devrait théoriquement pouvoir empêcher ces usages à tout moment. Certainement, la personne concernée à laquelle est reconnu un droit d'opposition peut l'invoquer dès l'instant où il existe « *des raisons tenant à sa situation particulière* »¹⁸⁰². L'exercice du droit d'opposition au traitement de ses données personnelles est subordonné à l'allégation de motifs légitimes tenant de manière prépondérante à des considérations propres au demandeur¹⁸⁰³. Pourtant, la CNIL fait fit de cette condition au sein de sa quatrième méthodologie de référence.

¹⁷⁹⁸ Cf. Paragraphe 279.

¹⁷⁹⁹ Article L.6111-1 du code de la santé publique.

¹⁸⁰⁰ LESAULNIER (F.), *Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données*, op. cit., p. 107.

¹⁸⁰¹ Article 21.4 du RGPD.

¹⁸⁰² Article 21.1 du RGPD.

¹⁸⁰³ CE, 10^{ème} et 9^{ème} ch., 18 mars 2019, n°406313, Rec. Lebon, T. ; D., 2019, n° 30, p. 1673, obs. W. Maxwell et C. Zolynski ; Dalloz IP/IT, 2019, n° 07-08, p. 450, obs. D. Forest ; JCP A, 2019, n° 13, act. 209, C. Friedrich.

L'autorité de contrôle y annonce que « *la personne qui entend s'opposer au traitement des données à caractère personnel la concernant à des fins de recherche dans le domaine de la santé peut exprimer, à tout moment et sans avoir à justifier sa décision, son opposition par tout moyen* »¹⁸⁰⁴. La suppression de cette condition à laquelle est communément assujéti l'exercice du droit d'opposition se révèle discriminatoire pour les patients concernés par l'utilisation de leurs données de recherche. Effectivement, les conditions d'exercice du droit d'opposition varient selon que le traitement se trouve en conformité avec la « MR-004 » ou qu'il a été préalablement autorisé par la CNIL. Dans l'hypothèse où la recherche n'impliquant pas la personne humaine n'entre pas dans le cadre de cette méthodologie de référence, elle doit être mise en œuvre dans le respect des dispositions du RGPD et de la loi Informatique et Libertés modifiée. Or, ces normes européennes et nationales conditionnent l'exercice du droit d'opposition au traitement à la démonstration de raisons légitimes inhérentes à la situation particulière de la personne concernée¹⁸⁰⁵.

A titre exceptionnel, le législateur européen ne conçoit une dérogation à la fourniture « *de motifs légitimes de nature à justifier cette opposition* »¹⁸⁰⁶ que pour les traitements à des fins de prospection¹⁸⁰⁷. Aucune autre entorse à cette condition n'est accordée par le droit à la protection des données personnelles, pas même au sein des « *dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé* »¹⁸⁰⁸. Au contraire, les dispositions du RGPD énoncent que « *lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique [...] la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant* »¹⁸⁰⁹. Etant donné que par *recherche scientifique* le législateur européen entend aussi bien « *le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé* »¹⁸¹⁰ que « *les études menées dans l'intérêt public*

¹⁸⁰⁴ CNIL, Délibération n° 2018-155 du 3 mai 2018, *loc. cit.*

¹⁸⁰⁵ Article 56 de la loi Informatique et Libertés modifiée ; Article 21.1 du RGPD.

¹⁸⁰⁶ CE, 10^{ème} et 9^{ème} ch., 18 mars 2019, n°406313, Rec. Lebon, T. ; D., 2019, n° 30, p. 1673, obs. W. Maxwell et C. Zolynski ; Dalloz IP/IT, 2019, n° 07-08, p. 450, obs. D. Forest ; JCP A, 2019, n° 13, act. 209, C. Friedrich.

¹⁸⁰⁷ Article 21.2 du RGPD.

¹⁸⁰⁸ Sous-section 2 de la Section 3 du Chapitre III du Titre II de la loi Informatique et Libertés modifiée.

¹⁸⁰⁹ Article 21.6 du RGPD.

¹⁸¹⁰ Considérant 159 du RGPD.

dans le domaine de la santé publique »¹⁸¹¹, la subordination de l'exercice du droit d'opposition à l'existence de raisons particulières au demandeur s'applique à toute recherche n'impliquant pas la personne humaine. Par suite, la « MR-004 » homologuée par la CNIL s'avère contraire aux dispositions normatives relatives à la protection des données personnelles.

523. Par conséquent, il est impossible de garantir au patient un droit d'opposition inconditionnel au traitement de ses données de recherche à des fins d'intérêt public dans le domaine de la santé. En effet, le promoteur de la recherche peut contester la légitimité des raisons personnelles alléguées par le patient concerné. De surcroît, il peut passer outre une demande d'opposition au traitement lorsqu'il démontre qu'il existe des motifs légitimes et impérieux qui prévalent sur les intérêts, les droits et les libertés des intéressés¹⁸¹², ou que le projet de recherche est nécessaire à l'exécution d'une mission d'intérêt public¹⁸¹³. Tandis que le fondement juridique du traitement permet d'ouvrir le droit d'opposition, la finalité poursuivie par le responsable de traitement permet de l'anéantir. Manifestement, le droit d'opposition au traitement n'est pas un droit absolu ; il comprend en effet de nombreuses limitations, y compris lorsqu'il est question de l'exploitation d'une chose anthropomorphique.

¹⁸¹¹ *Ibid.*

¹⁸¹² Article 21.1 du RGPD.

¹⁸¹³ Article 21.6 du RGPD.

B) Les limites normatives à l'exercice du droit d'opposition à l'utilisation des données de recherche

524. La finalité du traitement des données de recherche, correspondant aux motifs légitimes de sa mise en œuvre, peuvent contrevenir à l'exercice du droit d'opposition de la personne concernée. En effet, le législateur européen affirme à plusieurs égards qu'une dérogation au droit d'opposition visé à l'article 21 du RGPD peut être édictée par le droit de l'Union ou le droit d'un Etat membre lorsque les données à caractère personnel sont traitées à des fins de recherche scientifique¹⁸¹⁴.

525. C'est ainsi que le législateur national a limité le droit d'opposition au traitement des données médicales du patient dans le cadre du SNDS. D'une part, le patient ne peut empêcher l'intégration de ses données médicales dans la base principale de ce système et, conséquemment, leur requalification en données de recherche¹⁸¹⁵. D'autre part, il ne peut s'opposer à la mise à disposition permanente de ses données de recherche pour les traitements mis en œuvre par les services de l'Etat, les établissements publics et les organismes chargés d'une mission de service public¹⁸¹⁶ pour les besoins de l'accomplissement de leurs missions¹⁸¹⁷. Sans compter que le droit d'opposition ne s'applique pas lorsque le traitement à des fins de recherche scientifique est nécessaire à l'exécution d'une mission d'intérêt public¹⁸¹⁸, les dispositions du RGPD particulières aux recherches scientifiques précisent également que l'inapplicabilité du droit d'opposition peut être envisagée dans la mesure où son exercice risquerait de rendre impossible ou d'entraver la réalisation des finalités de la recherche¹⁸¹⁹. En d'autres termes, la dérogation au droit d'opposition au traitement des données de recherche doit être essentiel pour atteindre les finalités d'intérêt public dans le domaine de la santé poursuivies par le promoteur de la recherche¹⁸²⁰. Seulement, que l'étude rétrospective soit instituée par de grandes institutions publiques dans le cadre de l'exercice

¹⁸¹⁴ Voir en ce sens : article 89.2 du RGPD ; considérant 156 du RGPD.

¹⁸¹⁵ Article R.1461-9 II 1° du code de la santé publique.

¹⁸¹⁶ Dont la liste figure à l'article R.1461-12 du code de la santé publique

¹⁸¹⁷ Article R.1461-9 II 2° du code de la santé publique.

¹⁸¹⁸ Article 21.6 du RGPD.

¹⁸¹⁹ Article 89.2 du RGPD.

¹⁸²⁰ Article 89.2 du RGPD.

de leur mission ou par un petit auto-entrepreneur dans le secteur de la santé numérique, la fiabilité ainsi que la qualité de ses résultats requièrent indispensablement le traitement d'un large échantillon de données de recherche¹⁸²¹. Il est donc primordial que le responsable d'une étude fondée sur l'utilisation des données de recherche du patient dispose de l'intégralité des éléments immatériels du corps humain nécessaires à sa démonstration scientifique.

Si un droit d'opposition était admis au bénéfice de tous, chacun pourrait alors empêcher l'utilisation de ses données de recherche ; le cas échéant, la validité de l'étude serait entravée par l'altération de la représentativité de l'échantillon qui l'exposerait à des biais. En effet, le promoteur de la recherche rétrospective doit disposer d'un panel de données médicales comprenant des variables et divers facteurs confondants. A titre d'illustration, l'opposition à la réutilisation de données médicales « *de patients ayant été sujets à un événement indésirable induirait un biais majeur en faveur d'une amélioration du rapport bénéfice/risque* »¹⁸²² de l'étude rétrospective. Par conséquent, la dérogation au droit d'opposition du patient concerné se révèle nécessaire à la bonne administration de la finalité poursuivie.

526. Si le législateur européen a souhaité faciliter et favoriser la recherche scientifique en tolérant certaines dérogations aux droits des personnes concernées, pourquoi ne pas les étendre à l'ensemble des études dans le domaine de la santé ? Quels que soient l'envergure et l'objectif de la recherche n'impliquant pas la personne humaine, l'utilisation des données de recherche du patient doit toujours contribuer à l'intérêt public¹⁸²³. En conséquence, les recherches, les études et les évaluations dans le domaine de la santé ne peuvent être mises en œuvre qu'en considération de l'intérêt public qu'elles présentent¹⁸²⁴. Cela signifie que tout traitement de données de recherche à ces fins bénéficie systématiquement et prioritairement à la santé publique et, par suite, à la collectivité. La restriction de l'autodétermination informationnelle du patient à l'égard de la mise à disposition de ses données médicales à des fins de recherche ne serait-elle pas implicitement consacrée ?

¹⁸²¹ Considérant 157 du RGPD.

¹⁸²² CCNE, *Numérique & Santé Quels enjeux éthiques pour quelles régulations ?*, 19 novembre 2018, p. 45.

¹⁸²³ Article 66.I de la loi Informatique et Libertés modifiée.

¹⁸²⁴ Article 66 de la loi Informatique et Libertés.

Concrètement, chaque recherche contribue notamment à l'acquisition de nouvelles connaissances dans le domaine de la santé ou à l'amélioration de la qualité et de la sécurité des soins, des thérapeutiques et des dispositifs médicaux¹⁸²⁵. Par conséquent, les recherches rétrospectives d'intérêt public dans le domaine de la santé présentent toutes des motifs légitimes et impérieux qui prévalent, certes, sur l'autodétermination informationnelle des patients concernés, mais qui servent indirectement leurs intérêts¹⁸²⁶. En l'état du droit positif, et contrairement à son application actuelle, le patient ne devrait donc pouvoir s'opposer au traitement de ses données de recherche.

527. Cette restriction de l'autodétermination informationnelle du patient concerné par l'utilisation de ses données de recherche est admissible compte tenu du fait que « *le droit à la protection des données à caractère personnel n'est pas un droit absolu* »¹⁸²⁷. Bien qu'il soit fondamental¹⁸²⁸, ce droit « *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* »¹⁸²⁹. Certainement, la limitation des droits de la personne concernée doit constituer une mesure nécessaire et proportionnée dans une société démocratique d'une part, et respecter l'essence des libertés et des droits fondamentaux des intéressés d'autre part¹⁸³⁰.

528. D'abord, l'opposabilité du droit d'opposition à l'utilisation des données de recherche du patient apparaît indispensable à la conduite ainsi qu'à la fiabilité des recherches rétrospectives dans le domaine de la santé¹⁸³¹. En effet, « *le progrès de la connaissance au service de la santé et de la société passe par l'accès, l'utilisation et le partage de ces données [de recherche] dans le respect de la protection des personnes* »¹⁸³². Leur développement permet assurément d'acquérir de nouvelles connaissances scientifiques, d'améliorer la qualité des soins, de garantir des normes élevées de sécurité des médicaments et des

¹⁸²⁵ Article 66.I de la loi Informatique et Libertés modifiée.

¹⁸²⁶ Article 21.1 du RGPD.

¹⁸²⁷ Considérant 4 du RGPD.

¹⁸²⁸ Article 8 de la CDFUE.

¹⁸²⁹ Considérant 4 du RGPD.

¹⁸³⁰ Cf. Paragraphes 332 s.

¹⁸³¹ Cf. Paragraphe 525.

¹⁸³² LESAULNIER (F.), *op. cit.*, p. 114.

dispositifs médicaux, d'anticiper les risques sanitaires en population générale, ou encore de créer des outils d'intelligence artificielle d'aide au diagnostic, à la prescription ou à la dispensation. Partant, la recherche et l'innovation dans le domaine de la santé constituent indéniablement un moyen essentiel de parvenir à la protection de la santé publique. C'est pourquoi la recherche et l'innovation en santé ont été inscrites, comme des stratégies prioritaires, au programme d'action de l'Union européenne dans le domaine de la santé publique¹⁸³³. Le législateur européen considère que le renforcement de « *l'utilisation et la réutilisation des données de santé pour la fourniture de soins de santé ainsi que la recherche et l'innovation* »¹⁸³⁴ constitue un objectif spécifique « *garantissant un degré élevé de protection de la santé humaine dans toutes les politiques et activités de l'Union* »¹⁸³⁵.

A l'échelle nationale, la protection de la santé publique a été érigée en exigence constitutionnelle¹⁸³⁶ devant être garantie par l'Etat et mise en œuvre par les pouvoirs publics. Certainement, « *la responsabilité de l'État ainsi que le rôle du Parlement en matière de politique de santé publique sont affirmés, et c'est la raison pour laquelle les objectifs de la politique de santé publique sont adoptés par la représentation nationale* »¹⁸³⁷. L'effectivité du droit à la protection de la santé, dans sa dimension collective, emporte donc une obligation d'agir à la charge du législateur¹⁸³⁸. Compte tenu de l'objectif de protection de la santé et des enjeux inhérents aux recherches n'impliquant pas la personne humaine, le législateur pourrait-il restreindre l'autodétermination informationnelle du citoyen sur ses données de recherche ?

Pour parvenir à cette exigence constitutionnelle, le législateur national est habilité à restreindre les droits fondamentaux des individus « *afin de rendre effectifs les droits et libertés constitutionnels* »¹⁸³⁹. C'est ainsi que « *le droit à la protection de la santé [en qualité*

¹⁸³³ Règlement (UE) 2021/522 du parlement européen et du conseil du 24 mars 2021 établissant un programme d'action de l'Union dans le domaine de la santé (programme « L'UE pour la santé ») pour la période 2021-2027, et abrogeant le règlement (UE) n°282/2014.

¹⁸³⁴ Article 4 f) du Règlement (UE) 2021/522 du parlement européen et du conseil du 24 mars 2021.

¹⁸³⁵ Article 4 du Règlement (UE) 2021/522 du parlement européen et du conseil du 24 mars 2021.

¹⁸³⁶ Cons. Const., 8 janvier 1991, n° 90-283 DC, *Loi relative à la lutte contre le tabagisme et l'alcoolisme*, cons.11 : RDSS, 1991, n°02, p. 204, J.-S. Cayla ; AJDA, 1991, n° 05, p. 382, comm. P. Wachsmann.

¹⁸³⁷ Fiche d'orientation, *Santé publique*, Dalloz, septembre 2020.

¹⁸³⁸ Cons. Const., 29 juillet 1991, n° 91-296 DC, *loi portant diverses mesures d'ordre social*.

¹⁸³⁹ Fiches d'orientation, *Objectif de valeur constitutionnelle*, Dalloz, juin 2020.

d'objectif à valeur constitutionnelle] *prime sur les droits individuels, qu'ils soient civils et politiques ou sociaux* »¹⁸⁴⁰. De la même façon, le juge « *n'hésite pas à faire prévaloir la protection de la santé publique, composante de l'intérêt général, sur des intérêts particuliers* »¹⁸⁴¹. En effet, les utilisations des données de recherche « *représentent un fort potentiel de contribution à la santé individuelle et collective* »¹⁸⁴². Il en résulte que le Parlement français est fondé à restreindre le droit fondamental à la protection des données personnelles au profit d'une mise à disposition des données médicales pour la recherche et l'innovation. Autrement dit, l'objectif constitutionnel de protection de la santé publique poursuivi par le législateur l'autorise à limiter le droit d'opposition du patient à l'utilisation de ses données de recherche pour un motif d'intérêt public en santé.

529. Ensuite, les objectifs à valeur constitutionnelle « *ne doivent pas porter une atteinte excessive à ces droits en les dénaturant* »¹⁸⁴³. En effet, la diminution de l'autodétermination informationnelle du patient à l'égard de ses données de recherche ne doit pas porter atteinte à la substance, ni à l'esprit du droit à la protection des données personnelles. A travers ce droit fondamental, le législateur européen a entendu protéger le respect de l'intimité de la vie privée des individus. Et cette ambition est observée lorsque la chose anthropomorphique du patient est utilisée à des fins d'étude rétrospective dans le domaine de la santé. Certainement, la confidentialité des données exploitées à des fins de recherche se trouve préservée dans la mesure où seules des données pseudonymisées ou anonymisées peuvent être mises à la disposition des responsables de traitement¹⁸⁴⁴. De surcroît, le traitement de la chose anthropomorphique à des fins de recherche doit toujours être mis en œuvre conformément aux principes et aux règles régissant la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel¹⁸⁴⁵. A ce titre, le traitement des données de recherche du patient est impérieusement conditionné par la mise en œuvre de garanties appropriées pour leurs droits, leurs libertés et leurs intérêts¹⁸⁴⁶. Il en résulte que la limitation

¹⁸⁴⁰ GRÜNDLE (T.), *Le juge et le droit à la protection de la santé*, RDSS, 2010, n°05, p.835.

¹⁸⁴¹ GRÜNDLE (T.), *loc. cit.*

¹⁸⁴² LESAULNIER (F.), *op. cit.*, p. 114.

¹⁸⁴³ Fiches d'orientation, *Objectif de valeur constitutionnelle*, Dalloz, juin 2020.

¹⁸⁴⁴ Article L.1460-1 du code de la santé publique ; Article 89.1 du RGPD.

¹⁸⁴⁵ Considérant 156 du RGPD.

¹⁸⁴⁶ Cf. Paragraphe 478.

de l'autodétermination informationnelle du patient concerné ne méconnaît pas le contenu du droit fondamental à la protection des données personnelles. La réalisation d'une recherche rétrospective concourant à un motif d'intérêt public pour la santé publique ne préjudicie ni à l'intégrité du corps humain¹⁸⁴⁷, ni à la confidentialité de la chose anthropomorphe particulièrement intime. Compte tenu de ce qui précède, la restriction du droit d'opposition à l'utilisation des données de recherche apparaît équitablement légitimée par la protection de la santé publique. En conséquence, la limitation de l'autodétermination informationnelle du patient sur ses données de recherche constitue la solution la plus protectrice de l'intérêt le plus légitime¹⁸⁴⁸.

530. La restriction de l'autodétermination informationnelle du patient concerné par l'exploitation de ses données de recherche concerne également les personnes décédées. Alors que les droits de la personne concernée s'éteignent en principe à son décès¹⁸⁴⁹, elle peut définir des directives relatives au sort de ses données personnelles après ce malheureux événement¹⁸⁵⁰. Plus précisément, ces directives « *définissent la manière dont la personne entend que soient exercés, après son décès, les droits* » qu'elle détenait sur ses données personnelles de son vivant¹⁸⁵¹. Cela signifie que les directives qu'elle souhaite appliquer au traitement de ses données personnelles après son décès doivent correspondre aux prérogatives qui lui étaient concédées de son vivant. Autrement dit, les droits appliqués aux données personnelles de la personne décédée doivent lui être effectivement reconnus. Pour cela, le droit invoqué au sein des instructions laissées par la personne décédée doit réellement exister. Or, l'applicabilité d'un droit dépend de la nature catégorielle de la donnée personnelle, de la base légale du traitement, de sa finalité et des motifs poursuivis par le responsable de traitement. En l'occurrence, le motif d'intérêt public poursuivi par le responsable d'une recherche rétrospective peut contrarier l'application du droit d'opposition

¹⁸⁴⁷ Dans la mesure où les données de recherche constituent des données médicales produites à l'occasion de la prise en charge sanitaire du patient dans le cadre du consentement aux soins, à moins que le patient se trouvait hors d'état de s'exprimer ; Cf. Paragraphe 15.

¹⁸⁴⁸ Civ. 1^{ère}, 30 septembre 2015, n° 14-16.273, Bull. civ., I, n° 228 ; LEFP, 2015, n° 10, p. 2, note T. Douville ; Gaz. Pal., 2015, n° 288, p. 24, note C. Berlaud ; JCP G, 2015, n° 51, comm. 1385, P. Ducoulombier ; CCE, 2015, n° 11, comm. 92, obs. A. Lepage ; D., 2016, n° 05, p. 277, obs. E. Dreyer ; RTD civ., 2016, n° 02, p. 449, obs. N. Cayrol.

¹⁸⁴⁹ Article 84 de la loi Informatique et Libertés modifiée.

¹⁸⁵⁰ Article 85.I de la loi Informatique et Libertés modifiée.

¹⁸⁵¹ Article 85.I de la loi Informatique et Libertés modifiée.

à l'utilisation des données de recherche de la personne concernée¹⁸⁵². C'est alors que l'exploitation de la chose anthropomorphique à des fins d'intérêt public dans le domaine de la santé s'oppose également au patient décédé quand bien même il en aurait exprimé le refus.

531. Sous un prisme novateur, la restriction des droits du patient sur ses données de recherche pourrait être traduite à travers un devoir de mise à disposition de celles-ci au profit de la recherche et de l'innovation dans l'intérêt de la santé publique.

¹⁸⁵² Cf. Paragraphe 526.

Paragraphe 2 : L'instauration d'un devoir de concours à la recherche et à l'innovation au bénéfice de la santé publique

« La tâche du Déontologiste est de retirer de l'obscurité où on les a enfouis, ces points de devoirs dans lesquels la nature a associé les intérêts de l'individu à ses jouissances, dans lesquels son propre bien-être a été lié, combiné, identifié avec le bien-être d'autrui ; sa tâche, en un mot, est de donner au moteur social toute l'influence du moteur personnel. »¹⁸⁵³.

532. L'inefficacité du droit d'opposition à l'utilisation des données de recherche pourrait être transcrite à travers l'instauration législative d'un devoir de concours à la recherche et à l'innovation au bénéfice de la santé publique. De cette façon, le patient, en tant que membre de la société, collaborerait positivement au développement des progrès dans le domaine de la santé auxquels ils profitent (**A**). La contribution effective des citoyens aux *recherches n'impliquant pas la personne humaine* ne résiderait pas uniquement dans la mise à disposition de leurs données de recherche pour l'intérêt public de la santé collective. En effet, la création d'un devoir civique exigerait une participation démocratique à l'intégralité du processus de recherche. C'est pourquoi la société civile devrait prendre part à la gouvernance relative à l'ouverture du domaine commun informationnel dans le respect, évidemment, du droit à la protection des données personnelles. A cette occasion, les citoyens contrôlèrent chacune des finalités des usages de leurs données de recherche : en amont de la mise en œuvre du projet, ainsi qu'en aval de l'exécution de leur devoir de participation à la santé publique (**B**).

¹⁸⁵³ BENTHAM (J.), *Déontologie*, Chapitre II, éd. Posth. 1834.

A) *Le patient débiteur de la mise en œuvre de la protection de la santé publique*

533. En raison des enjeux sanitaires qu'elle comporte, la santé publique a été érigée en exigence à valeur constitutionnelle¹⁸⁵⁴ dont la mise en œuvre justifie des limitations aux droits et libertés individuels par le législateur. A cet égard, les dispositions du RGPD énoncent que toute limitation aux droits octroyés à la personne concernée sur ses données personnelles ne peut intervenir que par la voie de mesures législatives prises par le droit de l'Union ou le droit d'un Etat membre¹⁸⁵⁵. Cela signifie que la restriction des droits des citoyens sur leurs données médicales en faveur de la recherche doit être légalement consacrée. Certainement, « *sous la Ve République, seul le législateur est compétent pour fixer des règles qui touchent aux libertés publiques* »¹⁸⁵⁶. Il conviendrait alors de construire un arsenal législatif permettant de démontrer que la concrétisation de la protection de la santé publique par le biais de la recherche implique indéniablement l'opposabilité du droit d'opposition vis-à-vis de l'ensemble des citoyens. En effet, qu'advierait-il des études rétrospectives si l'intégralité des patients s'opposaient à l'utilisation de leurs données de recherche ? Une telle hypothèse paralyserait l'écosystème de l'innovation dans le secteur de la santé. Concrètement, cette restriction législative pourrait être objectivée par l'instauration d'un devoir de concours à la recherche et à l'innovation dans le domaine de la santé publique. Grâce à la primauté de l'objectif de protection de la santé publique à valeur constitutionnelle¹⁸⁵⁷, et compte tenu des dérogations réglementaires au droit d'opposition¹⁸⁵⁸, le législateur bénéficierait d'une solide assise juridique pour créer un tel devoir légal et contraignant. Certainement, « *le Parlement doit désormais démontrer que la politique*

¹⁸⁵⁴ Cons. Const., 8 janvier 1991, n° 90-283 DC, *Loi relative à la lutte contre le tabagisme et l'alcoolisme* : RDSS, 1991, n°02, p. 204, J.-S. Cayla ; AJDA, 1991, n° 05, p. 382, comm. P. Wachsmann ; Cons. Const., 13 août 1993, n° 93-325 DC, *Loi de la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France* : D., 1994, n° 13, p. 111, obs. D. Maillard Desgrées du Loû ; Dr. soc., 1994, n° 01, p. 69, étude J.-J. Dupeyroux et X. Prétot ; RFDA, 1993, n° 05, p. 871, note B. Genevois ; Rev. crit. DIP, 1994, n° 01, p. 01, ét. D. Turpin ; Cons. Const., 16 mai 2012, n° 2012-248 QPC : JCP G, 2012, n° 22, 630 ; Dr. fam., 2012, n° 07, comm. 120, C. Neirinck ; AJDA, 2012, n° 19, p. 1036 ; S. Brondel ; D., 2013, n° 21, p. 1436, obs. F. Granet-Lambrechts ; AJ fam., 2012, n° 07-08, p. 406, obs. F. Chénéde ; RDSS 2012, n° 04, p. 750, note D. Roman ; RTD civ., 2012, n° 03, p. 520, obs. J. Hauser.

¹⁸⁵⁵ Article 23 du RGPD.

¹⁸⁵⁶ PECHILLON (E.), *op. cit.*, p. 648.

¹⁸⁵⁷ Cons. Const., 15 janvier 1975, n° 74-54 DC : D., 1975, p. 529, note Hamon.

¹⁸⁵⁸ Cf. Paragraphes 524 à 531.

publique qu'il entend mettre en place est bien compatible avec les principes issus du bloc de constitutionnalité et ceux tirés du bloc de conventionnalité »¹⁸⁵⁹.

534. Bien que les recherches rétrospectives menées à partir de la réutilisation des données médicales n'impliquent pas la personne humaine, les patients concernés en deviendraient les acteurs. En effet, en tant que droit-créance¹⁸⁶⁰, la protection de la santé publique trouve d'abord son existence dans le cadre de la loi pour ensuite se réaliser « *indirectement à travers l'accomplissement par le débiteur d'une prestation* »¹⁸⁶¹. L'effectivité de la protection de la santé publique requiert, en première intention, l'intervention des pouvoirs publics et, en seconde intention, la contribution de la Nation¹⁸⁶². D'une certaine façon, l'exécution de la protection de la santé publique suppose la réalisation d'un contrat social synallagmatique. Aussi surprenant que cela puisse paraître, « *les droits-créances supposent [...] dans bien des cas, la participation active des bénéficiaires à la mise en œuvre de leurs droits* »¹⁸⁶³. Il en ressort que le citoyen doit participer à la satisfaction de la protection de la santé publique à laquelle il profite, et à l'égard de laquelle il est débiteur. Il apparaît donc que le patient est tenu d'exécuter une prestation à laquelle il profitera indirectement¹⁸⁶⁴. Le rôle du patient dans la mise à disposition de ses données médicales au profit de la recherche ne résiderait plus dans l'action négative consistant au choix de ne pas y participer.

535. Force est de constater que l'instauration d'un devoir de concours à la recherche et à l'innovation en santé, par la mise à disposition de ses données médicales requalifiées en données de recherche, fait écho au principe éthique de réciprocité. Lorsqu'elle est formulée « *comme un principe servant de guide à l'action, la réciprocité est souvent mise à contribution en santé publique pour s'assurer que les pouvoirs publics ou les individus prennent en considération et agissent en fonction des obligations qu'ils ont envers les uns et*

¹⁸⁵⁹ PECHILLON (E.), *loc. cit.*

¹⁸⁶⁰ Cf. Paragraphe 335.

¹⁸⁶¹ CASAUX-LABRUNEE (L.), *Le droit à la santé*, in CABRILLAC (R.), *Libertés et droits fondamentaux 2020, op. cit.*, p. 926.

¹⁸⁶² Cf. Paragraphe 335.

¹⁸⁶³ *Ibid.*

¹⁸⁶⁴ Article 72 de la loi Informatique et Libertés.

que les autres ont envers eux »¹⁸⁶⁵. La réciprocité est matérialisée par des attributs réactifs et proactifs qui supposent que l'on redonne les bienfaits que l'on a reçus et que l'on anticipe les actions à venir¹⁸⁶⁶. Plus spécifiquement, « *en éthique de la santé publique, la réciprocité peut nous aider [...] à penser aux obligations que nous avons les uns envers les autres du fait de notre interdépendance sociale* »¹⁸⁶⁷. Le devoir de concours aux recherches n'impliquant pas la personne humaine instituerait finalement un devoir de réciprocité aux bénéfices de l'innovation en santé par la participation à la recherche mise en œuvre dans l'intérêt public. En d'autres termes, le patient devrait s'acquitter d'un tel devoir au nom de la société à laquelle il est intégré. Assurément, en tant que membre de la société, le patient est observé comme l'ultime bénéficiaire des résultats subséquents aux recherches présentant un intérêt public dans le domaine de la santé publique. Compte tenu de la nature du droit fondamental à la protection de la santé, le citoyen deviendrait l'un des acteurs de la protection de la santé publique et serait conjointement responsable de la santé collective.

Tandis que l'instauration de ce devoir conduirait à restreindre la portée des droits du citoyen sur sa chose anthropomorphique, la limitation de ses droits fondamentaux interviendrait, licitement, par une action législative. Cette norme juridique pourrait alors être fondée sur les dispositions réglementaires qui restreignent d'ores et déjà la possibilité de s'opposer aux traitements à des fins de recherche scientifique présentant un motif d'intérêt public¹⁸⁶⁸. Néanmoins, en contrepartie de l'acquiescement de ce devoir sociétal pour la santé publique, tout citoyen percevrait une récompense nationale pour la participation à un acte civique d'intérêt général¹⁸⁶⁹.

536. L'instauration d'un tel devoir citoyen impliquerait une obligation réciproque chez les producteurs de données médicales. En tant que principaux gardiens des éléments immatériels

¹⁸⁶⁵ KEELING (M.), BELLEFLEUR (O.), *Le principe de réciprocité : comment peut-il éclairer la santé publique et les politiques publiques favorables à la santé ?*, Centre de collaboration nationale sur les politiques publiques et la santé du Québec, 2014, p. 1.

¹⁸⁶⁶ KEELING (M.), BELLEFLEUR (O.), *op. cit.*, p. 2.

¹⁸⁶⁷ KEELING (M.), BELLEFLEUR (O.), *op. cit.*, p. 1.

¹⁸⁶⁸ Cf. Paragraphes 524 à 531

¹⁸⁶⁹ Cf. B) du Paragraphe 2 de la Section 2 du Chapitre 2 du Titre 1 de la Partie 2 de la présente thèse.

du corps humain du citoyen¹⁸⁷⁰, l'acte positif de mise à disposition incomberait à l'ensemble des acteurs et des institutions du système de santé. Tant les centres hospitaliers universitaires, que les cliniques privées et les cabinets de médecine de ville devraient participer à la réalisation de ce droit-créance. Pour y parvenir, de nouveaux métiers devront émerger. En effet, cette ouverture généralisée des données de recherche du citoyen demande des compétences, une gouvernance, une architecture et une interopérabilité technique et sémantique déployées sur l'ensemble du territoire national. A supposer que le Système national des données de santé formaliserait le domaine commun informationnel, les données de recherche du patient seraient mises à disposition par le Health Data Hub¹⁸⁷¹ ; et c'est ainsi que le réseau des « Hub locaux »¹⁸⁷² entrerait en action. Comme le suggérait la mission de préfiguration du Health Data Hub, « *les services du Hub seraient proposés sur l'ensemble du territoire via un Hub central appuyé d'un réseau de Hub « locaux » [...]. Chaque Hub local serait à ce titre compétent et dimensionné pour accompagner le processus d'habilitation et les opérations de préparation des jeux de données et d'aide à leur valorisation, et disposerait à cette fin d'un réservoir de compétences en propre* »¹⁸⁷³.

En complément, le Health Data Hub devrait également réunir les données de santé des utilisateurs d'objets connectés et d'applications mobiles en santé référencés dans l'Espace numérique de santé (ENS). Ainsi, les collecteurs privés¹⁸⁷⁴ devraient également contribuer à l'exercice de ce devoir citoyen de participation à la protection de la santé publique. Il s'agirait alors d'instaurer un mécanisme de portabilité facilitant une extraction standardisée de l'intégralité des données médicales et, plus largement, des données de santé « domestiques » vers leurs exploitants. L'instauration d'un nouveau devoir juridique à la charge des citoyens mobiliserait *in fine* l'ensemble de la Nation. Au demeurant, l'Etat et le citoyen devraient veiller à l'accomplissement de ce devoir par les producteurs de données de santé et de données médicales. Assurément, la création d'un tel devoir ne pourrait être envisagée sans une gouvernance citoyenne et démocratique chargée de contrôler chacun des

¹⁸⁷⁰ Les acteurs intervenants dans le système de santé sont dépositaires du secret institué à l'article L.1110-4 du code de la santé publique.

¹⁸⁷¹ Cf. Paragraphe 466.

¹⁸⁷² Voir : CUGGIA (M.), POLTON (D.), WAINRIB (G.), COMBES (S.), *op. cit.*, p. 42.

¹⁸⁷³ CUGGIA (M.), POLTON (D.), WAINRIB (G.), COMBES (S.), *op. cit.*, p. 43.

¹⁸⁷⁴ Les éditeurs d'applications mobiles en santé, les fabricants d'objets connectés en santé, etc. ...

accès aux données de recherche du citoyen, de veiller au respect de leur sécurité et de leur confidentialité, et d'étudier la qualité et la pertinence scientifique et éthique de chaque projet de recherche envisagé.

B) Le contrôle de la finalité des usages des données de recherche par la société civile

537. La prospérité et l'efficacité de la recherche et de l'innovation dans le secteur de la santé réclament tant l'instauration d'un devoir citoyen que l'instauration d'un climat de confiance. Certainement, la création d'un devoir de mise à disposition de ses données intimes au profit de la recherche requiert, au préalable, l'acceptation des intéressés. Il apparaît donc indispensable « *de constituer un dispositif rassurant permettant de faciliter l'acceptabilité sociale de cette ouverture des données de santé* »¹⁸⁷⁵ dans le respect de la protection des données personnelles.

538. En premier lieu, les droits à la transparence et à l'information effectivement reconnus aux patients concernés par l'utilisation de leurs données de recherche devraient être renforcés afin de compenser la restriction du droit d'opposition à leur traitement à des fins d'intérêt public en santé. La commission des affaires sociales affirme que le fait de « *savoir à quoi peuvent servir les données cliniques participe aussi de l'adhésion à cette fameuse culture de recherche* »¹⁸⁷⁶. Partant, « *il importe à cet effet que les professionnels de santé soient davantage sensibilisés au devoir d'information des patients sur l'utilisation qui pourra être faite de leurs données* »¹⁸⁷⁷. En pratique, les professionnels de santé, en tant que acteurs opérationnels, peuvent être chargés de délivrer l'information relative à la collecte et au traitement des données médicales qu'ils produisent à des fins de recherche.

D'abord, lorsque l'information est fournie à l'occasion de la prise en charge sanitaire du patient, les professionnels de santé doivent l'avertir que les éléments immatériels de son corps humain seront certainement requalifiés en données de recherche et réutilisés pour des

¹⁸⁷⁵ SUPIOT (E.), *Du secret médical à la mise à disposition des données de santé - le Health data hub*, Revue des contrats, 2020, n°117, p. 84.

¹⁸⁷⁶ RIST (S.), MESNIER (T.), Rapport n°1767 fait au nom de la commission des affaires sociales sur le projet de loi relatif à l'organisation et à la transformation du système de santé, volume I, Assemblée nationale, 14 mars 2019, p. 8.

¹⁸⁷⁷ *Ibid.*

motifs d'intérêt public dans le domaine de la santé. Toutefois, ce premier niveau de transparence quant au potentiel devenir des données médicales devrait être complété d'une opération d'information nationale, *a fortiori* dans le cas où un devoir de participation aux recherches rétrospectives était prescrit. Cette communication pourrait être coordonnée par l'entité¹⁸⁷⁸ chargée de réunir, d'organiser et de mettre à disposition les données de recherche implémentées dans le domaine commun informationnel avec l'appui de nouveaux Comités citoyens¹⁸⁷⁹. Aux plans nationaux et locaux, les citoyens seraient alors informés des enjeux et des modalités de l'exploitation de leurs données médicales requalifiées en données de recherche. A ce titre, pourraient être déployés une documentation à diffuser sur les sites internet des structures de santé, des applications mobiles et objets connectés, des campagnes audios et audiovisuelles à relayer dans les médias, ou encore des notices imprimées accessibles chez les producteurs de données médicales et de recherche.

Néanmoins, « aucune information précise sur le devenir de ces données n'est disponible au moment de leur collecte »¹⁸⁸⁰. C'est pourquoi une information individuelle préalable à la mise en œuvre d'un projet de recherche impliquant l'utilisation effective des données de recherche des personnes concernées doit leur être délivrée¹⁸⁸¹. Seulement, le principe de l'information individuelle préalable à l'exploitation des données de recherche tend à s'effacer au profit de la diffusion d'une information collective¹⁸⁸². Quelle que soit la modalité de délivrance de l'information relative à l'usage des données de recherche, les notices d'informations spécifiques à chacune de leurs utilisations pour un projet déterminé devraient être annexées au répertoire public ayant vocation à recenser l'ensemble des projets de recherche n'impliquant pas la personne humaine¹⁸⁸³. Ainsi, quand l'information particulière à un projet de recherche ne peut être délivrée individuellement aux patients concernés¹⁸⁸⁴, l'ensemble de la société civile en serait néanmoins avisé. Qu'ils soient ou non

¹⁸⁷⁸ Qui pourrait être incarnée par le groupement d'intérêt public dénommé Plateforme nationale des données de santé.

¹⁸⁷⁹ Cf. Paragraphe 540.

¹⁸⁸⁰ CCNE, *Données massives et santé : Une nouvelle approche des enjeux éthiques*, Avis n°130, 29 mai 2019, p. 55.

¹⁸⁸¹ Cf. Paragraphe 487.

¹⁸⁸² Cf. Paragraphe 501.

¹⁸⁸³ Le « répertoire public des projets » est disponible sur le site [www.health-data-hub.fr].

¹⁸⁸⁴ Cf. Paragraphes 496 et 500.

concernés par les recherches effectuées, tous les membres de la société devraient alors veiller au contrôle des usages des données de recherche ainsi qu'à l'existence d'une finalité d'intérêt public concourant à la protection de la santé publique. En cas de soupçon sur les motifs effectivement poursuivis par le responsable de la recherche, la société civile jouirait du pouvoir de dénoncer l'illicéité du projet auprès de l'autorité de contrôle. Quel que soit le cadre réglementaire dans lequel s'inscrit la recherche rétrospective, l'information individuelle spécifique au projet de recherche devrait être systématiquement accompagnée d'une information délivrée collectivement.

539. Le renforcement de l'information et de la transparence du traitement des données de recherche permettrait de gagner la confiance des personnes concernées. *A posteriori*, elles disposeraient ainsi d'un meilleur contrôle des usages qui en sont faits et, conséquemment, des « *obligations incombant aux* » responsables de traitement¹⁸⁸⁵.

Ce contrôle ultérieur à la mise en œuvre de la recherche s'avère éminemment important lorsque ce traitement échappe à l'autorisation préalable de la CNIL en raison de sa conformité à une méthodologie de référence. Si le responsable de la recherche est présumé remplir les conditions fixées par la méthodologie à laquelle il a attesté de sa conformité¹⁸⁸⁶, il doit néanmoins être en mesure d'en démontrer la conformité à tout moment. Pendant que les citoyens auraient le devoir de concourir à la recherche et à l'innovation en santé, les promoteurs des recherches n'impliquant pas la personne humaine auraient l'obligation de rendre compte, à la société civile, de la façon dont ils participent effectivement à l'intérêt public de la santé collective. *In fine*, l'autodétermination informationnelle procède davantage du droit à l'information que de l'exercice du consentement préalable ou du droit d'opposition au traitement. En effet, l'autodétermination informationnelle ne réside pas uniquement dans le droit de décider des usages de ses données personnelles mais également dans le droit d'en vérifier les exploitations¹⁸⁸⁷. De plus, ce contrôle peut être exercé collectivement et démocratiquement par la société civile et s'en trouverait même plus efficace. Certainement, la recherche et l'innovation dans le domaine de la santé publique devrait être l'affaire de tous.

¹⁸⁸⁵ Article 1 alinéa 2 de la loi Informatique et Libertés modifiée.

¹⁸⁸⁶ Cf. Paragraphe 439.

¹⁸⁸⁷ Cf. Paragraphe 195.

540. En second lieu, « *il est également souhaitable que les patients ou leurs représentants intègrent les structures de gouvernance des infrastructures qui permettent l'utilisation secondaire des données (cohorte, biobanques) et participent à l'élaboration du projet, des principes directeurs et des procédures d'accès mises en place* »¹⁸⁸⁸. Autrement dit, la mise à disposition des données de recherche pour des projets concourant à l'intérêt public dans le secteur de la santé devrait notamment être orchestrée par une gouvernance citoyenne. En sus d'un contrôle *a posteriori* de l'objectif poursuivi par le responsable de la recherche au moyen de son droit d'accès¹⁸⁸⁹, la société civile devrait être impliquée dans l'examen préalable de toute utilisation des données de recherche pour un projet déterminé. A cet effet, des *Comités citoyens pour la protection de l'intérêt public de l'innovation médicale* pourraient être créés à l'instar du Comité de protection des personnes chargé de rendre un avis scientifique et éthique à l'égard de toute recherche impliquant la personne humaine¹⁸⁹⁰, ou du CESREES « *chargé de rendre, avant l'autorisation de la CNIL, des avis sur les projets d'études nécessitant le recours à des données personnelles de santé* »¹⁸⁹¹. Le terme *comité* correspondrait exactement à cette émanation particulière de la société civile. En effet, un comité est un « *petit groupe de personnes faisant partie d'un ensemble constitué, investi d'un pouvoir de surveillance, de décision* »¹⁸⁹². A titre d'illustration, ces Comités pourraient, autant que de besoin, être décentralisés dans chaque territoire de démocratie sanitaire à l'échelle infrarégionale¹⁸⁹³, et tenus à la disposition des fournisseurs de données de recherche exerçant dans le ressort de ces territoires.

541. D'une part, ces comités de représentation de la société civile seraient chargés de définir la notion d'intérêt public dans le domaine de la santé. Cette conception est déterminante dans la mise en œuvre des traitements de données médicales aux fins de recherche. En effet, le caractère d'intérêt public de la recherche rétrospective conditionne la réalisation de ce traitement des éléments immatériels du corps humain du patient. Seulement,

¹⁸⁸⁸ LESAULNIER (F.), *op. cit.*, p. 108.

¹⁸⁸⁹ Cf. Paragraphes 485 et 494.

¹⁸⁹⁰ Article L.1123-7 du code de la santé publique.

¹⁸⁹¹ Documentation du SNDS, *CESREES - Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé*. Disponible en ligne sur le site [www.documentation-snds.health-data-hub.fr]. Consulté le 08 octobre 2021.

¹⁸⁹² Définition du mot « comité » par le CNRTL. Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 08 octobre 2021.

¹⁸⁹³ Article L.1434-9 du code de la santé publique.

cette notion essentielle n'est assortie d'aucune définition juridique ni d'aucun critère de détermination. Dès lors, comment s'assurer du respect de cette condition d'accès aux choses anthropomorphiques du citoyen ? La définition de l'intérêt public dans le domaine de la santé devrait se construire autour d'un consensus entre les citoyens concernés et les acteurs chargés d'en appliquer le concept. Alors que le fossé entre la société et l'écosystème de l'innovation se creuse, les citoyens pourraient être associés, au nom de la démocratie sanitaire et *via* une centralisation des Comités citoyens pour la protection de l'intérêt public de l'innovation médicale, à l'élaboration de cette orientation de santé publique¹⁸⁹⁴. La détermination de la notion d'intérêt public par la société civile permettrait de border, en toute conscience, les limites du devoir qui incomberait à chacun. Même si le patient ne peut s'opposer à l'utilisation de ses données de recherche, sa participation à la définition de la notion d'intérêt public dans le secteur de la santé circonscrirait les finalités pour lesquelles il accepterait une réduction proportionnée de son autodétermination informationnelle. Les citoyens pourraient ainsi identifier les finalités de recherche pour lesquelles la mise à disposition de leurs données intimes semblerait admissible. Cette implication permettrait d'instaurer un climat de confiance dans l'édification d'un devoir de concours à la recherche et à l'innovation dans le domaine de la santé.

542. D'autre part, les Comités citoyens pour la protection de l'intérêt public de l'innovation médicale pourraient examiner l'existence du caractère d'intérêt public – défini démocratiquement – lorsque l'utilisation de données de recherche est exemptée de l'avis du CESREES. Bien que le CESREES, au sein duquel siègent deux représentants de l'Union nationale des associations agréées d'usagers du système de santé, est d'ores et déjà chargé de se prononcer sur le caractère d'intérêt public des projets de recherche n'impliquant pas la personne humaine, son avis n'est sollicité que pour les projets soumis à l'autorisation préalable de la CNIL¹⁸⁹⁵. Lorsque le projet de recherche est conforme à une méthodologie de référence, il peut être mis en œuvre sans formalité préalable¹⁸⁹⁶. Le cas échéant, l'évaluation du motif d'intérêt public du projet est laissée à la seule appréciation du promoteur de la recherche. Pourtant, n'y a-t-il pas un conflit entre les intérêts du responsable de la recherche qui envisage de traiter les choses anthropomorphiques des patients concernés, les intérêts

¹⁸⁹⁴ Article L.1411-1 du code de la santé publique.

¹⁸⁹⁵ Article 66.III de la loi Informatique et Libertés.

¹⁸⁹⁶ Article 73 de la loi Informatique et Libertés.

personnels de ces principaux intéressés et l'intérêt public ? Etant donné que la recherche et l'innovation en santé permettent notamment de générer de l'économie¹⁸⁹⁷, les exploitants des données de recherche pourraient être tentés de privilégier leurs intérêts financiers au détriment des droits des personnes concernées et des intérêts collectifs pour la santé publique. Par suite, l'évaluation de ce motif apparaît particulièrement essentielle lorsque l'accès aux données de recherche du patient est sollicité par des acteurs privés tels que les entreprises du médicament ou les fabricants de logiciels et d'applications mobiles en santé.

543. C'est pourquoi les Comités citoyens pourraient être systématiquement consultés préalablement à toute recherche n'impliquant pas la personne humaine afin de réaliser « *une évaluation rigoureuse et transparente de l'intérêt des recherches, qui doivent contribuer au bénéfice de tous à un enrichissement des connaissances dans le domaine de la santé* »¹⁸⁹⁸. Alors que ces Comités citoyens seraient automatiquement chargés d'évaluer le motif poursuivi par les projets exemptés d'une autorisation de la CNIL et de l'avis du CESREES, quelles devraient être la forme, la force et la valeur de leurs délibérations ?

Si les méthodologies de référence permettent de présumer la conformité du traitement aux principes de protection des données personnelles, aucune appréciation ne permet véritablement d'assurer la pertinence éthique et scientifique des projets de recherche. Ces Comités citoyens, en représentation de la société civile, deviendraient alors les garants de l'intérêt public des recherches et de l'innovation en santé au bénéfice desquelles les citoyens seraient astreints à un devoir. A cet effet, ils disposeraient de leviers permettant de dénoncer tout usage contraire à l'intérêt public préalablement défini. Si l'intérêt public pour la santé publique faisait défaut, il appartiendrait à ces Comités de suspendre la mise en œuvre de la recherche à la révision des motifs invoqués par son promoteur. A défaut de correction probante, l'accès aux données de recherche ne pourrait être dû aux responsables d'une recherche ne concourant pas à la protection de la santé publique. Au risque de favoriser la défense des intérêts personnels des citoyens, ces Comités pourraient éventuellement intégrer des experts en matière de recherche dans le domaine de la santé, de l'éthique et du droit. Le cas échéant, ces Comités citoyens constitueraient des représentations locales du CESREES qui seraient, en toutes circonstances, saisies préalablement au démarrage de toute

¹⁸⁹⁷ Cf. Paragraphe 438.

¹⁸⁹⁸ CCNE, *Données massives et santé : Une nouvelle approche des enjeux éthiques*, op. cit., p. 58.

recherche n'impliquant pas la personne humaine. Ainsi, la présence de l'intérêt public, tel que défini et accepté par la société civile, serait invariablement garantie par la société civile elle-même.

Le devoir de concours à la recherche et à l'innovation au bénéfice de la santé publique au moyen de la mise à disposition des données de recherche des patients serait donc maîtrisé et contrôlé par la démocratie sanitaire.

Conclusion du chapitre

544. Curieusement, les traitements des données de recherche à des fins d'étude scientifique en santé sont perçus comme une circonstance dérogatoire aux principes directeurs du droit à la protection des données personnelles, laquelle requiert paradoxalement de renforcer les droits et les intérêts des personnes concernées. Cette antinomie tente de concilier la facilitation de la mise en œuvre de la recherche scientifique avec le maintien de la protection de la chose anthropomorphique ainsi exploitée. En effet, les dérogations juridiques au profit de la recherche scientifique ont vocation à mobiliser les personnes concernées, les producteurs de données médicales ainsi que les promoteurs de recherche. Seulement, la participation effective de l'ensemble de la Nation à l'innovation sanitaire commande d'instaurer un devoir légal contraignant accompagné d'un régime juridique rassurant.

D'une part, la création d'un devoir légal de concours à la recherche et à l'innovation au bénéfice de la santé publique impliquerait une mise à disposition coordonnée des données de recherche essentielles aux progrès dans le domaine de la santé. En conséquence, l'ensemble des citoyens composé des patients, des fournisseurs des données de recherche et des porteurs de projets d'intérêt public dans le domaine de la santé devraient concourir à leur utilisation effective au profit de la collectivité. D'autre part, la diminution de l'autodétermination informationnelle du citoyen exigerait d'accroître la protection de ses données médicales. C'est pourquoi l'édification d'un régime spécifique aux choses anthropomorphiques nécessiterait, à nouveau, d'être consacrée.

545. Cette double exigence pourrait se concrétiser à travers la construction d'un domaine commun informationnel rassemblant l'intégralité des données médicales produites par les établissements et les professionnels de santé à l'occasion de toute prise en charge sanitaire sans condition de financement. De toute évidence, leur implémentation supposerait préalablement leur requalification en données de recherche et, subséquentement, leur pseudonymisation ou leur anonymisation.

L'intégration des données de recherche de tout citoyen au sein du domaine commun informationnel résulterait du statut de la chose anthropomorphique en sa qualité de chose

commune¹⁸⁹⁹. Contrairement à l'actuel Système national des données de santé, ce regroupement ne découlerait pas des modalités de prise en charge des frais de santé en matière de maladie, de maternité, d'accidents du travail ou de maladies professionnelles¹⁹⁰⁰. Si le SNDS a été élargi à certaines données médicales, ce n'est qu'à la condition qu'elles aient été recueillies à l'occasion d'actes financés par la solidarité nationale¹⁹⁰¹. Selon le raisonnement retenu, les données médicales collectées à l'occasion d'un acte financé par l'assurance maladie seraient, par raccourci, des données financées par la communauté. En conséquence, ces données constitueraient un patrimoine commun appartenant à la collectivité qui pourrait en faire usage et les exploiter. Seulement, la totalité des dépenses liées à un acte ou à une prestation en santé n'est pas toujours couverte par la sécurité sociale¹⁹⁰². Bien qu'un pourcentage des dépenses associées au service rendu par un professionnel de santé soit pris en charge par l'Assurance maladie obligatoire, une partie des dépenses, nommée ticket modérateur, peut rester à la charge du patient¹⁹⁰³. Néanmoins, ce ticket modérateur peut être réglé, pour tout ou partie, par une *assurance complémentaire santé*. Les frais non couverts par l'Assurance maladie obligatoire restant à la charge du patient peuvent donc être remboursés par une *complémentaire santé* selon les termes du contrat souscrit. Les actes et les prestations en santé sont donc payés par l'Assurance maladie obligatoire ainsi que par les régimes complémentaires et les patients eux-mêmes. Alors, si les pouvoirs publics estiment que les données médicales tomberaient dans un « patrimoine commun » par le simple fait qu'elles soient financées par l'Assurance maladie, nous ne pourrions qu'admettre que les données médicales seraient également acquises dans le patrimoine des mutualistes. Afin de pallier cette dangereuse éventualité, le statut de la chose anthropomorphique – commune – devrait être juridiquement consacré. En effet, sa nature extrapatrimoniale, son exclusion du marché et son adjonction aux côtés des choses communes s'opposeraient à toute acquisition par un quelconque financement.

546. Au demeurant, l'implémentation de la chose anthropomorphique dans le domaine commun informationnel permettrait de l'écarter définitivement de la communauté des biens

¹⁸⁹⁹ Cf. Paragraphe 466.

¹⁹⁰⁰ Article L.1461-1 I 6° du code de la santé publique.

¹⁹⁰¹ CUGGIA (M.), POLTON (D.), WAINRIB (G.), COMBES (S.), *op. cit.*, p. 3, p. 5, P. 40.

¹⁹⁰² Article L.160-14 du code de la sécurité sociale.

¹⁹⁰³ Article L.160-13 du code de la sécurité sociale.

ainsi que de toute dérive mercantile¹⁹⁰⁴. Les éléments immatériels du corps humain du patient, anonymisés ou pseudonymisés à leur implémentation, seraient universellement accessibles pour tout projet d'intérêt public dans le domaine de la santé publique. L'organisme public chargé de sa gouvernance, en lien avec les *Comités citoyens pour la protection de l'intérêt public de l'innovation médicale*, constituerait le guichet unique de l'accès à toute donnée de recherche ainsi requalifiée. Les promoteurs de recherche n'auraient plus à s'adresser aux producteurs des données médicales ni à réaliser des études rétrospectives multicentriques pour obtenir suffisamment d'éléments nécessaires à l'accomplissement des objectifs décrits dans le protocole scientifique de la recherche. Ainsi, les responsables de recherche dans l'intérêt public de la santé ne seraient plus contractuellement liés qu'avec l'entité responsable du domaine commun informationnel. De la même façon, cette personne morale de droit public serait l'unique point de contact des citoyens concernés. Grâce à l'instauration d'un tiers de confiance dépositaire du secret professionnel médical et gardien de la table de correspondance des pseudonymes, les personnes concernées par l'utilisation de leur chose anthropomorphique seraient systématiquement informées individuellement de la concrétisation de leur devoir. Pareillement, l'exercice des droits qui leurs sont effectivement reconnus s'en trouverait considérablement facilité, notamment par des téléservices pouvant devenir accessibles *via* l'Espace numérique de santé.

547. En définitive, cette centralisation participerait à l'accroissement de la transparence et de la confiance dans le *Bigdata* de la recherche rétrospective dans le domaine de la santé. Les données médicales du patient ne feraient plus l'objet d'extractions temporaires des dossiers médicaux engendrant des risques sécuritaires évidents. A l'inverse, les capacités de recherche n'impliquant pas la personne humaine seraient décuplées, facilitées et généralisées, tandis que la protection des données de recherche des citoyens astreints au devoir de concours à la recherche et à l'innovation au bénéfice de la santé publique serait prodigieusement renforcée.

Dans la mesure où la création de ce domaine commun informationnel participerait à la concrétisation de la protection de la santé publique, la chose anthropomorphique du patient pourrait être utilisée pour tout motif d'intérêt public dans le domaine de la santé. Par

¹⁹⁰⁴ Cf. Paragraphe 466.

conséquent, la création d'un domaine commun informationnel concentrant toute chose anthropomorphique favoriserait la lutte contre les menaces sanitaires pesant sur la santé des citoyens et revêtirait, à cet égard, une importance stratégique forte.

Chapitre 2 : La lutte contre les menaces sanitaires par la datasurveillance : l'exemple des traitements déployés pour faire face à la pandémie de la Covid-19

« La pandémie de COVID-19 est une urgence de santé publique de portée internationale qui requiert une réponse coordonnée et de grande ampleur de la part des gouvernements du monde entier. Cependant, les initiatives des États visant à contenir le virus ne doivent pas servir de prétexte à entrer dans une nouvelle ère de systèmes généralisés de surveillance numérique invasive. »¹⁹⁰⁵.

548. La surveillance sanitaire, définie comme « *le processus de collecte systématique, organisé et continu de données de santé ainsi que leur analyse, interprétation et dissémination dans une perspective d'aide à la décision et d'évaluation* »¹⁹⁰⁶, constitue l'« *outil de base de la santé publique et de la sécurité sanitaire* »¹⁹⁰⁷. En effet, la surveillance individuelle des malades comme la surveillance de la santé des populations sont au cœur de la santé publique depuis la médecine hippocratique¹⁹⁰⁸. La datasurveillance a donc largement précédé à la gestion de la pandémie de la Covid-19 et perpétuera aux fins de veille, de préparation et de réponse aux menaces sanitaires à venir. Cependant, l'emploi de la datasurveillance par les pouvoirs publics, pour faire face à la crise sanitaire liée au SARS-CoV-2, a été vivement décrié par une portion de la doctrine juridique¹⁹⁰⁹ et a entraîné une défiance populationnelle.

¹⁹⁰⁵ Amnesty International, Déclaration conjointe de la société civile, Le recours aux technologies de surveillance numérique pour combattre la pandémie doit se faire dans le respect des droits humains, 2 avril 2020. Disponible en ligne sur le site [www.amnesty.org]. Consulté le 18 octobre 2021.

¹⁹⁰⁶ DESENCLOS (J.-C.), *Surveillance et veille sanitaire : concepts, définition et organisation*, In DABIS (F.), DESENCLOS (J.-C.), *Épidémiologie de terrain*, 2^{ème} ed., John Libbey Eurotext, 2017, p. 84.

¹⁹⁰⁷ DESENCLOS (J.-C.), BRÜCKER (G.), *Surveillance*, In BOURDILLON (F.), BRÜCKER (G.), TABUTEAU (D.), *Traité de santé publique*, Lavoisier, 2016, p. 79.

¹⁹⁰⁸ Cf. Paragraphe 608.

¹⁹⁰⁹ Voir notamment : PAWLOTSKY (A.), *L'utilisation des données personnelles dans le cadre de la lutte contre l'épidémie de Covid-19, un risque pour les droits et libertés ?*, La Revue des droits de l'homme, Actualités Droits-Libertés, avril 2020 ; ZORN (C.), *État d'urgence pour les données de santé (II) : sidep et contact covid*, Dalloz actualité, 26 mai 2020 ; PY (B.), *Les épidémies et le secret professionnel*, RDS, 2020, n° 96, p. 700.

Eu égard au caractère inédit de cette menace sanitaire, les pouvoirs publics ont en effet recouru à des systèmes d'informations fondés sur la réutilisation des données médicales de la population et proportionnels à l'ampleur et à la gravité de la pandémie (**Section 1**). Par conséquent, des traitements massifs de données médicales nominatives, centralisés par l'administration, ont été généralisés sur l'ensemble du territoire de la République. Au surplus de ce fichage de masse, des dispositifs numériques, destinés à l'usage des membres de la société et établis à partir de leurs données médicales pseudonymisées, ont infiltré leur vie privée.

549. S'il est évident que l'emploi de ces systèmes d'information emporte des atteintes aux droits à la vie privée et à la protection des données, que les technologies du numérique comportent des risques sécuritaires endogènes et que leurs usages peuvent dégénérer vers des dérives totalitaires, il apparaît essentiel de saisir les opportunités que l'informatique procure. Si la réutilisation des données médicales semble incontournable pour lutter contre une menace sanitaire, les dispositifs numériques en facilite le traitement dans un contexte d'urgence globalisé. Ils présentent alors un appui considérable pour l'objectivation des stratégies sanitaires de crise et des politiques de santé publique. Bien que « *le débat très franco-français a sans doute été contre-productif et a révélé une vision fantasmée de Big Brother* »¹⁹¹⁰, l'encadrement juridique et éthique de la réutilisation de données médicales à grande échelle offre un garde-fou permettant de jouir de l'informatique pour préserver notre bien commun qu'est la santé publique et, *in fine*, pour servir l'humanité (**Section 2**).

550. Les spécificités juridiques des traitements de données médicales à des fins de lutte contre une menace sanitaire seront illustrées à travers les dispositifs SI-DEP, Contact Covid, TousAntiCovid ainsi que les Passes sanitaire et vaccinal déployés par l'Etat français dans le contexte de la pandémie de la Covid-19.

Sommairement, le système d'information SI-DEP, mis en œuvre par le ministère de la santé, centralise l'ensemble des résultats des examens virologiques et sérologiques au SARS-CoV-2. Ce fichage permet principalement de réaliser de la surveillance épidémiologique ainsi que des investigations de *contact tracing* au moyen du système

¹⁹¹⁰ BLOCH (L.), *Rapport de synthèse*, In BLOCH (L.), *Numérique et crise sanitaire*, Université de Bordeaux, LEH Édition, Actes et séminaires, février 2021, p. 49.

d'information Contact Covid. En effet, le dispositif Contact Covid, mis en œuvre par la Caisse nationale d'assurance maladie, permet de contacter les personnes infectées par le virus de la Covid-19 dans l'espoir d'identifier et d'alerter les personnes à risque de contamination et, concomitamment, de rompre les chaînes de transmission.

En complément des enquêtes sanitaires conduites par les brigades de l'Assurance maladie et des Agences régionales de santé, le ministère de la santé a déployé le dispositif TousAntiCovid. S'ils le désirent, les individus équipés d'un ordiphone ont la faculté de télécharger cette application mobile afin d'être alertés d'un risque de contamination lorsqu'ils ont été à proximité d'un utilisateur déclaré positif au SARS-CoV-2.

En outre, les citoyens peuvent, le cas échéant, générer un *Passe sanitaire* ou un *Passe vaccinal*, auxquels est intégré le Certificat numérique européen¹⁹¹¹, afin de voyager en dehors du territoire hexagonal et d'accéder aux lieux, aux événements et aux services subordonnés à sa présentation. Le *Passe sanitaire* est un justificatif apportant la preuve que son titulaire a reçu un schéma vaccinal complet, qu'il a été testé négativement au virus de la Covid-19 ou qu'il a acquis une immunité après avoir été infecté par ce virus. Depuis le 24 janvier 2022, ce justificatif est requis pour les personnes âgées de douze à quinze ans qui désirent bénéficier des activités du quotidien comme les activités culturelles, les activités de restauration commerciales ou encore l'accès aux grands centres commerciaux¹⁹¹². Le *Passe sanitaire* est également demandé à toute personne âgée de plus de douze ans souhaitant voyager à destination ou en provenance du territoire hexagonal¹⁹¹³, ou accéder aux services et aux établissements de santé, sociaux et médico-sociaux¹⁹¹⁴. Par ailleurs, le *Passe vaccinal* est un justificatif établissant l'unique preuve selon laquelle son titulaire a reçu un schéma vaccinal complet. Cette obligation vaccinale est requise pour toute personne âgée de plus de seize ans qui désire – notamment – exercer des activités de loisirs, des activités de restauration

¹⁹¹¹ Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19, *JOUE* L 211/1, 15 juin 2021.

¹⁹¹² Article 1^{er} II-A 3° b) de la loi n° 2021-689 du 31 mai 2021, *JORF* n°125, 1^{er} juin 2021, texte n° 1, dans sa version en vigueur au 24 janvier 2022.

¹⁹¹³ Article 1^{er} II-A 1° de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

¹⁹¹⁴ Article 1^{er} II-A 3° a) de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

commerciale ou de débit de boissons, emprunter des transports publics interrégionaux ou encore participer à des foires, des séminaires et des salons professionnels¹⁹¹⁵.

L'ensemble de ces systèmes d'information ont été instaurés dans le cadre exceptionnel de l'état d'urgence sanitaire. Leur existence comme leur caducité apparaissent donc imbriquées à la temporalité de ce régime – théoriquement – provisoire.

¹⁹¹⁵ Article 1^{er} II-A 2° de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

Section 1 : L'exceptionnalité du fichage massif de données sensibles

551. L'état d'urgence sanitaire est un régime de crise pendant lequel les pouvoirs sont concentrés entre les mains de l'exécutif, alors autorisé à restreindre certaines des libertés individuelles et collectives¹⁹¹⁶. Néanmoins, lorsque l'action du Gouvernement a pour effet de limiter les droits fondamentaux des individus, leur restriction ne peut être autorisée que par un acte législatif¹⁹¹⁷. En substance, « *le processus de limitation pourrait se définir comme l'opération qui consiste à restreindre, par une règle de droit, la portée ou l'exercice d'un droit ou d'une liberté garantie, dans un but prévu par le Constituant* »¹⁹¹⁸. Afin de favoriser l'accomplissement de l'objectif constitutionnel de protection de la santé, le législateur a usé de ce processus de limitation des droits fondamentaux. Pour renforcer les capacités des traitements exceptionnellement déployés pour lutter contre la menace sanitaire, il a donc restreint les droits reconnus aux personnes concernées sur leurs données médicales personnelles (**Paragraphe 2**), et a élargi les professionnels habilités à connaître ces informations intimes (**Paragraphe 1**). Bien que les circonstances exceptionnelles justifient des mesures exceptionnelles¹⁹¹⁹, les sages de la rue Montpensier ont rappelé qu'il appartenait au législateur « *d'assurer la conciliation entre l'objectif de valeur constitutionnelle de protection de la santé et le respect des droits et libertés reconnus à tous ceux qui résident sur le territoire de la République* »¹⁹²⁰.

Paragraphe 1 : L'exception de la communication des données médicales confidentielles

552. Dans l'unique espoir de protéger la santé publique, des dispositions législatives ont autorisé la mise en œuvre de traitements de données médicales afin de lutter contre la menace sanitaire provoquée par le SARS-CoV-2. Si la santé publique repose immanquablement sur le traitement des données relatives à la santé des membres de la société, la divulgation des données médicales des personnes fichées constitue une ingérence notoire au sein de leur vie

¹⁹¹⁶ Article L.3131-15 du code de la santé publique.

¹⁹¹⁷ Cf. Paragraphe 593.

¹⁹¹⁸ GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, Les nouveaux cahiers du Conseil constitutionnel, octobre 2014, n°45.

¹⁹¹⁹ Théorie jurisprudentielle des circonstances exceptionnelles.

¹⁹²⁰ Cons. Const., 11 mai 2020, n°2020-800 DC, Communiqué de presse du 11 mai 2020.

privée (A). Néanmoins, la préservation de la confidentialité de ces informations secrètes, au moyen de mesures juridiques et techniques, tend à limiter les atteintes portées par ces systèmes d'information (B).

A) La divulgation des données médicales de la personne fichée

553. Différents traitements manuels et informatiques des données personnelles des membres de la société ont été déployés afin de lutter contre la crise sanitaire liée à la pandémie de la Covid-19. Ces systèmes d'information ont été directement intégrés aux stratégies globales de lutte contre la propagation de ce virus telles que définies au niveau international, européen et national. Notamment, ces dispositifs sont au cœur du triptyque « *protéger, tester, isoler* »¹⁹²¹ et visent à rompre les chaînes de contamination ainsi qu'à réduire les risques d'infection au SARS-CoV-2. En somme, ces systèmes d'information constituent les outils d'objectivation de la politique de protection de la santé publique édifiée par le Gouvernement. Toutefois, ces outils de gestion de crise sanitaire impliquent le traitement, à grande échelle, de données connexes à la santé des citoyens et, particulièrement, de données médicales. Le cas échéant, seront traitées les données relatives à la virologie, à la sérologie ou à l'immunologie des personnes concernées ainsi que toutes données cliniques permettant d'en établir le diagnostic de façon probante. De toute évidence, les systèmes d'information dédiés à la lutte contre la crise sanitaire, et centralisés par l'administration, représentent un fichage extraordinairement sensible des éléments immatériels du corps humain de la quasi-totalité des résidents français. Par conséquent, « *ils constituent [...] un risque pour le droit au secret des données à caractère personnel, le droit au respect de la vie privée ou encore le secret médical* »¹⁹²².

554. En dépit des dangers endogènes au traitement des données médicales de plusieurs centaines de milliers de personnes fichées¹⁹²³, le droit à la protection des données

¹⁹²¹ Déclaration de M. Édouard Philippe, Premier ministre, sur la stratégie nationale de déconfinement suite à l'épidémie de covid-19 à compter du 11 mai prononcée à l'Assemblée nationale le 28 avril 2020. Disponible en ligne sur le site [www.vie-publique.fr]. Consulté le 20 octobre 2021.

¹⁹²² PELLEGRINI (F.), SKRZYPNIAK (H.), *Les libertés publiques face au traçage numérique*, In BLOCH (Laurent), *Numérique et crise sanitaire*, Université de Bordeaux, LEH Édition, Actes et séminaires, février 2021, p. 19.

¹⁹²³ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 22.

personnelles concède leur utilisation lorsqu'elle poursuit des motifs d'intérêt public dans le domaine de la santé publique. Le législateur européen considère en effet que « *des dérogations à l'interdiction de traiter des catégories particulières de données à caractère personnel devraient également être autorisées [...] lorsque l'intérêt public le commande [...] à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé* »¹⁹²⁴. A ce titre, les dispositions de droit commun du RGPD permettent aux Etats membres de l'Union européenne de fonder la licéité du traitement des données médicales de leurs ressortissants sur l'exécution d'une mission d'intérêt public, définie par une disposition normative, dont sera investi l'organisme chargé de sa mise en œuvre¹⁹²⁵. Egalement, les dispositions européennes n'appliquent pas le principe d'interdiction de traitement des données sensibles lorsqu'il apparaît « *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* »¹⁹²⁶.

A droit constant, « *le cadre posé par ces instruments ouvre [donc] la voie à plusieurs possibilités d'utilisation des données personnelles par le gouvernement dans le cadre de la lutte contre l'épidémie de Covid-19* »¹⁹²⁷. C'est ainsi que l'ensemble des systèmes d'information mis en œuvre par les pouvoirs publics dans la lutte contre la propagation du SARS-CoV-2 ont trouvé une assise juridique permettant d'approuver l'utilisation des données médicales des citoyens et des résidents français. En effet, « *les exigences en matière de protection des données ne font pas obstacle à la collecte et au traitement de données à caractère personnel en lien avec la pandémie* »¹⁹²⁸, quand bien même il s'agirait de données médicales. Il résulte de ce qui précède que les systèmes d'information créés dans le cadre de la gestion de la crise sanitaire ne reposent aucunement sur le consentement des personnes concernées. Autrement dit, les personnes fichées ne peuvent consentir au traitement de leurs

¹⁹²⁴ Considérant 52 du RGPD.

¹⁹²⁵ Article 6.1 e) du RGPD.

¹⁹²⁶ Article 9.2 i) du RGPD.

¹⁹²⁷ PAWLOTSKY (A.), *op. cit.*, § 4.

¹⁹²⁸ METALLINOS (N.), *Covid-19 : l'état d'urgence sanitaire à l'épreuve du droit de la protection des données à caractère personnel*, LexisNexis, Communication - Commerce Electronique, 2020, n° 5, étude n°9, § 1.

données médicales à des fins d'intérêt public dans le domaine de la santé publique, nonobstant leur caractère nominatif ou pseudonymisé.

555. Toutefois, « *il n'y a pas de partage [d'informations nominatives à caractère secret] entre deux individus exerçant des métiers étrangers [...] sauf dans les cas où la loi l'impose ou l'autorise* »¹⁹²⁹. C'est ainsi que le législateur a exceptionnellement étendu le partage du secret professionnel médical entre les professionnels intervenant dans le cadre des systèmes SI-DEP et Contact Covid¹⁹³⁰. En effet, ces deux systèmes d'information reposent sur le traitement de données médicales nominatives permettant d'identifier directement les personnes fichées. Il était donc obligatoire que les professionnels chargés de « *réaliser l'ensemble des nombreuses enquêtes nécessaires au dépistage et à l'identification des chaînes de transmission* »¹⁹³¹ soient légalement dépositaires d'un secret identique. En effet, lorsque le législateur autorise la communication d'informations à caractère secret entre des professionnels exerçant des missions étrangères, ils « *sont bien tenus au secret dans les termes de l'article 226-13 du code pénal* »¹⁹³². Virginie Peltier rappelle que « *le secret est professionnel parce que la loi le dit* »¹⁹³³. Le législateur pouvait donc décider de soumettre les personnes mobilisées dans la mise en œuvre des systèmes d'information SI-DEP et Contact Covid au secret de toutes données médicales connues à l'occasion de cette mission de protection de la santé publique.

Concrètement, les brigades sanitaires de l'Assurance maladie et des Agences régionales de santé accèdent, au moyen du dispositif Contact Covid, aux données médicales relatives aux personnes contaminées. Ces informations confidentielles y sont renseignées à partir des résultats de dépistages colligés au sein du dispositif SI-DEP, ou par le médecin ayant conclu à une infection au SARS-CoV-2 sur le fondement d'éléments cliniques probants. Une fois identifiée dans le système Contact Covid, la personne contaminée est alors

¹⁹²⁹ PELTIER (V.), *Révélation d'une information à caractère secret . – Conditions d'existence de l'infraction . – Pénalités*, JurisClasseur Pénal, Fasc. 20, mai 2015, actu. mai 2021, § 32.

¹⁹³⁰ Article 11 I de la loi n°2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, *JORF* 12 mai 2020, texte n°1.

¹⁹³¹ CE, avis n°400104 du 1^{er} mai 2020 sur un projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, cons. 19.

¹⁹³² PELTIER (V.), *op. cit.*, § 30.

¹⁹³³ *Ibid.*

contactée par les enquêteurs sanitaires en vue d'identifier et d'alerter les personnes à risque de contamination. Alors que le patient peut ordinairement s'opposer¹⁹³⁴ ou refuser¹⁹³⁵ le partage de ses informations médicales entre les professionnels concourant à la coordination de ses soins, la personne contaminée par le virus de la Covid-19 ne peut ni consentir, ni s'opposer au partage de ses informations médicales à des fins de *contact tracing* dès l'instant où elle a été diagnostiquée ou dépistée positive. Effectivement, ce partage exceptionnel est, d'une part, fondé sur l'exécution d'une mission d'intérêt public dont est investi le responsable de traitement¹⁹³⁶ et, d'autre part, autorisé pour des motifs d'intérêt public dans le domaine de la santé publique¹⁹³⁷. Sans qu'il n'y ait eu besoin de recourir au consentement de la personne concernée, le législateur français était donc fondé à autoriser, « *par dérogation aux dispositions de l'article L.1110-4 du code de la santé publique, des personnes qui ne sont pas des professionnels participant à la prise en charge d'une personne, à avoir accès aux données de santé de ces personnes protégées par le secret médical* »¹⁹³⁸. Bien que des données médicales nominatives puissent être partagées par un nombre considérable d'acteurs, les intéressés ne peuvent interdire l'extension du secret professionnel médical entre les professionnels qui en sont dépositaires. Quand bien même la personne fichée était titulaire du secret protégeant ses données médicales, ces dernières peuvent être exploitées, sous le sceau de la confidentialité, par tout professionnel soumis légalement au secret.

De même que la première condition à la communication des données médicales du patient dans le cadre de sa prise en charge sanitaire réside dans l'inscription du destinataire sur l'inventaire de l'article R.1110-2 du code de la santé publique¹⁹³⁹, les professionnels appelés à connaître les données médicales nominatives des patients atteints de la Covid-19 dans la mise en œuvre de la protection de la santé publique sont exhaustivement énumérés à l'article 11 de la loi n°2020-546 du 11 mai 2020. De même que les données médicales d'un patient peuvent être communiquées à des « non-professionnels de santé » intervenant dans le cadre d'une prise en charge sanitaire, les données médicales des citoyens contaminés par le

¹⁹³⁴ Cf. Paragraphe 284.

¹⁹³⁵ Cf. Paragraphe 285.

¹⁹³⁶ Article 6.1 e) du RGPD.

¹⁹³⁷ Article 9.2 i) du RGPD.

¹⁹³⁸ CE, avis n°400104, *op. cit.*, cons. 18.

¹⁹³⁹ Cf. Paragraphe 261.

SARS-CoV-2 peuvent être partagées à des professionnels péri-médicaux. Finalement, lorsque les professionnels exercent des missions distinctes, l'unique condition au partage d'informations à caractère secret réside dans la déposition dictée par le législateur.

556. Quand bien même tout traitement de données sensibles engendre inextricablement des risques pour les libertés et les droits des personnes fichées, le secret professionnel doit être considéré comme la garantie principale de leur confidentialité¹⁹⁴⁰. Assurément, la Cour européenne des droits de l'homme a eu l'occasion de juger que la protection de la confidentialité des données médicales était capitale « *non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général* »¹⁹⁴¹. Identiquement, « *la protection de la santé publique dépend fondamentalement de la somme des confiances individuelles des patients dans les soignants* »¹⁹⁴². Bien qu'elle apparaisse gage de protection, l'extension légale du secret professionnel médical aux brigades sanitaires ne risque-t-elle pas de bouleverser la confiance que l'ensemble des individus place dans le système de santé ?

Quand le partage des données médicales du patient est légalement autorisé par-delà sa prise en charge sanitaire, cette opération de traitement pourrait fragiliser la relation de confiance qui unit le patient au professionnel de santé auquel il a confié la réalisation des actes de prévention, de diagnostic ou de soins. La particularité du secret professionnel médical s'attache à la notion de confiance, elle-même convenue comme la confiance intime d'une communication que l'on donne ou que l'on reçoit sous le sceau du secret¹⁹⁴³. En effet, le patient a conscience de confier ses données médicales personnelles et nominatives au professionnel de santé qui les a générées dans les limites d'un colloque singulier. Si le patient peut également s'attendre à ce que ces informations intimes puissent être transmises aux autres professionnels – soumis au secret – intervenant à sa prise en charge sanitaire, il ne réalise sans doute pas que ces éléments profondément intimes puissent être communiqués à d'autres fins que ses soins. Sous le prisme du patient, ce partage – quoi que légal – des

¹⁹⁴⁰ Cf. Paragraphe 566.

¹⁹⁴¹ CEDH, 25 février 1997, arrêt Z. c. Finlande, Requête n°22009/93 : JCP G, 1998, I, 107, n° 35 ; RSC, 1998, n° 02, p. 385, obs. R. Koering-Joulin.

¹⁹⁴² PY (B.), *Les épidémies et le secret professionnel*, loc. cit.

¹⁹⁴³ Définition du substantif « confiance » proposée par le CNRTL. Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 20 octobre 2021.

éléments immatériels de son corps humain pourrait être vécu comme une violation du secret qu'il a – initialement – partagé avec son professionnel de santé. En dépit de la préservation de la confidentialité des données médicales par l'ensemble des professionnels dépositaires du secret, leur partage à d'autres fins que la prise en charge sanitaire du patient constitue une ingérence dans sa vie privée. Si le partage des informations médicales entre les professionnels dépositaires d'un même secret ne constitue pas une violation pénalement répréhensible de leur confidentialité, ce partage attente à l'intimité de la vie privée de la personne concernée.

A cet égard, Bruno Py considère que « *la crise sanitaire et la loi qui en découle entérinent temporairement une nouvelle dérogation au secret professionnel au risque de sacrifier la confiance de chaque patient sur l'autel de la santé publique* »¹⁹⁴⁴. Certes, « *il n'y a pas de santé publique sans confiance publique, de confiance publique sans confiance individuelle et de confiance individuelle sans garantie du secret professionnel* »¹⁹⁴⁵. Mais dans l'hypothèse d'une menace sanitaire grave, il ne peut y avoir de santé publique sans le partage et l'exploitation des données virologiques des citoyens qui composent la société¹⁹⁴⁶. De surcroît, la confiance publique repose davantage sur l'éthique gouvernementale que sur le secret individuel. En effet, la confiance dans les institutions publiques s'appuie sur la transparence, la bienveillance, la probité et l'intégrité¹⁹⁴⁷. Lorsque le patient est honnêtement informé que les seules données médicales strictement nécessaires à la protection de la santé publique seront traitées, de façon confidentielle, par des professionnels soumis au secret, à des fins exclusives de lutte contre la propagation d'un virus virulent, et qu'elles feront l'objet d'une destruction à bref délai, la confiance de la relation médicale bilatérale semble-t-elle trahie ? La clé de la confiance se trouve également dans la communication.

557. Il serait alors plus juste de considérer qu'il n'y a pas de santé publique sans l'extension d'un secret professionnel garanti. Certainement, la lutte contre les menaces sanitaires telles que les épidémies de grande ampleur ou les pandémies nécessite le traitement des données médicales nominatives des citoyens. En effet, face à certains virus particulièrement

¹⁹⁴⁴ PY (B.), *Les épidémies et le secret professionnel*, loc. cit. ; PY (B.), *Fallait-il sacrifier le secret professionnel sur l'autel de la santé publique ?*, Médecine & Droit, 2021, n° 166, p. 1 à p. 2.

¹⁹⁴⁵ *Ibid.*

¹⁹⁴⁶ Cf. Paragraphe 548.

¹⁹⁴⁷ Voir : BOISVERT (Y.), *Crise de confiance et crise de légitimité : de l'éthique gouvernementale à l'éthique publique*, Éthique de l'administration et du service public, Vol. 4, 2002, n° 1.

dangereux et contagieux, des moyens d'action et de prévention à la source doivent être déployés pour limiter les conséquences sur la santé de la population.

C'est ainsi qu'en temps ordinaires¹⁹⁴⁸, le législateur a prescrit une obligation de signaler, à l'agence régionale de santé, les cas de maladies nécessitant une intervention urgente locale, nationale ou internationale, à la charge des médecins et des responsables des services et laboratoires de biologie médicale¹⁹⁴⁹. Ce signalement obligatoire des données individuelles à l'autorité sanitaire doit être distingué de la notification obligatoire à l'agence nationale de santé publique des données individuelles. Alors que la procédure de notification implique la transmission de données anonymisées à des fins de surveillance épidémiologique¹⁹⁵⁰, la procédure de signalement des maladies implique de transmettre l'identité et l'adresse du patient afin d'instaurer, en urgence, des mesures de prévention individuelle et collective et, le cas échéant, de déclencher des investigations pour identifier l'origine de la contamination ou de l'exposition¹⁹⁵¹. A cet effet, les informations nominatives « peuvent être transmises à d'autres professionnels lorsque leur intervention est indispensable pour la mise en œuvre des mesures de prévention »¹⁹⁵² et « ne sont conservées que le temps nécessaire à l'investigation et à l'intervention »¹⁹⁵³. Les deux procédures poursuivent des finalités différentes en fonction de la gravité et de la transmissibilité de la maladie diagnostiquée. Alors que l'une permet de suivre l'évolution des maladies au sein d'une population¹⁹⁵⁴, l'autre déclenche des mesures d'investigation et d'intervention auprès des personnes contaminées ou risquant de l'être¹⁹⁵⁵. Quelle que soit la procédure adéquatement mise en œuvre, « toute personne appelée à connaître, à quelque titre que ce soit, les données individuelles transmises [...] est astreinte au secret professionnel sous les peines prévues à l'article 226-13 du code pénal »¹⁹⁵⁶. Lorsque Bruno Py s'insurge que « le

¹⁹⁴⁸ Ou en dehors du régime temporaire de l'état d'urgence sanitaire.

¹⁹⁴⁹ Article L.3113-1 I. 1° du code de la santé publique.

¹⁹⁵⁰ Article R.3113-2 du code de la santé publique.

¹⁹⁵¹ Article R.3113-4 du code de la santé publique.

¹⁹⁵² *Ibid.*

¹⁹⁵³ *Ibid.*

¹⁹⁵⁴ La procédure de notification.

¹⁹⁵⁵ La procédure de signalement.

¹⁹⁵⁶ Article R.3113-5 du code de la santé publique.

secret est et reste plus fort que le Sida »¹⁹⁵⁷ alors qu'il n'en est pas autant de la Covid-19, c'est parce que le VIH est inscrit sur « *la liste des maladies qui relèvent de la procédure de notification* »¹⁹⁵⁸ anonyme. Si la contamination d'une personne par le VIH ne requiert pas d'intervention urgente auprès de l'ensemble de la population, la contamination d'une personne par le SARS-CoV-2 commande la mise en place d'actions supplémentaires à la surveillance épidémiologique.

Le partage des données médicales nominatives à des fins de lutte contre la propagation d'une maladie infectieuse au moyen de la procédure de signalement, et sans le consentement du patient, préexistait donc à la création des systèmes d'information SI-DEP et Contact Covid. Force est d'observer que « *l'obligation de transmission des informations n'est donc pas une dérogation nouvelle au secret médical, mais l'extension d'une pratique existante à une nouvelle maladie : la covid-19* »¹⁹⁵⁹. D'ailleurs, les dispositions législatives relatives à la création de ces deux dispositifs précisent que « *les données individuelles relatives à la covid-19 font l'objet d'une transmission obligatoire à l'autorité sanitaire prévue à l'article L. 3113-1 du code de la santé publique [...] au moyen des systèmes d'information mentionnés au présent article* »¹⁹⁶⁰. Alors, pourquoi ne pas avoir simplement étendu la liste des maladies qui relèvent de la procédure de signalement¹⁹⁶¹ au SARS-CoV-2 ? Compte tenu des circonstances sanitaires exceptionnelles, du nombre de personnes diagnostiquées – et donc fichées –, et de l'indispensable adaptation du système de santé, il convenait de créer des systèmes d'information spécifiques, centralisés et accommodés aux traitements massifs de données sensibles dans le respect du droit à la protection des données personnelles. Pendant l'application du régime de l'état d'urgence sanitaire, la transmission obligatoire des données individuelles relatives à la Covid-19 se fait donc *via* des systèmes d'informations spécialement et temporairement créés à cet effet. Cela suppose qu'en dehors de toute urgence sanitaire, le SARS-CoV-2 pourrait certainement rejoindre la liste des maladies à signalement ou à notification obligatoire en fonction de sa gravité et de sa contagiosité. Au demeurant, « *l'article L. 3131-9-1 du CSP prévoit également certaines modalités de collecte de données*

¹⁹⁵⁷ PY (B.), *Les épidémies et le secret professionnel*, *loc. cit.*

¹⁹⁵⁸ Article D.3113-7 du code de la santé publique.

¹⁹⁵⁹ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 38

¹⁹⁶⁰ Article 11 VI de la loi n°2020-546 du 11 mai 2020, *loc. cit.*

¹⁹⁶¹ Article D.3113-6 du code de la santé publique.

à caractère personnel de santé, notamment dans le cadre du dispositif d'organisation de la réponse du système de santé en cas de situation sanitaire exceptionnelle (ORSAN), dispositif déclenché le 23 février 2020 pour faire face à l'épidémie de Covid-19 »¹⁹⁶².

In fine, le partage des informations médicales liées à certaines maladies transmissibles entre les professionnels dépositaires d'un même secret constitue un impératif technique répondant à une finalité limitée et spécifique à la protection de la santé publique.

558. Tandis que le partage des données médicales nominatives relatives à la Covid-19 entre les professionnels légalement autorisés à en connaître ne constitue pas une violation du secret professionnel¹⁹⁶³, la révélation de telles informations à des tiers non autorisés doit être considérée comme une atteinte à ce secret¹⁹⁶⁴. Au demeurant, le pouvoir exécutif a autorisé la révélation de l'identité de la personne diagnostiquée positive au SARS-CoV-2, par les agents chargés des enquêtes sanitaires soumis au secret professionnel, à des tiers exempts de ce secret. En effet, cette révélation peut être consentie, par le patient zéro, à chaque personne à risque de contamination, ainsi qu'aux responsables des structures ou lieux d'hébergement collectifs, des structures d'accueil du jeune enfant, des structures en milieu scolaire et universitaire, des établissements de santé, de lieux de travail et des établissements recevant du public dans lesquels les mesures barrières ne peuvent être pleinement respectées tels que les lieux de restauration collective dans un cadre professionnel, restaurants, bars ou salles de sport que la personne infectée aurait fréquentés, et aux responsables des rassemblements, événements ou activités impliquant plus de six personnes auxquels la personne infectée aurait participé¹⁹⁶⁵. Manifestement, le dispositif Contact Covid concède une large divulgation d'informations médicales couvertes par le secret professionnel à des personnes physiques non habilitées à les recevoir. Pourtant, le consentement de la personne concernée à la révélation des informations à caractère secret ne saurait délier le professionnel du secret dont

¹⁹⁶² LANNA (M.), *Crise sanitaire - Les données personnelles de santé, nouvelle composante de la prévention sanitaire ?*, Droit Administratif, 2020, n° 6, étude 7, § 19 à § 20.

¹⁹⁶³ Article 226-14 alinéa 1 du code pénal.

¹⁹⁶⁴ Article 226-13 du code pénal.

¹⁹⁶⁵ Article 2 II 1° o) du décret n° 2020-551 du 12 mai 2020.

il est légalement investi¹⁹⁶⁶. De façon absolue, le secret professionnel est opposable aux individus qui n'en sont pas dépositaires.

Cette disposition *contra legem* apparaît surprenante dans la mesure où seule l'information relative à un risque de contamination est suffisante pour orienter les personnes susceptibles d'être infectées vers la réalisation d'un examen de dépistage et des prescriptions médicales d'isolement prophylactiques¹⁹⁶⁷. De la même façon, les responsables d'établissements recevant du public et de rassemblements, d'évènements ou d'activités réunissant concomitamment plus de six personnes n'ont pas à connaître l'identité de la personne infectée. L'unique information selon laquelle une personne contaminée a fréquenté un lieu public sur une plage horaire donnée, ou a participé à un événement particulier suffit à considérer que les individus ayant fréquenté ce même lieu sur la même plage horaire, ou ayant participé à ce même événement sont à risque de contamination. Le cas échéant, le responsable du lieu ou de l'évènement devrait simplement communiquer la liste des personnes identifiées comme à risque de contamination, suite à leur recensement au moyen des cahiers de rappel¹⁹⁶⁸, aux brigades sanitaires chargées du *contact tracing*. En plus d'être contraire à l'obligation de secret professionnel, la révélation de l'identité de la personne infectée est contraire à l'obligation de minimisation des données personnelles collectées. Assurément, cette communication n'apparaît pas nécessaire à la finalité du traitement, à savoir l'information relative à un risque d'infection visant à rompre la chaîne des contaminations. A l'inverse, rien n'empêche le patient de divulguer ses propres données médicales et d'informer les personnes avec lesquelles il a été en contact de son infection au SARS-CoV-2¹⁹⁶⁹.

559. A l'opposé, la lutte contre les chaînes de contamination au SARS-CoV-2 au moyen de l'application TousAntiCovid ne pose aucune difficulté relative à la divulgation des

¹⁹⁶⁶ Crim., 8 avril 1998, n° 97-83.656, Bull. crim., n° 138 ; D., 1999, n° 43, p. 381, obs. J. Penneau ; Dr. pén., 1998, comm. 113, M. Véron..

¹⁹⁶⁷ Voir : Article 1 III 3° du décret n°2020-551 du 12 mai 2020.

¹⁹⁶⁸ Voir : CNIL, *COVID-19 : les recommandations de la CNIL pour les cahiers de rappel papier*, 08 juin 2021 ; CNIL, *La CNIL revient sur la nouvelle fonctionnalité TousAntiCovid Signal*, 08 juin 2021.

¹⁹⁶⁹ Crim., 18 novembre 1986, n° 85-93.308, Bull. crim., n° 345 ; Gaz. Pal., 1987, 167, note J.-P. Doucet et Le Fauc.

informations médicales de la personne fichée¹⁹⁷⁰. En effet, l'alerte numérique des personnes à risque de contamination préserve l'anonymat de la personne infectée avec laquelle elles ont été à proximité ou ont partagé un même lieu sur une plage horaire similaire. Cet outil numérique présente l'avantage de « *pouvoir alerter les personnes que l'on ne connaît pas* »¹⁹⁷¹ tout en respectant la confidentialité de l'identité des citoyens contaminés par le virus et de leurs informations médicales. En effet, les « *personnes identifiées comme contacts à risque de contamination reçoivent alors, par l'intermédiaire de l'application, la seule information selon laquelle elles ont été à proximité, au cours d'une période donnée [...] d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du covid-19* »¹⁹⁷². Toutefois, il peut exister une possibilité limitée d'identification indirecte des personnes contaminées. En effet, cette éventualité se manifeste lorsqu'au cours de cette période de contagiosité les personnes à risque de contamination ont eu un très faible nombre de contacts ou ont fréquenté des lieux où se trouvait, au même moment, un faible nombre de personnes¹⁹⁷³.

560. Au contraire, le Passe sanitaire et le Passe vaccinal, qui permettent aux personnes présentant un faible risque de développer ou de transmettre le virus de la Covid-19 de voyager à l'étranger, de se rendre sur le territoire français et d'accéder à certains lieux, établissements ou événements impliquant un grand rassemblement de personnes, peuvent révéler les informations médicales connexes au SARS-CoV-2 de la personne concernée. En effet, les acteurs chargés de contrôler le Passe sanitaire – auquel est intégré le *Certificat numérique européen* – lors de déplacements à destination ou en provenance de l'étranger sont amenés à lire « *les noms, prénoms et date de naissance de la personne concernée par le justificatif, ainsi que les informations relatives à l'examen de dépistage ou au vaccin réalisé* »¹⁹⁷⁴. En revanche, les personnes habilitées à contrôler l'accès aux lieux, établissements ou événements subordonnés à la présentation d'un Passe vaccinal pour les personnes âgées de

¹⁹⁷⁰ Voir : DESGENS-PASANAU (G.), *Traçage des données mobiles : ne sacrifions pas la protection de nos données sur l'autel de la crise sanitaire*, In *Le droit face au coronavirus, Comment une pandémie inédite à mis à l'épreuve notre système juridique*, LexisNexis, 2021, p. 439 à p. 441.

¹⁹⁷¹ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 22.

¹⁹⁷² Article 2 6° du décret n°2020-650 du 29 mai 2020 relatif au traitement de données dénommé « TousAntiCovid », *JOFR* n°131, 30 mai 2020.

¹⁹⁷³ Article 2 6° du décret n°2020-650 du 29 mai 2020 *loc. cit.*

¹⁹⁷⁴ Article 2-3 III du décret n° 2021-699 du 1^{er} juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire, *JOFR* n°126, 2 juin 2021, texte n°16.

plus de seize ans et d'un Passe sanitaire pour les personnes âgées de douze à quinze ans ne prennent connaissance que des « *noms, prénoms et date de naissance de la personne concernée par le justificatif, ainsi qu'un résultat positif ou négatif de détention d'un justificatif conforme* »¹⁹⁷⁵. Quel que soit le dispositif de lecture de ces justificatifs de vaccination, de dépistage négatif ou de rétablissement et la finalité de leur présentation, les données qu'ils contiennent ne peuvent être lues qu'à l'instant du contrôle et conservées au-delà de ce contrôle¹⁹⁷⁶. Si les applications numériques ont été fortement décriées, elles s'avèrent plus protectrices de la confidentialité des données médicales des personnes fichées que le dispositif Contact Covid au moyen duquel est effectué le *contact tracing* manuel.

Plus largement, l'ensemble des systèmes d'information élaborés dans le cadre de la gestion de la crise sanitaire doivent garantir la confidentialité logique, technique et organisationnelle des données médicales partagées à cette fin. Bien que l'objectif d'intérêt général de protection de la santé publique permet de restreindre le droit à la vie privée et à la protection des données des personnes fichées, la confidentialité des données à caractère personnel traitées doit être préservée.

B) La préservation de la confidentialité des données médicales divulguées

561. Le contrôleur qui a inféré des informations immunologiques ou virologiques lors de la vérification du Passe sanitaire ou du Passe vaccinal doit en préserver le secret quand bien même le législateur ne l'y aurait pas astreint. Aussi, le professionnel dépositaire des informations médicales des personnes fichées, en l'absence de confession volontaire, doit singulièrement veiller à la confidentialité de ces données à caractère secret. Les sages de la rue Montpensier ont en effet jugé que « *le partage de données médicales à caractère personnel [nominatives ou pseudonymisées], sans le consentement de l'intéressé, n'est pas nécessairement contraire au droit au respect de la vie privée : tout dépend des modalités de ce partage, des finalités poursuivies et des garanties prévues* »¹⁹⁷⁷. Outre la probité de la personne physique à qui ces informations sensibles ont été révélées, l'architecture des

¹⁹⁷⁵ *Ibid.*

¹⁹⁷⁶ *Ibid.*

¹⁹⁷⁷ Cons. Const., Commentaire de la décision n° 2020-800 DC du 11 mai 2020 relative à la loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, p. 18.

systèmes d'information de lutte contre une menace sanitaire doit être conçue de façon à garantir, par défaut, la confidentialité et la protection des données personnelles traitées. A cet effet, ces dispositifs autorisés par le législateur, et mis en œuvre selon des modalités fixées par décret, doivent introduire des garanties appropriées dès la conception du traitement et, de manière dynamique, jusqu'à son terme. Assurément, le RGPD impose à toute entité traitant des données personnelles une obligation de sécurité, d'intégrité et de confidentialité¹⁹⁷⁸ dont il doit pouvoir justifier à tout moment¹⁹⁷⁹. Force est de constater qu'une « *règle d'action s'impose donc aux opérateurs concernés. Ils doivent intégrer à leur fonctionnement [...] les mesures visant à prévenir les cyber-risques. Il ne s'agit pas seulement pour eux de respecter des exigences en matière de cybersécurité mais d'en être les acteurs.* »¹⁹⁸⁰. Il appartient donc au responsable de traitement et à ses sous-traitants de mettre en œuvre des mesures appropriées afin de garantir un niveau de sécurité adapté au risque inhérent au traitement¹⁹⁸¹. Il en ressort que la sécurité du traitement et la confidentialité des données personnelles sont une priorité tant juridique que technique. Certainement, « *les architectures techniques sont intrinsèquement juridiques : leur modèle conditionne la mise en œuvre du droit. Il est donc indispensable qu'elles répondent, en retour, à des exigences juridiques fortes, intégrées by design* »¹⁹⁸². L'objet de cet examen ne consiste pas à détailler chaque mesure de sécurité des données médicales traitées par chacun des systèmes d'information instaurés en appui de la crise sanitaire, mais à balayer quelques-unes des garanties de confidentialité apportées par leur responsable respectif.

562. D'abord, les mesures de protection des données médicales traitées à des fins de protection de la santé publique reposent sur la limitation de leurs destinataires, *a fortiori* lorsque les dispositifs sont envisagés au niveau national, et qu'ils impliquent un nombre d'acteurs considérable pour accomplir « *la masse des démarches à entreprendre pour organiser la collecte des informations nécessaires à la lutte contre le développement de*

¹⁹⁷⁸ Article 5.1 f) du RGPD.

¹⁹⁷⁹ Article 5.2 du RGPD.

¹⁹⁸⁰ DOUVILLE (T.), *L'émergence des cyber-risques*, Archives de philosophie du droit, Vol. 62, 2020, n°01, p. 295.

¹⁹⁸¹ Article 32.1 du RGPD.

¹⁹⁸² LEQUESNE ROTH (C.), *Covid-19 et applications de traçage : à la croisée des libertés et des technologies*, Recueil Dalloz, 2020, p.1096.

l'épidémie »¹⁹⁸³. Bien que les données médicales des citoyens soient rendues accessibles à une quantité astronomique de personnes, chaque catégorie de destinataires doit être précisément et exhaustivement énumérée pour chacun des systèmes d'information ainsi que pour chacune de leurs opérations de traitement correspondant à une finalité déterminée. Pendant que le législateur a identifié, pour chaque dispositif, les catégories de professionnels autorisées ou habilitées à accéder aux données sensibles de la personne fichée, les décrets en Conseil d'Etat sont venus distinctement préciser les modalités de désignation des différents destinataires propre à chaque organisme auquel ils sont rattachés. L'identification nominative des professionnels accédant aux données médicales du citoyen, dans le cadre d'un partage d'information par l'utilisation de Contact Covid ou d'une révélation consentie lors de la présentation du Passe sanitaire et du Passe vaccinal, contribue directement à la confidentialité des données personnelles. En ce sens, le Conseil constitutionnel rassure que « *la confidentialité est ce qui assure que n'auront pas accès aux données à caractère personnel d'autres personnes que celles expressément citées dans la loi, qui sont les seules pour lesquelles le Conseil a pu s'assurer du caractère justifié, adéquat et proportionné de leur accès* »¹⁹⁸⁴. C'est ainsi que le mécanisme d'identification permet de vérifier que le destinataire des informations intimes était dument habilité à en connaître. A défaut, des sanctions pénales pourraient être prononcées¹⁹⁸⁵. Afin de s'en assurer, toute opération effectuée sur les données médicales contenues dans les fichiers SI-DEP et Contact Covid doit être enregistrée et tracée. Les mesures de traçabilité permettent, d'une part, « *d'assurer aux personnes concernées un très haut niveau de transparence* »¹⁹⁸⁶ et, d'autre part, « *d'imputer de façon fiable toute opération réalisée par les personnes habilitées* »¹⁹⁸⁷.

A titre d'exemple, le décret n° 2021-699 du 1^{er} juin 2021 prescrivant les mesures du Passe sanitaire et du Passe vaccinal, dans sa version en vigueur au 24 janvier 2022, précise

¹⁹⁸³ Cons. Const., Décision n°2020-800 DC, 11 mai 2020, cons. 69 : Gaz. Pal., 2016, n° 20, p. 16, note J. Gicquel ; AJDA, 2020, n° 22, p. 1242, note M. Verpeaux ; LDFP, 2020, n° 06, p. 01, obs. D. Larralde ; D., 2020, n° 22, p. 1262, obs. W. Maxwell et C. Zolynski.

¹⁹⁸⁴ Cons. Const., Commentaire de la décision n° 2020-800 DC du 11 mai 2020 relative à la loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions, p. 22.

¹⁹⁸⁵ Cf. Paragraphe 566.

¹⁹⁸⁶ CNIL, Délibération n°2020-051 du 8 mai 2020 portant avis sur un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire, JOFR n°117, 13 mai 2020, texte n°74, p. 11.

¹⁹⁸⁷ CNIL, Délibération n°2020-051 du 8 mai 2020, *op. cit.*, p. 12.

que seuls sont autorisés à contrôler ces justificatifs¹⁹⁸⁸ « *dans la limite de ce qui est nécessaire au contrôle des déplacements et de l'accès aux lieux, établissements, services ou évènements* »¹⁹⁸⁹ : les exploitants de services de transport de voyageurs, les personnes chargées du contrôle sanitaire aux frontières et les responsables des lieux, établissements et services ou les organisateurs des évènements dont l'accès est subordonné à leur présentation¹⁹⁹⁰. Ces catégories de destinataires doivent ensuite habilitier « *nommément les personnes et services autorisés à contrôler les justificatifs pour leur compte* »¹⁹⁹¹ au moyen d'un dispositif numérique de lecture conforme aux conditions fixées par arrêté¹⁹⁹². A ce titre, « *elles tiennent un registre détaillant les personnes et services ainsi habilités et la date de leur habilitation, ainsi que les jours et horaires des contrôles effectués par ces personnes et services* »¹⁹⁹³.

563. Si l'identification des contrôleurs en charge de la vérification du Passe sanitaire et du Passe vaccinal apparaît aisément réalisable, l'identification des professionnels accédant aux données médicales des personnes fichées au moyen des systèmes SI-DEP et Contact Covid doit être accompagnée d'une authentification forte. En effet, ces outils ont pour particularité de centraliser et de partager l'ensemble des données médicales des personnes infectées et de celles à risque de contamination. Malgré un large partage des données médicales des citoyens, chaque destinataire – dépositaire du secret professionnel – doit pouvoir justifier qu'il est personnellement légitime à accéder à ces deux systèmes. En effet, « *l'architecture de ces applications étant centralisée, les seuls mécanismes pouvant être mis en œuvre pour limiter les accès consistent en des systèmes d'authentification des accédants, afin que seules les personnes autorisées puissent effectivement consulter les données de la base* »¹⁹⁹⁴. En quelque sorte, l'autorisation légale de l'extension du secret professionnel médical doit techniquement se traduire par un processus d'authentification approprié à la sensibilité des

¹⁹⁸⁸ Outre les agents de contrôle habilités à constater les infractions prévues à l'article L.3136-1 du code de la santé publique.

¹⁹⁸⁹ Article 2-3 II du décret n° 2021-699 du 1^{er} juin 2021, *loc. cit.*

¹⁹⁹⁰ *Ibid.*

¹⁹⁹¹ *Ibid.*

¹⁹⁹² Arrêté du 24 août 2021 pris en application du III de l'article 2-3 du décret n° 2021-699 du 1^{er} juin 2021 prescrivant les mesures générales nécessaires à la gestion de sortie de crise sanitaire, *JORF* n°227, 29 septembre 2021, texte n° 27.

¹⁹⁹³ *Ibid.*

¹⁹⁹⁴ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 21.

données. La connexion à ces dispositifs ne devrait donc pouvoir être empruntée que par une identification¹⁹⁹⁵ et une authentification¹⁹⁹⁶ conforme à la Politique Générale de Sécurité des Systèmes d'Information de Santé¹⁹⁹⁷. A tout le moins, le responsable de traitement doit s'assurer « *a minima que la politique de mot de passe prévue sera conforme à sa délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, ainsi qu'à réaliser une surveillance renforcée du traitement afin de détecter toute utilisation anormale dès l'ouverture du service* »¹⁹⁹⁸.

564. Après que les destinataires limitativement habilités à accéder aux données médicales des citoyens fichés aient été rigoureusement identifiés, les mesures de protection des systèmes d'information doivent ensuite reposer sur la limitation des données accessibles¹⁹⁹⁹. Malgré la grande variété de données collectées par les différents dispositifs numériques, chaque destinataire ne doit pouvoir accéder qu'aux seules informations sensibles strictement nécessaires à l'accomplissement de la mission dont il est effectivement investi. Immanquablement, les données médicales des citoyens fichés ne peuvent être utilisées que pour les strictes nécessités afférentes à la lutte contre la pandémie de la Covid-19. Par conséquent, les décrets instaurant les systèmes d'information déployés face à ce virus doivent exhaustivement énumérer les destinataires chargés de chaque opération de traitement d'une part, ainsi que les seules données nécessaires à chaque opération de traitement d'autre part. En ce sens, la CNIL insiste sur la « *nécessité de justifier, pour chaque catégorie de données dont le traitement est envisagé, du besoin d'en connaître de chaque catégorie de destinataires* »²⁰⁰⁰.

En pratique, ces mesures juridiques de confidentialité devraient être transcrites par des matrices d'habilitation corollaires au processus d'authentification. Certainement, les accès doivent être différemment limités et la granularité des données médicales accessibles

¹⁹⁹⁵ ASIP Santé, DSSIS, *Référentiel d'identification des acteurs sanitaires et médico-sociaux*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), V 1.0, décembre 2014.

¹⁹⁹⁶ ASIP Santé, DSSIS, *Référentiel d'authentification des acteurs de santé*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), V 2.0, décembre 2014.

¹⁹⁹⁷ Construite par la Délégation ministérielle au numérique en santé et l'Agence du numérique en santé.

¹⁹⁹⁸ CNIL, Délibération n°2020-051 du 8 mai 2020, *op. cit.*, p. 11 à p. 12

¹⁹⁹⁹ Article 5.1 c) du RGPD.

²⁰⁰⁰ CNIL, Délibération n°2020-051 du 8 mai 2020, *op. cit.*, p. 15.

doit être paramétrée en fonction des besoins de chaque destinataire. A titre d'illustration, le dispositif de lecture du Passe sanitaire et du Passe vaccinal permet de réduire les données accessibles en fonction de la finalité du contrôle. Dans le cadre d'une inspection sanitaire aux frontières, le contrôleur habilité par son organisme à vérifier le *Certificat numérique européen* peut accéder à l'identité de son détenteur ainsi qu'« *aux informations relatives à l'examen de dépistage ou au vaccin réalisé* »²⁰⁰¹ selon les exigences du pays de destination. Cependant, lorsque la vérification du Passe sanitaire ou du Passe vaccinal est préalable à l'accès à un lieu, à un service ou à un évènement, les personnes habilitées à effectuer ce contrôle ne peuvent accéder qu'à l'identité de la personne fichée ainsi qu'au résultat de conformité de son justificatif « *sans qu'apparaisse la catégorie de preuve mobilisée* »²⁰⁰². La matrice d'habilitation du dispositif numérique de lecture de ces Passes permet de déverrouiller l'accès à des données dont la granularité est minimisée selon la finalité du contrôle. La CNIL considère qu'un tel paramétrage contribue à réduire considérablement « *les données accessibles aux personnes habilitées à vérifier le statut des personnes concernées* »²⁰⁰³.

565. Par ailleurs, les mesures de sécurité et de confidentialité des données médicales incluent, autant que possible, leur pseudonymisation et leur cryptage. S'agissant de la pseudonymisation, l'application TousAntiCovid fonctionne grâce à la technologie *Bluetooth*. L'activation de cette fonctionnalité permet d'enregistrer les pseudo-identifiants des ordiphones se trouvant à proximité pendant un laps de temps et une distance donnés. Lorsqu'un utilisateur de ce dispositif se déclare volontairement positif à la Covid-19, l'historique des pseudo-identifiants enregistrés dans son ordiphone sont envoyés vers un serveur central. A cet instant, les utilisateurs dont le crypto-identifiant est disponible sur ce serveur reçoivent une notification leur indiquant qu'ils présentent un risque de contamination²⁰⁰⁴. Tout en favorisant le *contact tracing*, « *le gouvernement français garantit qu'il est impossible d'identifier les utilisateurs de l'application, ni même le lieu et le moment*

²⁰⁰¹ CNIL, *COVID-19 : questions-réponses sur le passe sanitaire et l'obligation vaccinale*, 29 septembre 2021.

²⁰⁰² CNIL, Délibération n° 2021-054 du 12 mai 2021 portant avis sur le projet de mise en place d'un passe sanitaire conditionnant l'accès à certains lieux, évènements ou établissements impliquant de grands rassemblements de personnes, cons. 35.

²⁰⁰³ CNIL, Délibération n° 2021-054 du 12 mai 2021, *op. cit.*, cons. 36.

²⁰⁰⁴ Pour plus d'informations sur ce fonctionnement, voir le site [faq.tousanticovid.gouv.fr].

où ils ont croisé un autre appareil ayant activé l'application »²⁰⁰⁵. S'agissant du cryptage, le Passe sanitaire et le Passe vaccinal, contenant des données immunologiques ou virologiques, se présentent sous la forme d'un code-barres à deux dimensions. Les informations personnelles renfermées dans ces dispositifs sont lisibles numériquement grâce un dispositif de lecture ne donnant accès qu'à celles nécessaires à la finalité pour laquelle la présentation de tels justificatifs est requise²⁰⁰⁶. Les données médicales qu'ils renferment ne sont révélées que dans l'hypothèse du contrôle des « *personnes âgées d'au moins douze ans souhaitant se déplacer à destination ou en provenance du territoire hexagonal, de la Corse ou de l'une des collectivités* »²⁰⁰⁷ d'outre-mer. Dans les autres cas, seule l'identité de leur titulaire ne sera révélée au contrôleur. Si la pseudonymisation des données médicales colligées dans les fichiers SI-DEP et Contact Covid ne semble pas compatible avec l'identification et le traçage manuels des contacts à risque de contamination, leur chiffrement devrait être garanti. Dans cette hypothèse, la clé de déchiffrement pourrait être associée à l'authentification des professionnels nommément autorisés à partager des informations aussi sensibles.

566. En complément des aspects techniques évoqués, l'efficience de la confidentialité des données médicales peut être assurée grâce à la formation et à la sensibilisation des professionnels habilités à en connaître. C'est pourquoi la CNIL a recommandé que « *chaque organisme dont les agents [...] ou personnels [...] seront autorisés à consulter ou enregistrer des données [dans les systèmes SI-DEP et Contact Covid], devra avoir sensibilisé ceux-ci à leurs obligations : protection des données à caractère personnel, respect du secret professionnel et risques de sanctions pénales encourues en cas de détournement de finalité du traitement* »²⁰⁰⁸. À la suite de la dispensation d'une telle formation, l'autorité de contrôle estime, qu'en complément, « *il serait pertinent qu'un engagement formalisé de respecter ces principes soit obtenu préalablement à l'habilitation* »²⁰⁰⁹. Pareillement, les professionnels appelés à connaître ou à inférer les informations contenues dans les Passes sanitaire et vaccinal des citoyens devraient être sensibilisés « *à leurs obligations en matière de respect de la protection des données à caractère personnel, notamment s'agissant du respect de la*

²⁰⁰⁵ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 29.

²⁰⁰⁶ Cf. Paragraphe 564.

²⁰⁰⁷ Article 1^{er} II-A 1^o de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

²⁰⁰⁸ CNIL, Délibération n°2020-051 du 8 mai 2020, *op. cit.*, p. 7.

²⁰⁰⁹ *Ibid.*

confidentialité des données traitées et de la nécessité de supprimer les éléments transmis à l'issue de l'opération de conversion »²⁰¹⁰. La sensibilisation à la protection des données médicales traitées au moyen des systèmes d'information de lutte contre la propagation de la Covid-19 s'avère primordiale dans la mesure où toute atteinte à leur confidentialité peut faire l'objet d'une sanction pénale. *A fortiori*, ces instructions se révèlent primordiales lorsque le professionnel amené à y accéder n'est ni accoutumé au traitement de données à caractère personnel, ni formé à la notion de secret professionnel.

En premier lieu, toute personne qui, à l'occasion d'un traitement de données à caractère personnel, a recueilli des informations dont la divulgation aurait pour effet de porter atteinte à l'intimité de la vie privée de l'intéressé, puis les a portées, sans son autorisation, à la connaissance d'un tiers n'ayant pas qualité pour les recevoir, encourt une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende²⁰¹¹. Cette sanction est réduite à trois ans d'emprisonnement et 100 000 euros d'amende lorsque la divulgation a été commise par imprudence ou négligence²⁰¹². En cas de méconnaissance de la confidentialité des données sensibles, l'ensemble des professionnels intervenant dans la mise en œuvre des systèmes d'information déployés pour lutter contre la crise sanitaire apparaît potentiellement concerné par cette infraction. En deuxième lieu, le professionnel qui a divulgué une information à caractère secret alors qu'il en était dépositaire et sans qu'il n'y soit exceptionnellement autorisé encourt une peine d'un an d'emprisonnement et de 15 000 euros d'amende²⁰¹³. Cette infraction pénale ne peut spécifiquement être commise que par les catégories de professionnels légalement autorisées à accéder aux données médicales des citoyens fichés dans les systèmes SI-DEP et Contact Covid. En troisième lieu, le législateur a pris l'initiative de créer des infractions temporaires et spécifiques au Passe sanitaire et au Passe vaccinal. Le contrôleur qui conserverait ces justificatifs à l'issue du processus de vérification²⁰¹⁴, ou qui les réutiliserait à d'autres fins, encourt une peine d'un an d'emprisonnement et de 45 000

²⁰¹⁰ CNIL, Délibération n° 2021-097 du 6 août 2021 portant avis sur un projet de décret modifiant le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire et le décret n° 2021-901 du 6 juillet 2021 relatif au traitement automatisé de données à caractère personnel dénommé « Convertisseur de certificats », *JORF* n°183, 8 août 2021, texte n° 93.

²⁰¹¹ Article 226-22 alinéa 1 du code pénal.

²⁰¹² Article 226-22 alinéa 2 du code pénal.

²⁰¹³ Article 226-13 du code pénal.

²⁰¹⁴ Excepté le cas où l'employeur conserverait le justificatif de statut vaccinal de son employé jusqu'à la fin de l'état d'urgence sanitaire (Article 1 II E alinéa 2 de la loi n°2021-689 du 31 mai 2021).

euros d'amende²⁰¹⁵. Est puni de la même peine celui qui exigerait la présentation de ces Passes pour accéder à des lieux, établissements, services ou évènements autres que ceux auxquels le législateur subordonne la vérification de ces justificatifs²⁰¹⁶.

567. Finalement, chacune des mesures de sécurité et de confidentialité envisagées pour chacun des systèmes d'information instaurés dans la lutte contre le virus de la Covid-19 doit être évaluée à l'occasion d'une analyse d'impact relative à la protection des données (AIPD). Concrètement, il s'agit d'une étude permettant de construire un traitement de données personnelles conforme au RGPD et respectueux de l'intimité de la vie privée des personnes concernées afin de pallier les risques qu'il est susceptible d'engendrer pour leurs droits et libertés. Cette obligation incombe à chacun des responsables de traitements créés dans le contexte pandémique préalablement à leur déploiement effectif. En effet, une analyse d'impact est requise pour tout traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, *a fortiori* lorsqu'il s'agit d'un « *traitement à grande échelle de catégories particulières de données* »²⁰¹⁷. S'il ne fait aucun doute que les systèmes d'information conçus en appui de la lutte contre la menace sanitaire répondent à ces critères, l'article 67 de la loi Informatique et Libertés modifiée précise que l'AIPD est toujours exigée pour les traitements « *ayant pour seule finalité de répondre, en cas de situation d'urgence, à une alerte sanitaire et d'en gérer les suites* ».

Afin d'identifier les dangers du traitement pour la vie privée des personnes concernées, l'AIPD doit notamment contenir « *une évaluation des risques pour les droits et libertés des personnes concernées* »²⁰¹⁸ accompagnée des mesures envisagées pour y faire face. Cette étude juridique et technique vise essentiellement à déterminer la nécessité et la proportionnalité du traitement eu égard aux droits fondamentaux reconnus par le droit de l'Union et des Etats membres²⁰¹⁹. Dans l'hypothèse où les mesures apportées par le responsable de traitement ne suffisent pas à atténuer la gravité du risque, l'autorité de contrôle

²⁰¹⁵ Article 1 II E al. 3 de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

²⁰¹⁶ Article 1 II F al. 2 de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

²⁰¹⁷ Article 35.3 b) du RGPD.

²⁰¹⁸ Article 35.7 b) du RGPD.

²⁰¹⁹ Cf. Paragraphe 334.

doit être consultée avant que la mise en œuvre du traitement n'ait lieu²⁰²⁰. Si la CNIL a été effectivement consultée avant la mise en œuvre de chaque traitement instauré à des fins de lutte contre la pandémie de la Covid-19, ce n'est pas en raison des résultats de l'analyse d'impact. En effet, chacune des consultations préalables de l'autorité nationale de contrôle était imposée par le législateur²⁰²¹, ou faisait suite à une saisine pour avis adressée par les pouvoirs publics²⁰²². Indépendamment des leurs résultats, la CNIL a donc pu évaluer les AIPD afférentes à ces traitements et s'assurer que les risques pour les droits et libertés des citoyens se situaient à un niveau acceptable. Il en résulte que l'AIPD constitue les prémices de l'évaluation de la proportionnalité entre les finalités du traitement et leur impact sur les droits fondamentaux des personnes concernées²⁰²³. Effectivement, « *nombre des facteurs pertinents pour effectuer l'AIPD sont également pertinents dans le cadre de l'évaluation du coût d'une mesure législative en matière de vie privée* »²⁰²⁴.

568. Il ressort de ce qui précède que les responsables des différents traitements créés pour faire face à la pandémie du SARS-CoV-2²⁰²⁵ doivent scrupuleusement respecter les principes de protection des données personnelles, par défaut, dès leur conception. A cet égard, il leur appartient d'employer des mesures techniques et organisationnelles de nature à garantir un niveau de sécurité adéquat aux caractéristiques du traitement. A défaut, les responsables de traitement encourent une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende. Au surplus d'une condamnation pénale, la CNIL est en mesure de prononcer des sanctions administratives à l'encontre des responsables de traitement ayant attenté à la confidentialité des données médicales consécutivement à une faille de sécurité informatique non résolue. C'est ainsi que deux médecins ont été condamnés à une amende de plusieurs milliers d'euros pour avoir négligé les principes élémentaires en matière de sécurité informatique (dont le chiffrement des données) ayant permis un libre accès à leurs serveurs informatiques

²⁰²⁰ Considérant 84 du RGPD.

²⁰²¹ Article 11 IX de la loi n°2020-546 du 11 mai 2020, *loc. cit.* ; Article 1 II J de la loi n°2021-689 du 31 mai 2021, *loc. cit.*

²⁰²² Sur le fondement de l'article 8. I. 2° e) de la loi Informatique et Libertés modifiée.

²⁰²³ Cf. Paragraphe 601.

²⁰²⁴ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, note 46.

²⁰²⁵ Le ministre chargé de la santé pour SI-DEP ; La caisse nationale de l'assurance maladie pour Contact Covid ; Le ministre chargé de la santé pour TousAntiCovid ; Le ministre chargé de la santé pour TousAntiCovid Vérif permettant de lire le Passe sanitaire.

d'imageries médicales contenant des clichés nominatifs²⁰²⁶. Il « *ne s'agit donc plus de sanctionner a posteriori ceux qui sont à l'origine d'un incident de sécurité mais de l'anticiper. Cette anticipation s'accompagne d'un déplacement des destinataires des règles de droit. Plutôt que de viser les auteurs des incidents, des obligations sont mises à la charge des opérateurs de réseaux ou de systèmes d'information, des producteurs de dispositifs connectés et des responsables de traitement et des sous-traitants en matière de données à caractère personnel* »²⁰²⁷. Bien qu'« *aucune solution technologique ne permet de garantir une absence totale de risques* »²⁰²⁸, les responsables de traitement ont l'obligation d'agir activement pour minimiser les risques inhérents à tout traitement de données personnelles. Il n'en demeure pas moins que « *si dans l'abstrait, l'encadrement de ces traitements permet de considérer que les ingérences dans les droits et libertés des personnes concernées sont nécessaires et proportionnées à la lutte contre la covid-19, les conditions concrètes de leur mise en œuvre ne sont [jamais] pleinement satisfaisantes* »²⁰²⁹. C'est pourquoi les acteurs d'un traitement de données personnelles ne sont tenus qu'à une obligation de moyen dans les moyens déployés pour prévenir et contrer les cyber-risques et leurs conséquences²⁰³⁰.

Paragraphe 2 : L'exception aux droits et libertés fondamentaux de la personne fichée

569. Les systèmes d'information, élaborés par les pouvoirs publics afin de lutter contre la pandémie de la Covid-19, correspondent à des traitements de données médicales exceptionnels poursuivant un motif d'intérêt public dans le domaine de la santé publique²⁰³¹. Bien que la CNIL ait rappelé que « *des situations telles que l'épidémie actuelle de COVID-19 ne suspendent ni ne restreignent, par principe, la possibilité pour les personnes concernées d'exercer leurs droits sur leurs données à caractère personnel* »²⁰³², cet impératif d'intérêt général justifie néanmoins une limitation des droits qui leurs sont théoriquement

²⁰²⁶ CNIL, Délibération de la formation restreinte n°SAN-2020-014 du 7 décembre 2020 ; CNIL, Délibération de la formation restreinte n°SAN-2020-015 du 7 décembre 2020.

²⁰²⁷ DOUVILLE (T.), *L'émergence des cyber-risques*, *op. cit.*, p. 291.

²⁰²⁸ METALLINOS (N.), *op. cit.*, § 22.

²⁰²⁹ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 40.

²⁰³⁰ DOUVILLE (T.), *L'émergence des cyber-risques*, *op. cit.*, p. 297.

²⁰³¹ D'ailleurs l'ensemble des traitements de ces données sensibles sont exceptionnellement autorisés parce qu'ils poursuivent cette finalité conformément à l'article 9.2 i) du RGPD.

²⁰³² CNIL, Délibération n° 2020-046 du 24 avril 2020, *loc. cit.*

reconnus. Bien que ces traitements exceptionnels aient été autorisés par le pouvoir législatif, le pouvoir exécutif chargé de leur mise en œuvre a alors usé des restrictions concédées à l'article 23 du RGPD. Que la mise en œuvre du traitement présente un caractère obligatoire (A) ou dépende de la volonté des personnes fichées (B), la maîtrise de leurs données médicales se trouve systématiquement diminuée. Il en résulte que les systèmes d'information instaurés pour faire face à la crise sanitaire sont définitivement attentatoires à l'autodétermination informationnelle des citoyens.

A) Le traitement obligatoire des données médicales des citoyens au bénéfice de la lutte contre la crise sanitaire

570. La lutte contre la propagation du SARS-CoV-2 a d'abord requis la création du *système d'information national de dépistage*, dénommé SI-DEP, dans lequel sont centralisés les résultats positifs et négatifs des examens de dépistage virologique et sérologique à ce virus²⁰³³. L'enregistrement, sans délai, des résultats de ces examens par les professionnels habilités à les réaliser constitue une exigence analogue à la transmission obligatoire des données individuelles à l'autorité sanitaire, autrefois désignée par la « communication des maladies à déclaration obligatoire ». En effet, les données individuelles relatives à la Covid-19 font l'objet d'un signalement obligatoire *via* ce système d'information²⁰³⁴. Lorsque les résultats apparaissent positifs, l'identification des personnes infectées permet d'actionner l'intervention des brigades sanitaires afin d'investiguer sur l'origine de l'infection, d'identifier les personnes à risque de contamination et de rompre les chaînes de transmission. Les finalités du dispositif SI-DEP²⁰³⁵ apparaissent exactement similaires aux objectifs de la procédure de signalement obligatoire des données individuelles nominatives à l'autorité sanitaire²⁰³⁶. En outre, l'enregistrement des résultats positifs et négatifs dans le fichier SI-DEP favorise le suivi épidémiologique, après leur pseudonymisation, par l'Agence nationale

²⁰³³ Article 8 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰³⁴ *Cf.* Paragraphe 557.

²⁰³⁵ Telles que décrites à l'article 8 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰³⁶ Tels que définis à l'article R.3113-4 du code de la santé publique.

de santé publique²⁰³⁷. Cette seconde finalité se rapproche de la procédure de notification des données individuelles pseudonymisées auprès de l'autorité publique²⁰³⁸.

Compte tenu du caractère obligatoire du recensement des personnes dépistées et des motifs de santé publique légitimement poursuivis, le premier ministre a décrété l'exclusion, pour les personnes fichées, du droit de s'y opposer²⁰³⁹. En principe, le droit d'opposition est reconnu à la personne concernée dans les seuls cas où le traitement de ses données personnelles est « *fondé sur l'article 6, paragraphe 1, point e) ou f)* »²⁰⁴⁰ du RGPD. Le traitement SI-DEP étant basé sur la mission d'intérêt public incombant au ministre chargé de la santé, un droit d'opposition était, *de jure*, octroyé aux citoyens fichés. La consécration de la limitation de ce droit par la réglementation française était donc inéluctable. Il en résulte que la réalisation d'un test ou d'un examen de dépistage au SARS-CoV-2 emporte indiscutablement le fichage des personnes concernées et la réalisation de diverses opérations de traitement. En effet, après leur enregistrement, ces données médicales peuvent être mises « *à disposition des organismes chargés de déterminer les personnes ayant été en contact avec des personnes infectées, de réaliser des enquêtes sanitaires en présence de cas groupés pour rompre les chaînes de contamination, d'orienter, de suivre et d'accompagner les personnes concernées, et de faciliter le suivi épidémiologique aux niveaux national et local* »²⁰⁴¹ sans que les intéressés ne puissent véritablement y faire obstacle. Dans le cadre du traitement SI-DEP, la capacitation des citoyens fichés est donc réduite à néant²⁰⁴². Toutefois, la restriction apportée au droit des personnes fichées doit apparaître nécessaire à l'accomplissement des finalités du traitement. Compte tenu de l'interdépendance entre les différentes finalités des dispositifs SI-DEP et Contact Covid, et du caractère global du *contact tracing*, l'exercice du droit d'opposition des citoyens aurait pu contrevenir à la lutte contre la propagation du virus de la Covid-19, à laquelle chaque citoyen doit participer. Bien que le motif de santé publique poursuivi soit impérieux, et que chaque membre de la société soit

²⁰³⁷ Article 10 III 1° du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰³⁸ Article R.3113-2 du code de la santé publique.

²⁰³⁹ Article 13 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰⁴⁰ Article 21.1 du RGPD.

²⁰⁴¹ Article 8 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰⁴² Hormis la reconnaissance du droit de s'opposer à ce que les données médicales enregistrées dans le traitement SI-DEP soient intégrées dans le Système national des données de santé à l'article 13 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

concerné par son exécution, la création d'un méga fichier centralisé par l'administration aurait pu engendrer de la méfiance et, conséquemment, des demandes d'opposition à ce fichage²⁰⁴³. Alors, l'efficacité de ces deux dispositifs de datasurveillance supposait l'affirmation de la limitation du droit d'opposition au traitement.

571. Pour le reste, Caroline Zorn craint de voir se dessiner « *un mouvement de défiance d'une partie de la population qui associerait la prise en charge médicale à un fichage dont il ne percevrait pas les bénéfices* »²⁰⁴⁴. Il semble important de rappeler que le droit à la protection des données à caractère personnel a émergé avec le développement de l'informatique dans le secteur public, et que l'adoption de la première loi Informatique et Libertés constitue les suites de l'affaire du *Système automatisé des fichiers administratifs et du répertoire des individus* dénommé « SAFARI »²⁰⁴⁵. Evidemment, dans un contexte pandémique, ce fichage peut entraîner une réduction des libertés individuelles et collectives en complément d'une réduction de l'autodétermination informationnelle des individus. Par exemple, l'analyse épidémiologique des données médicales collectées au moyen de l'outil SI-DEP peut notamment conduire à des mesures administratives de confinement ou de couvre-feu attentatoires aux libertés fondamentales. Mais ces restrictions comportent des bénéfices pour la protection de la santé publique et, subséquemment, pour la préservation de certaines libertés individuelles ou encore pour l'activité économique auxquels profitent chaque citoyen.

572. Néanmoins, la méfiance d'un fichage de masse des personnes positives au SARS-CoV-2 et la crainte de répercussions individuelles sont regrettamment apparues justifiées. En effet, le projet de loi relatif à la gestion de la crise sanitaire, adopté le 25 juillet 2021, proposait un placement en isolement automatique des personnes positives au virus de la Covid-19 pour une durée non renouvelable de dix jours. Concrètement, pour assurer cette évolution, le législateur suggérait d'adapter « *le cadre applicable aux systèmes d'information mis en œuvre pour lutter contre l'épidémie de covid-19, en complétant les finalités et la liste des autorités autorisées à accéder aux données du système dédié au dépistage populationnel*

²⁰⁴³ CEDH, 16 février 2000, n° 27798/95, *aff. Amman c. Suisse* : AJDA, 2000, n° 12, p. 1006, chron. J.-F. Flauss ; RFDA, 2001, n° 06, p. 1250, chron. H. Labayle et F. Sudre : le traitement des données à caractère personnel des individus par une autorité publique constitue *de facto* une limitation du droit au respect de sa vie privée.

²⁰⁴⁴ ZORN (C.), *État d'urgence pour les données de santé (II) : sidep et contact covid*, *loc. cit.*

²⁰⁴⁵ Cf. Paragraphe 12.

(« *SIDEP* »). »²⁰⁴⁶. A cet effet, l'article 7 du projet de loi prévoyait de compléter les finalités du dispositif SI-DEP, détaillées à l'article 11 de la loi n°2020-546 du 11 mai 2020, par l'insertion d'un « 6° ainsi rédigé : « 6° S'agissant des résultats des examens de dépistage virologique ou sérologique concluant à une contamination, des données d'identification et des coordonnées des personnes qui en ont fait l'objet, le suivi et le contrôle du respect des mesures d'isolement mentionnées à l'article 9 de la loi [...] relative à la gestion de la crise sanitaire. » »²⁰⁴⁷. Si le Conseil constitutionnel n'avait pas déclaré l'inconstitutionnalité de ces dispositions, le fichier SI-DEP aurait directement appuyé des décisions individuelles d'enfermement, le contrôle de l'observance de l'enfermement ainsi que la constatation et la sanction du manquement à l'enfermement²⁰⁴⁸. Or, cette finalité aurait relevé du régime spécial applicable aux traitements relevant de la directive européenne relative à la protection des personnes physiques à l'égard du traitement de leurs données personnelles à des fins de prévention et de détection des infractions pénales²⁰⁴⁹. Fort heureusement, les sages de la rue Montpensier ont décidé qu'un isolement applicable de plein droit à toute personne testée positive au SARS-CoV-2 constituait une privation de liberté dont la nécessité, l'adaptation et la proportionnalité n'étaient pas garanties²⁰⁵⁰.

Bien que les juges constitutionnels aient considéré que l'isolement obligatoire des personnes infectées par le virus de la Covid-19 poursuivait l'objectif de valeur constitutionnelle de protection de la santé²⁰⁵¹, il n'empêche que l'extension des finalités du traitement SI-DEP aurait été excessivement démesurée par rapport à l'atteinte caractérisée et extrêmement éloignée des objectifs initiaux de ce traitement²⁰⁵². En effet, le Gouvernement

²⁰⁴⁶ Etude d'impact du projet de loi relatif à la gestion de la crise sanitaire, 19 juillet 2021, p. 5.

²⁰⁴⁷ Projet de loi relatif à la gestion de la crise sanitaire, texte définitivement adopté par l'Assemblée nationale dans les conditions prévues à l'article 45, alinéa 3, de la Constitution, 25 juillet 2021.

²⁰⁴⁸ Article 9 du projet de loi relatif à la gestion de la crise sanitaire, texte définitivement adopté par l'Assemblée nationale dans les conditions prévues à l'article 45, alinéa 3, de la Constitution, 25 juillet 2021.

²⁰⁴⁹ 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JOUE* L 119/89, 4 mai 2016.

²⁰⁵⁰ Cons. Const., Décision n° 2021-824 DC du 5 août 2021, cons. 117 : D., 2021, n° 29, p. 1548 ; AJDA 2021, n° 44, p. 2610, note M. Verpeaux ; AJ fam., 2021, n° 09, p. 448, obs. A. Dionisi-Peyrusse.

²⁰⁵¹ Cons. Const., Décision n° 2021-824 DC du 5 août 2021, cons. 114.

²⁰⁵² Voir : DOUNOT (C.), *La démesure du « pass sanitaire »*, Recueil Dalloz, 2021 p. 1387.

présentait originairement le traitement SI-DEP comme « *l'outil pivot qui permet de suivre au niveau national les examens biologiques concernant la COVID-19, rendant ainsi possible le contact tracing, le suivi épidémiologique et ouvrant une réelle opportunité de mieux comprendre le virus grâce à la recherche qui pourra être faite sur ces données* »²⁰⁵³. De surcroît, l'addition d'une telle finalité aurait été contraire au principe de limitation des finalités²⁰⁵⁴, lequel permet d'éviter que les données personnelles ne fassent l'objet d'une utilisation qui n'aurait pas été initialement prévue par le responsable de traitement, et qui n'aurait pas été portée à la connaissance de la personne concernée lors du recueil de ses données personnelles. En d'autres termes, le « *principe de finalité limite la manière dont le responsable de traitement peut utiliser ou réutiliser ces données dans le futur* »²⁰⁵⁵ et tout manquement est sanctionné pénalement²⁰⁵⁶.

En outre, cette modification substantielle du traitement SI-DEP n'aurait pu être observée comme une finalité compatible avec les finalités initialement déterminées. Eu égard aux cinq critères de compatibilité des finalités²⁰⁵⁷, le responsable de traitement est notamment tenu de prendre en compte le « *contexte dans lequel les données à caractère personnel ont été collectées* »²⁰⁵⁸, « *les attentes raisonnables des personnes concernées* »²⁰⁵⁹, « *la nature des données à caractère personnel* »²⁰⁶⁰ réutilisées, « *les conséquences pour les personnes concernées du traitement ultérieur* »²⁰⁶¹ ainsi que « *l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur* »²⁰⁶². En l'espèce, les citoyens se prêtant à un examen de dépistage au virus de la Covid-19 n'auraient raisonnablement pu s'attendre à ce que cet acte médical de prévention et de diagnostic puisse immédiatement conduire à une privation de liberté arbitraire sous peine de sanction pénale,

²⁰⁵³ Rapport du Gouvernement transmis au Parlement le 9 septembre 2020 concernant les systèmes d'information SI-DEP et Contact Covid, p. 12.

²⁰⁵⁴ Article 5.1 b) du RGPD.

²⁰⁵⁵ CNIL, Définition du principe de « finalité d'un traitement ». Disponible en ligne sur le site [www.cnil.fr]. Consulté le 27 octobre 2021.

²⁰⁵⁶ Article 226-21 du code pénal.

²⁰⁵⁷ Cf. Paragraphe 476.

²⁰⁵⁸ Considérant 50 du RGPD.

²⁰⁵⁹ *Ibid.*

²⁰⁶⁰ *Ibid.*

²⁰⁶¹ *Ibid.*

²⁰⁶² *Ibid.*

sans qu'aucune des exigences de l'article 66 de la Constitution²⁰⁶³ ne soient garanties. Il en advient que la nouvelle finalité proposée par le législateur était, par-delà son inconstitutionnalité, incompatible avec le traitement SI-DEP. L'adjonction totalitaire de finalités ultérieures incompatibles avec celles dont les personnes concernées ont été loyalement informées conduirait à la défiance des citoyens envers les pouvoirs publics d'une part, et les traitements de données personnelles mis en œuvre par l'administration d'autre part. Or, comment gagner la confiance de la société lorsque l'on découvre que les principes essentiels du RGPD sont aisément détournés par le législateur national ? Pourtant, « *l'application de la législation en matière de protection des données personnelles a [théoriquement] un rôle structurant pour garantir le respect des droits et libertés fondamentaux et prévenir le risque de mésusage* »²⁰⁶⁴. La préservation de la confiance de la société en ces systèmes d'information exige que les pouvoirs publics respectent rigoureusement ce cadre normatif et se tiennent aux engagements licites, loyaux et transparents communiqués initialement aux personnes concernées.

573. Il aura suffi de quelques mois pour que la surveillance et le contrôle d'un nouveau virus ait risqué d'évoluer vers une surveillance et un contrôle social, sous le couvert de la protection de la santé publique²⁰⁶⁵. L'unique façon d'y échapper aurait été la soustraction des individus aux examens de dépistage au SARS-CoV-2 ; et cette issue aurait été effroyable pour la protection de la santé individuelle comme collective. Le Comité national pilote d'éthique du numérique ne manque pas de rappeler que « *des mesures imposées pourraient produire un effet inverse à celui qui est visé en induisant des comportements de désaccord* »²⁰⁶⁶. Le respect des mesures d'isolement prophylactique devrait davantage résulter d'une éducation sanitaire que de la crainte d'un traitement de données médicales despotique. En effet, « *l'idée de « la santé par l'éducation » répond à une conception selon*

²⁰⁶³ L'article 66 de la Constitution dispose que « *nul ne peut être arbitrairement détenu. L'autorité judiciaire, gardienne de la liberté individuelle, assure le respect de ce principe dans les conditions prévues par la loi.* ».

²⁰⁶⁴ METALLINOS (N.), *loc. cit.*

²⁰⁶⁵ Voir : HIRSCH (E.), *Une démocratie confinée. L'éthique quoi qu'il en coûte*, Érès, 2021 ; FASSIN (D.), HENCKES (N.), KEMPF (R.) et al., *La démocratie à l'épreuve de l'épidémie*, *Esprit*, 2020 n° 10, p. 81 à p. 106.

²⁰⁶⁶ Comité National Pilote d'Éthique du Numérique, *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, Bulletin de veille n°1, 7 avril 2020, p. 11.

laquelle la vie de l'être humain serait directement liée à sa capacité éducationnelle »²⁰⁶⁷. Ainsi « *la survie des espèces, et en particulier celle de l'espèce humaine, passerait par sa capacité à s'éduquer* »²⁰⁶⁸. De la même façon que le singe et la fourmi malades pratiquent instinctivement la distanciation sociale pour protéger leurs congénères²⁰⁶⁹, l'être humain devrait intelligemment s'isoler des membres la société lorsqu'il est atteint d'une maladie transmissible. A cet égard, les finalités originaires du dispositif SI-DEP apparaissent adéquatement indispensables pour le suivi médical des personnes infectées ainsi que pour la prévention des personnes risquant de l'être grâce à leur isolement spontané et volontaire.

Si l'exclusion réglementaire du droit d'opposition par les pouvoirs publics permettait d'affirmer le caractère obligatoire du traitement SI-DEP, le législateur européen avait déjà écarté l'application de cette prérogative « *dans la mesure où le traitement est nécessaire [...] pour des motifs d'intérêt public dans le domaine de la santé publique* »²⁰⁷⁰. De surcroît, le responsable de traitement n'est pas tenu de faire droit à la demande d'opposition dès lors qu'il existe des motifs légitimes et impérieux importants pour le traitement qui prévalent sur les intérêts, les droits et les libertés de la personne concernée²⁰⁷¹. En tout état de cause, il en résulte que la finalité poursuivie par ce système d'information emporte conséquemment une réduction de l'autonomie de décision des personnes concernées.

574. Cette réduction de l'autodétermination informationnelle doit néanmoins être accompagnée d'une information préalable renforcée. La transparence étant gage de confiance, la CNIL a attiré l'attention du ministère chargé de la santé « *sur la nécessité de prévoir des modalités permettant une diffusion auprès de l'ensemble des personnes concernées d'une information claire, transparente et pédagogique* »²⁰⁷². La pédagogie étant une méthode d'éducation, l'information délivrée préalablement à l'examen de dépistage, puis

²⁰⁶⁷ STEVENIN (P.), *La santé par l'éducation*, Les Sciences de l'éducation - Pour l'Ère nouvelle, vol. 39, , 2006, n°1, p. 81.

²⁰⁶⁸ *Ibid.*

²⁰⁶⁹ Voir : ROMANO (V.), MACINTOSH (A.), SUEUR (C.), *Stemming the flow: information, infection and social evolution*, Trends in Ecology & Evolution, Vol. 35, 2020, n°10, p. 849.

²⁰⁷⁰ Article 17.3 c) du RGPD.

²⁰⁷¹ Article 21.1 du RGPD.

²⁰⁷² CNIL, Délibération n° 2020-051 du 8 mai 2020, *loc. cit.*

lors de la réception du résultat individuel²⁰⁷³, devrait expressément enseigner l'importance des enjeux liés à la finalité du traitement obligatoire des données médicales. L'implication et l'adhésion des citoyens – fussent-elles contraignantes – à la politique de lutte contre la menace sanitaire tendent à la démocratie sanitaire²⁰⁷⁴. Aucun citoyen ne devant en être écarté, la CNIL appelle à ce que le document d'information relatif au traitement SI-DEP soit remis en main propre « *aux personnes qui ne disposeraient pas d'un accès à Internet ou qui souhaiteraient disposer d'un tel document* »²⁰⁷⁵. Ce traitement étant national et obligatoire pour toute personne testée, la prévention de la fracture numérique exige qu'il y soit porté la mention « *d'une adresse postale, en plus d'une adresse électronique, afin de permettre aux personnes concernées de demander des informations sur le traitement et d'exercer les droits par cette voie* »²⁰⁷⁶.

Si les citoyens fichés dans SI-DEP ne peuvent s'opposer au traitement de leurs données médicales, ils jouissent néanmoins du droit d'y accéder. Ce droit d'accès accroît l'information et la transparence dues aux personnes concernées. Certainement, les citoyens fichés peuvent prendre connaissances des données retranscrivant toute intervention réalisée sur les informations qui les concernent. Par suite, « *les personnes devraient pouvoir accéder au détail des opérations effectuées sur leurs données, à l'exclusion des données qui pourraient permettre l'identification des personnes habilitées ayant réalisé lesdites opérations* »²⁰⁷⁷. Alors que les professionnels intervenant dans le traitement SI-DEP sont habilités à connaître les informations intimes des citoyens fichés, pourquoi les personnes fichées ne pourraient-elles pas contrôler l'identité et l'habilitation des individus exploitant leur chose anthropomorphique ? Compte tenu des menaces et des agressions perpétrées à l'encontre des acteurs agissant contre la propagation du virus de la Covid-19²⁰⁷⁸, l'anonymat des données de traçabilité contribuerait à leur sécurité. Par surcroît, la vérification de l'authentification des connexions appartient au responsable de traitement. En cas de violation

²⁰⁷³ Conformément à l'article 12 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰⁷⁴ Cf. Paragraphe 615.

²⁰⁷⁵ CNIL, Délibération n° 2020-051 du 8 mai 2020, *loc. cit.*

²⁰⁷⁶ *Ibid.*

²⁰⁷⁷ *Ibid.*

²⁰⁷⁸ Safeguarding Health in Conflict, *New map depicts 412 acts of pandemic-related violence and threats to health workers and services around the world in 2020*, 03 février 2021. Article de l'ONG disponible en ligne sur le site [www.safeguardinghealth.org]. Consulté le 24 octobre 2021.

des données médicales « *susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique* »²⁰⁷⁹, les citoyens fichés en seraient informés dans les meilleurs délais par le responsable de traitement.

Par ailleurs, si une erreur ou une incomplétude administrative était constatée lors de l'exercice du droit d'accès, les personnes concernées pourraient en demander la rectification auprès de la direction générale de la santé. Dans cette attente, elles devraient pouvoir demander la limitation du traitement de leurs données médicales, à moins que leur utilisation ne soit nécessaire pour des motifs d'intérêt public importants²⁰⁸⁰. Eu égard à l'urgence des mesures de *contact tracing*, le droit à la limitation du traitement semblerait néanmoins inapplicable²⁰⁸¹.

575. De même que les personnes effectuant un examen de dépistage au SARS-CoV-2 ne peuvent s'opposer à l'enregistrement du résultat dans le fichier SI-DEP, les personnes effectivement infectées ne peuvent s'opposer à leur identification au sein du dispositif Contact Covid. En effet, lorsqu'une personne est testée positive au virus de la Covid-19, ses données médicales et administratives y sont intégrées par l'intermédiaire du traitement SI-DEP²⁰⁸². Lorsque le diagnostic au SARS-CoV-2 n'est pas établi à l'appui d'un dépistage virologique ou sérologique, mais à la suite d'un diagnostic clinique fondé sur une imagerie médicale pertinente ou sur des éléments cliniques susceptibles de caractériser l'infection, il appartient au professionnel de santé l'ayant élaboré d'enregistrer le patient positif dans le fichier Contact Covid²⁰⁸³. Il en résulte que tout citoyen diagnostiqué positif au SARS-CoV-2 ne peut subséquentement refuser l'attache des enquêteurs sanitaires aux fins de *contact tracing*. Ce système d'information étant fondé sur la mission d'intérêt public dévolue à la caisse nationale de l'assurance maladie, le Premier ministre a expressément écarté l'application du droit d'opposition²⁰⁸⁴. Cette exclusion « *doit s'analyser comme la faculté, prévue par l'article 23 du RGPD, de limiter les droits des personnes pour, notamment, des*

²⁰⁷⁹ Article 34.1 du RGPD.

²⁰⁸⁰ Article 18.2 du RGPD.

²⁰⁸¹ Cf. Paragraphe 515.

²⁰⁸² Article 2 I 2° du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰⁸³ Article 1 III 1° du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰⁸⁴ Article 7 I du décret n°2020-551 du 12 mai 2020, *loc. cit.*

objectifs importants de santé publique »²⁰⁸⁵. Alors que le droit d'opposition devient inexistant, les personnes concernées devraient, en principe, être informées de cette limitation²⁰⁸⁶.

576. Lors du premier contact avec la personne infectée, l'agent habilité à réaliser l'enquête sanitaire doit préalablement l'informer des caractéristiques du dispositif Contact Covid conformément à l'article 13 du RGPD²⁰⁸⁷. En complément de cette information orale, les notices d'information « *sont également diffusées sur les sites internet du ministère chargé de la santé et de la Caisse nationale de l'Assurance maladie* »²⁰⁸⁸. Néanmoins, aucune disposition réglementaire ne préserve les risques de discrimination liés à la connexion numérique. Face « *à la création d'un écosystème complexe, nécessitant que les personnes concernées disposent des renseignements nécessaires et des moyens de faire valoir leurs droits* »²⁰⁸⁹, une information orale complétée d'une information numérique apparaît insuffisante. Une fois la communication téléphonique interrompue, comment le citoyen déconnecté peut-il étudier les éléments d'information – *a priori* – expliqués oralement ? Comment peut-il se reporter aux modalités d'exercice de ses droits d'accès, de rectification et – dans la mince éventualité où il pourrait être appliqué – de limitation ? L'enseignement des caractéristiques du traitement à des fins de protection de la santé publique semble singulièrement capital, *a fortiori* lorsque sa mise en œuvre est obligatoire.

577. A l'inverse, si les personnes infectées ne peuvent s'opposer à leur identification dans le dispositif Contact Covid, elles restent libres de participer au *contact tracing*. Après avoir été informé des spécificités de ce traitement préalablement à l'enquête sanitaire, rien ne contraint le citoyen fiché à fournir les données nécessaires à l'identification des personnes à risque de contamination, si ce n'est un devoir de réciprocité ou encore une responsabilité

²⁰⁸⁵ CNIL, Délibération n° 2020-051 du 8 mai 2020, *loc. cit.*

²⁰⁸⁶ Article 23.2 h) du RGPD.

²⁰⁸⁷ Article 6 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

²⁰⁸⁸ *Ibid.*

²⁰⁸⁹ CNIL, Délibération n° 2021-077 du 1^{er} juillet 2021 portant avis sur un projet de décret modifiant le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions et le 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, *JORF* n°0162, 14 juillet 2021, texte n°103.

commune à l'égard de la protection de la santé de la société²⁰⁹⁰. Pourquoi créer un traitement obligatoire à des fins de traçage des contacts alors que le traçage des contacts est facultatif ?

Dans un contexte pandémique, la clé de voûte pour endiguer la propagation d'un virus réside dans la rupture des chaînes de contamination²⁰⁹¹. Finalement, l'efficacité du fichage des citoyens dans la lutte contre la crise sanitaire dépend de la somme des comportements individuels²⁰⁹². En dépit du caractère obligatoire du traitement SI-DEP au profit de la protection de la santé publique, la contribution volontaire de toute personne contaminée à l'identification des cas potentiels constitue une étape fondamentale pour rompre les chaînes de transmission et ainsi enrayer la circulation du SARS-CoV-2. Vraisemblablement, l'ensemble des personnes qui ont été infectées par le virus de la Covid-19 ont un point commun : la première personne atteinte par cette maladie. Certainement, toutes les personnes ayant contracté ce virus sont un maillon de la chaîne internationale de contamination. Alors, ce fichage obligatoire à des fins de *contact tracing* ne présenterait aucune utilité si toute personne contaminée se soustrayait à l'identification des personnes à risque de contamination²⁰⁹³. Le cas échéant, cette opération de traitement ne consisterait qu'en un méga stockage administratif de données médicales. Il en advient que le comportement des individus peut réduire à néant la finalité du dispositif Contact Covid et subséquemment, le démunir de toute raison d'être. Si ce traitement de données médicales ne présentait pas un caractère intégralement obligatoire, ne conviendrait-il pas d'assortir le *contact tracing* d'un véritable droit au consentement accompagné d'un droit à l'effacement ?

²⁰⁹⁰ Cf. Paragraphe 613.

²⁰⁹¹ Assurance maladie, *Pour améliorer le contact tracing, le téléservice Contact Covid évolue*, 30 novembre 2020, mis à jour le 31 mai 2021. Disponible en ligne sur le site [www.ameli.fr]. Consulté le 24 octobre 2021.

²⁰⁹² Cf. Paragraphe 611.

²⁰⁹³ Cf. Paragraphes 589 et 611.

B) Le traitement facultatif des données médicales des citoyens en appui de la gestion de la crise sanitaire

578. Bien que les personnes contaminées par le SARS-CoV-2 ne peuvent s'opposer à l'enregistrement de leurs données administratives et médicales dans le dispositif Contact Covid, elles peuvent refuser de révéler les lieux publics qu'elles ont fréquentés, les événements auxquels elles ont participé et l'identité des personnes qu'elles ont côtoyées. En revanche, les personnes à risque de contamination, identifiées par les personnes contaminées ou par l'intermédiaire des responsables d'établissements recevant du public ou d'événements, peuvent s'opposer au traitement de leurs données personnelles. D'abord, les personnes à risque de contamination peuvent décliner l'entretien sanitaire après que l'enquêteur les ait informées des caractéristiques du traitement lors de la communication téléphonique²⁰⁹⁴. Ensuite, elles peuvent s'opposer à la réutilisation de leurs données personnelles recueillies auprès des personnes les ayant évaluées comme cas contact ou personne co-exposée, et demander qu'elles soient effacées du système d'information. Cette demande d'exercice des droits doit être adressée auprès de leur organisme d'assurance maladie de rattachement, à condition – évidemment – que les modalités d'exercice leur aient été effectivement expliquées.

A la réception d'une telle demande, le responsable de traitement est tenu d'examiner les raisons tenant à la situation particulière de la personne à risque de contamination²⁰⁹⁵. Il est autorisé à passer outre ce droit d'opposition s'il démontre que les intérêts impérieux de santé publique définis à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prévalent sur les intérêts, les droits et les libertés du demandeur²⁰⁹⁶. Cette mise en balance, affirmée par décret²⁰⁹⁷, se trouve biaisée dans le contexte de la crise sanitaire. Certainement, l'ensemble des systèmes d'information mis en œuvre pour lutter contre la propagation de la Covid-19 constituent, par essence, des traitements dérogatoires aux droits et aux libertés des personnes fichées. Assurément, la finalité du dispositif Contact Covid légitime tant sa mise en œuvre que la contravention à l'exercice du droit d'opposition des personnes concernées. Si ces

²⁰⁹⁴ Conformément aux articles 13 et 14 du RGPD.

²⁰⁹⁵ Cf. Paragraphe 522.

²⁰⁹⁶ Article 7 I du décret n°2020-551 du 12 mai 2020, *loc. cit.* ; Article 21.1 du RGPD.

²⁰⁹⁷ Article 7 I du décret n°2020-551 du 12 mai 2020, *loc. cit.*

traitements temporaires ont pu être légalement déployés, ce n'est qu'en considération des motifs impérieux pour la santé publique auxquels ils concourent. Autrement dit, la balance entre l'atteinte aux droits et libertés des citoyens et le bénéfice pour la protection de la santé publique a été pesée préalablement à l'instauration de ces dispositifs. Tandis que l'objectif de lutte contre cette pandémie permet de déroger aux droits individuels de l'ensemble des membres de la société, pourquoi les intérêts particuliers d'un citoyen devraient prévaloir ? Cette possibilité, admise par le pouvoir exécutif²⁰⁹⁸, engendre une rupture d'égalité entre l'unité du sacrifice collectif des droits particuliers au nom des intérêts généraux de la société et l'individu qui aurait conservé son droit individuel. Il en résulte que le fondement juridique du traitement Contact Covid s'accommode mal de l'existence d'un droit d'opposition. C'est la raison pour laquelle le législateur européen a, de façon générique, écarté l'application du droit d'opposition « *dans la mesure où le traitement est nécessaire [...] pour des motifs d'intérêt public dans le domaine de la santé publique* »²⁰⁹⁹. Il aurait donc été préférable que le pouvoir exécutif exclut – de nouveau – la reconnaissance de ce droit non absolu.

579. L'enquête sanitaire étant facultative, le fichage des personnes contaminées et à risque de contamination est-il nécessaire à la finalité du dispositif Contact Covid au cas où elles refuseraient de s'y prêter ? Dans l'hypothèse où la personne contaminée par le virus de la Covid-19 récuserait l'enquête sanitaire, les informations contenues dans le fichier Contact Covid porteraient uniquement sur celles recueillies par l'intermédiaire du dispositif SI-DEP. Le cas échéant, cet enregistrement dans l'outil Contact Covid ne présenterait aucun intérêt pour les finalités décrites au premier article du décret n° 2020-551 du 12 mai 2020. En effet, le *contact tracing* ne pourrait être réalisé tandis que la surveillance épidémiologique et la recherche pourraient être développées à partir des données identiquement colligées dans le fichier SI-DEP. Or, le principe de la limitation de la conservation des données à caractère personnel exige qu'elles soient effacées ou anonymisées dès l'instant où la finalité du traitement est révolue²¹⁰⁰. Par suite, « *le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais* »²¹⁰¹ lorsqu'elles « *ne sont plus*

²⁰⁹⁸ *Ibid.*

²⁰⁹⁹ Article 17.3 c) du RGPD ; Cf. Paragraphe 526.

²¹⁰⁰ Article 5.1 e) du RGPD.

²¹⁰¹ Article 17.1 a) du RGPD.

nécessaires au regard des finalités pour lesquelles elles ont été collectées »²¹⁰². L'absence de réponse de la personne contaminée à l'enquête sanitaire devrait donc entraîner l'effacement des données personnelles la concernant du fichier Contact Covid. De la même façon, la conservation des données d'identification des personnes à risque de contamination dans ce dispositif ne présente aucune utilité pour la lutte contre la propagation du SARS-CoV-2 lorsqu'elles déclinent l'enquête sanitaire proposée. Certainement, seules des données strictement adéquates, pertinentes et limitées à ce qui est nécessaire à la finalité de ce traitement exceptionnel peuvent être licitement traitées²¹⁰³. En conséquence, l'absence de participation du citoyen évalué comme cas contact ou personne co-exposée au *contact tracing* devrait emporter l'effacement des données personnelles recueillies auprès de tiers.

Au demeurant, la communication téléphonique adressée aux personnes à risque de contamination, en vue de procéder à l'entretien sanitaire, peut être observée comme une alerte à l'instar de la notification générée par l'application TousAntiCovid. Avertie du risque, il revient à la personne concernée la responsabilité morale de se soumettre à un examen de dépistage virologique ou sérologique ainsi qu'à l'isolement. La participation de la personne contaminée à l'enquête sanitaire à des fins de *contact tracing* présente donc une réelle importance pour la personne à risque de contamination. Dans un second temps, si la personne à risque de contamination prenait la responsabilité de se faire dépister, les résultats virologiques ou sérologiques de son examen seraient obligatoirement inscrits dans le fichier SI-DEP. Dans le cas où le dépistage au SARS-CoV-2 se révélait positif, la personne effectivement infectée serait alors inscrite au sein du fichier Contact Covid pour la réalisation de l'enquête sanitaire. Le cas échéant, elle se trouverait, à son tour, libre d'y répondre. Cependant, l'alerte des personnes à risque de contamination devrait être observée comme un devoir civique de concours à la protection de la santé d'autrui. L'essentiel de la prévention contre la propagation d'un virus consiste davantage en l'information d'un risque de contamination que sur la collecte centralisée d'informations relatives aux personnes à risque d'infection. Après avoir été alertées d'un risque de contamination, les informations relatives aux personnes en contact ou co-exposées au virus devraient alors être effacées conformément au principe de limitation de conservation.

²¹⁰² *Ibid.*

²¹⁰³ Article 5.1 c) du RGPD.

580. Conformément aux recommandations du Comité européen de la protection des données²¹⁰⁴, la réalisation du *contact tracing* au moyen de l'application TousAntiCovid repose également sur le volontariat des citoyens – obligatoirement – connectés au numérique. Bien que ce système d'information ne soit pas légalement appuyé sur le consentement²¹⁰⁵ des utilisateurs, « *le volontariat se matérialise dans toutes les composantes du dispositif* »²¹⁰⁶. Les motifs d'intérêt public dont est investi le ministre chargé de la santé, en sa qualité de responsable de traitement, fondent légalement un dispositif qui dépend, par ailleurs, du volontariat des personnes concernées.

Le choix de cette base légale présente des avantages. D'abord, il permet « *de concilier en toute sécurité juridique le caractère volontaire de l'utilisation de cette application et les éventuelles incitations des pouvoirs publics à une telle utilisation, afin de promouvoir son utilisation la plus large possible* »²¹⁰⁷. Ensuite, il permet d'écarter un consentement qui, dans un contexte pandémique, serait probablement vicié. En effet, le législateur européen ne valide le consentement que s'il est exprimé « *par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant* »²¹⁰⁸. Or, des auteurs ont révélé que les conditions applicables au consentement n'auraient pu être aisément réunies en raison de la crainte de la maladie, de pressions sociales ou de détournements abusifs de l'application²¹⁰⁹. Bien que le *volontariat* ne corresponde pas à un *consentement*, les pouvoirs publics ont tenté de maintenir son intégrité en certifiant que l'absence d'utilisation de l'application n'emporterait aucune conséquence négative sur les citoyens. Le caractère volontaire de ce traitement sensible doit donc être distingué d'un consentement au traitement. Cela n'empêche que les citoyens puissent sciemment désirer contribuer à la lutte contre la circulation du

²¹⁰⁴ EDPB, *Letter concerning the European Commission's draft Guidance on apps supporting the fight against the Covid-19 pandemic*, Ref: OUT2020-0028, 14 avril 2020.

²¹⁰⁵ Sur la notion de consentement voir : FERAL-SCHUHL (C.), *La protection des données personnelles*, Dalloz, 2019, p. 45 s.

²¹⁰⁶ CNIL, Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », *JORF* n°131, 30 mai 2020, texte n°106.

²¹⁰⁷ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 31

²¹⁰⁸ Considérant 32 du RGPD.

²¹⁰⁹ METALLINOS (N.), *op. cit.*, § 25 ; GAVANON (I.), LE MAREC (V.), *Application de contact tracing : « un choix individuel gage de responsabilité collective » encadré par le CEPD*, Dalloz actualité, 21 avril 2020 ; PAWLOTSKY (A.), *op. cit.*, § 10 ; BENSAMOUN (A.), MARTIAL-BRAZ (N.), *StopCovid : sortir des postures ! Point de vue sur l'avis de la CNIL*, Dalloz IP/IT, 2020, n° 05, p. 280 à p. 283.

SARS-CoV-2. D'ailleurs, le Comité national pilote d'éthique du numérique, créé afin d'identifier les questions éthiques liées à l'usages du numérique dans le cadre de la crise sanitaire, estime que l'adhésion volontaire devrait être « *encouragée par une information au public sur l'utilité du suivi et par un appel au sens civique* »²¹¹⁰.

L'assurance de cette participation volontaire tend à préserver l'autodétermination informationnelle des utilisateurs de l'application TousAntiCovid. Certainement, les dispositions du décret fixant les modalités de ce traitement énoncent que « *l'application TousAntiCovid est installée librement et gratuitement par les utilisateurs. Ceux-ci ont la faculté d'activer ou non la fonctionnalité de l'application permettant de constituer l'historique de proximité* »²¹¹¹. De plus, « *en cas de diagnostic clinique positif au virus du covid-19 ou de résultat positif à un examen de dépistage à ce virus, les utilisateurs de l'application sont libres de notifier ou non ce résultat dans l'application et de transmettre au serveur l'historique de proximité* »²¹¹². Aussi, « *l'application peut être désinstallée à tout moment* »²¹¹³. Il en advient que le droit d'opposition à ce traitement est objectivé par la liberté, pour l'utilisateur, de désactiver l'application, de la désinstaller ou de se désabonner du serveur à tout moment et sans intermédiaire. Alors que le désabonnement entraîne l'effacement automatique des données pseudonymisées enregistrées en local et sur le serveur central, la désinstallation de l'application conduit à la suppression des données en local²¹¹⁴. En conséquence, « *les données potentiellement présentes sur le serveur central ne pourront alors plus être rattachées à un utilisateur* »²¹¹⁵. Toutefois, cette application ne fonctionnant qu'à partir de pseudonymes, le décret instaurant cette application prévient que « *les droits d'accès, de rectification ainsi que le droit à la limitation [...] ne peuvent s'exercer auprès du responsable de traitement* »²¹¹⁶. La préservation de la sécurité et de la confidentialité de ces données sensibles au moyen de la pseudonymisation justifie qu'aucune information

²¹¹⁰ Comité National Pilote d'Éthique du Numérique, *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, Bulletin de veille n°1, 7 avril 2020, p. 11.

²¹¹¹ Article 1 III du décret n°2020-650 du 29 mai 2020 relatif au traitement de données dénommé « TousAntiCovid », *JOFR* n°131, 30 mai 2020.

²¹¹² *Ibid.*

²¹¹³ *Ibid.*

²¹¹⁴ CNIL, Délibération n° 2020-056 du 25 mai 2020, *loc. cit.*

²¹¹⁵ *Ibid.*

²¹¹⁶ Article 4 du décret n°2020-650 du 29 mai 2020, *loc. cit.*

nominative ne puisse être traitée pour identifier l'utilisateur à la seule fin de respecter ses droits²¹¹⁷. Il n'en demeure pas moins que « *dans la logique d'empowerment promue par le RGPD, c'est en effet l'utilisateur qui contrôle ses données* »²¹¹⁸ dans le cadre de l'utilisation de l'application TousAntiCovid. Selon le CNPEN, cette autonomie de décision représente un levier essentiel de régulation de l'usage des technologies du numérique²¹¹⁹.

581. Identiquement, le titulaire d'un Passe sanitaire ou d'un Passe vaccinal semble détenir le contrôle des données sensibles qu'il contient. En effet, tout citoyen remplissant les conditions de son obtention peut volontairement le générer aux fins d'en apporter la preuve. Ce justificatif est délivré à la demande du citoyen remplissant les conditions réglementairement nécessaires à sa production²¹²⁰ au format papier ou sur support numérique²¹²¹. Le citoyen en possession d'un *Passe* en possède alors l'entière maîtrise. D'une part, la révélation des informations qu'il renferme *via* sa présentation lui appartient. D'autre part, sa suppression des supports numériques ou la destruction des supports papiers qui le formalise lui revient. Néanmoins, l'exercice de cette autodétermination informationnelle engendre des conséquences pour les libertés individuelles des personnes concernées. Certainement, la présentation du Passe sanitaire ou du Passe vaccinal peut subordonner le franchissement des frontières des Etats membres de l'Union européenne ainsi que l'accès aux lieux, services et événements qui le requièrent. Dès lors que le citoyen souhaite volontairement voyager à l'étranger ou se rendre dans ces lieux et événements, il se voit contraint de révéler ses données personnelles inférant des informations sensibles au moyen de son Passe sanitaire ou de son Passe vaccinal. Il est vrai que le dispositif « *vise à conditionner l'accès à certains lieux, établissements ou événements à la présentation de la preuve de l'état de santé des personnes* »²¹²². Alors, si le citoyen conservait son autonomie de décision en décidant de ne pas générer ce justificatif, de le détruire ou de ne pas le présenter, il ne pourrait parvenir aux services qui l'exigent. A défaut, il commettrait une infraction pénale édictée à l'article L.3136-1 du code de la santé publique sur le fondement

²¹¹⁷ Article 11.1 du RGPD.

²¹¹⁸ CLUZEL-METAYER (L.), *La datasurveillance de la Covid-19*, RDSS, 2020, p. 919

²¹¹⁹ Comité National Pilote d'Ethique du Numérique, *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, Bulletin de veille n°1, 7 avril 2020, p. 11.

²¹²⁰ Article 2-3 I du décret n°2021-699 du 1^{er} juin 2021, *loc. cit.*

²¹²¹ Article 2-3 II du décret n°2021-699 du 1^{er} juin 2021, *loc. cit.*

²¹²² CNIL, Délibération n° 2021-054 du 12 mai 2021, *op. cit.*, cons. 7.

de l'article L.3131-15 du même code. Il encourrait alors une contravention de quatrième classe. Si cette infraction était constatée à nouveau dans un délai de quinze jours, une contravention de cinquième classe serait prononcée²¹²³. En cas de nouvelle récidive dans un délai de trente jours, les faits seraient « *punis de six mois d'emprisonnement et de 3 750 € d'amende ainsi que de la peine complémentaire de travail d'intérêt général* »²¹²⁴.

Par ailleurs, l'obligation de présentation d'un Passe vaccinal – ou, le cas échéant, d'un Passe sanitaire – s'applique également « *aux personnes qui interviennent dans ces lieux, établissements, services ou évènements concernés lorsque la gravité des risques de contamination en lien avec l'exercice des activités qui y sont pratiquées le justifie* »²¹²⁵. Lorsqu'un employé ou un agent public soumis à cette obligation exerce son autodétermination informationnelle en se soustrayant à la présentation de ce justificatif, il ne peut exercer son emploi et se trouve obligé d'utiliser des jours de repos conventionnels ou des jours de congés payés. A défaut, la suspension de son contrat de travail et l'interruption du versement de sa rémunération sont prononcées par son employeur jusqu'à ce qu'il produise le justificatif requis²¹²⁶. Par surcroît, lorsque cette situation « *se prolonge au-delà d'une durée équivalente à trois jours travaillés, l'employeur convoque l'agent à un entretien afin d'examiner avec lui les moyens de régulariser sa situation, notamment les possibilités d'affectation, le cas échéant temporaire, sur un autre poste non soumis à cette obligation* »²¹²⁷.

Il en advient que « *la présentation d'un passe [vaccinal ou d'un passe] sanitaire pour accéder au restaurant ou à la terrasse d'un bar est nécessairement attentatoire à la vie privée des personnes* »²¹²⁸ et « *affecte plusieurs libertés fondamentales puisque des entraves existent dans la possibilité de circuler, de se réunir, de travailler* »²¹²⁹. Cependant, la restriction de l'autonomie de décision quant à l'usage de ses informations sensibles permet,

²¹²³ Article 3136-1 alinéa 3 du code de la santé publique.

²¹²⁴ Article 3136-1 alinéa 4 du code de la santé publique.

²¹²⁵ Article 1 II A de la loi n°2021-689 du 31 mai 2021, *loc. cit.*

²¹²⁶ Article 1 II C de la loi n°2021-689 du 31 mai 2021, *loc. cit.*

²¹²⁷ Article 1 II C de la loi n°2021-689 du 31 mai 2021, *loc. cit.*

²¹²⁸ BOULANGER (A.), *L'impact du « passe sanitaire » sur les droits et libertés fondamentaux des personnes*, Revue Juridique Personnes et Famille, 2021, n° 10, § 5.

²¹²⁹ BOULANGER (A.), *op. cit.*, § 7.

en contrepartie, de retrouver certaines libertés. Effectivement, l'introduction du Passe sanitaire puis du Passe vaccinal « *a été conçu pour faciliter la reprise ou le maintien de certaines activités ou déplacements qui à défaut auraient dû être durablement restreints voire interdits* »²¹³⁰. Egalement, le législateur européen considère que « *la libre circulation des personnes qui, selon des preuves scientifiques solides, ne présentent pas de risque important pour la santé publique [...] ne devrait pas être soumise à des restrictions* »²¹³¹.

582. En définitive, que le fichage soit obligatoire ou volontaire, les mesures de police administrative prises à l'appui des systèmes d'information destinés à la lutte contre la crise sanitaire conduisent à restreindre les droits et les libertés fondamentaux des citoyens. Il en ressort que le traitement des données médicales des personnes fichées engendre des conséquences liberticides individuelles et collectives. En définitive, le traitement des données médicales des citoyens devient un outil d'ouverture ou de restriction de l'ensemble des droits et des libertés fondamentaux. Toutefois, comme le souligne raisonnablement Augustin Boulanger, « *ces atteintes, aussi contraignantes soient-elles, peuvent néanmoins être admises dans le cadre de la lutte contre la Covid-19, à condition toutefois de respecter un principe de proportionnalité* »²¹³². Evidemment, la mise en œuvre de l'objectif de protection de la santé publique a généralement pour effet d'entraver les libertés et les droits fondamentaux. Néanmoins, ce motif impérieux exige de concilier l'intérêt général et les intérêts particuliers tout en sachant que l'intérêt commun est considéré comme « *l'intérêt particulier d'un peuple* »²¹³³. La protection de la santé publique contre les menaces sanitaires légitime donc le traitement des données médicales des citoyens et justifie une restriction de leur autodétermination informationnelle à leur égard.

²¹³⁰ Etude d'impact du projet de loi relatif à la gestion de la crise sanitaire, 19 juillet 2021, p. 11.

²¹³¹ RÈGLEMENT (UE) 2021/953 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19, cons. 7.

²¹³² BOULANGER (A.), *loc. cit.*

²¹³³ PENIGAUD DE MOURGUES (T.), *Intérêt commun ou intérêt général ? De l'enjeu d'une décision terminologique chez Rousseau*, Astéris, 2017, n°17, § 3.

Section 2 : La légitimation des fichages d'exception par la préservation de la santé publique

« Comme l'explique Max Weber, dès lors que, dans une société, la légitimité du pouvoir repose sur la raison, les citoyens n'acceptent de se soumettre aux décisions des gouvernants que parce qu'ils les jugent conformes à l'intérêt de tous et de chacun. »²¹³⁴.

583. La notion d'intérêt général constitue un outil capital pour la protection des droits fondamentaux. En effet, les pouvoirs du législateur sont circonscrits par la satisfaction d'un intérêt général lorsqu'il entend restreindre l'exercice d'un droit fondamental consacré par la Constitution ou par le droit de l'Union²¹³⁵. Si la lutte contre une menace sanitaire pesant sur la santé d'une population présente indubitablement un intérêt public justifiant la mise en œuvre d'un traitement de données sensibles²¹³⁶, ce motif d'intérêt général doit prendre essence dans le bloc de constitutionnalité lorsque le système d'information, créé par le législateur, a pour effet de limiter les droits fondamentaux des personnes fichées. Pour cause, la notion d'intérêt général constitue une condition de constitutionnalité de la loi²¹³⁷. C'est alors que l'objectif à valeur constitutionnel de protection de la santé publique, consacré par le Préambule de la Constitution de 1946, fonde le motif d'intérêt général poursuivi par la lutte contre une menace sanitaire (**Paragraphe 1**). Il en advient que la mise en œuvre d'un traitement de données médicales à cette fin prévaut sur les droits à la vie privée et à la protection des données des personnes concernées.

584. Bien que la poursuite d'un intérêt commun devrait favoriser l'acceptabilité de la restriction des droits fondamentaux des citoyens, elle ne suffit pas à objectiver la protection de la santé publique. Assurément, le succès d'une stratégie de santé publique repose tant sur son acceptabilité sociale que sur le concours des membres de la société. Si « *les droits de l'homme et les libertés fondamentales constituent l'un des fondements essentiels de toute*

²¹³⁴ MERLAND (G.), *L'intérêt général, instrument efficace de protection des droits fondamentaux ?*, Cahiers du Conseil constitutionnel, 2004, n° 16.

²¹³⁵ Article 52.1 de la Charte des droits fondamentaux de l'union européenne, *JOUE* C 326/391, 26 octobre 2012 ; Cons. Const., décision n° 79-107 DC, 12 juillet 1979, Rec. p. 31 ; RD publ., 1979, p. 1728.

²¹³⁶ Article 9.2 i) du RGPD ; Considérants 46 et 52 du RGPD.

²¹³⁷ Cons. Const., décision n° 79-107 DC, 12 juillet 1979, Rec. p. 31 ; RD publ., 1979, p. 1728.

société démocratique »²¹³⁸, la concrétisation du droit à la protection de la santé publique devrait alors être mise en œuvre selon un processus démocratique (**Paragraphe 2**). Certainement, sans une participation citoyenne appuyée par l'affermissement de la démocratie sanitaire, la mise en œuvre des traitements de données médicales à des fins de lutte contre une menace sanitaire ne saurait être efficace pour la protection de la santé publique.

Paragraphe 1 : La prévalence de la protection de la santé publique

*« La lutte contre cette épidémie, qui relève de l'objectif à valeur constitutionnelle de protection de la santé, constitue un impératif majeur de nature à justifier, dans certaines conditions, des atteintes transitoires au droit à la protection de la vie privée et des données à caractère personnel. »*²¹³⁹

585. Comme le souligne justement Guillaume Merland, *« si l'intérêt général est une condition nécessaire pour qu'une restriction législative puisse satisfaire aux exigences du contrôle de constitutionnalité, elle n'est jamais une condition suffisante »*²¹⁴⁰. Bien que les traitements de données médicales aux fins de lutte contre une menace sanitaire présentent théoriquement un intérêt pour la protection de la santé publique, encore faut-il que leur mise en œuvre soit véritablement nécessaire à cette finalité et proportionnée aux atteintes portées aux droits à la vie privée et à la protection des données personnelles (**A**). Ces traitements exceptionnels, parce qu'ils attentent aux droits fondamentaux des personnes concernées, ne doivent perdurer que pendant le temps strictement nécessaire à l'accomplissement de leur finalité et, tout au plus, pendant la seule période de lutte contre la menace sanitaire (**B**). Certainement, l'objectif impérieux de protection de la santé ne saurait justifier une dataturveillance généralisée, illimitée et démesurée. Ainsi que l'exige l'Etat de droit, l'application de ces critères apparaît essentielle pour trouver un équilibre raisonnable entre la protection de la santé publique et la préservation des droits fondamentaux des personnes fichées.

²¹³⁸ OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, LGDJ, ed. 8, août 2021.

²¹³⁹ CNIL, Délibération n° 2020-056 du 25 mai 2020, *loc. cit.*

²¹⁴⁰ MERLAND (G.), *loc. cit.*

A) La poursuite d'un motif d'intérêt général nécessaire et proportionné

« Au-delà de sa propre nécessité qui semble dictée par les circonstances, l'état d'urgence sanitaire ainsi consacré soulève, à nouveau, le questionnement sur l'équilibre à maintenir, dans un État de droit, entre le sort de la société et de la Nation et les libertés en période de crise grave. »²¹⁴¹.

586. Depuis le 16 octobre 2011²¹⁴², « le triple test de l'adaptation, de la nécessité et de la proportionnalité »²¹⁴³ est devenu « le standard international ou, à tout le moins, européen »²¹⁴⁴ en matière d'évaluation des atteintes légales aux droits et libertés fondamentaux. Si « le fonctionnement harmonieux d'une société démocratique exige que le législateur puisse réglementer les conditions d'exercice des droits et libertés des citoyens »²¹⁴⁵, encore faut-il que la disposition législative réponde à cette appréciation standardisée. Les traitements de données médicales des citoyens peuvent être déployés contre une menace sanitaire à condition que le législateur satisfasse à la triple exigence de nécessité, de pertinence et donc de proportionnalité. En effet, le critère de nécessité (1) est consubstantiel aux principes d'adéquation et de proportionnalité (2). Lorsque des moyens n'apparaissent pas nécessaires à la poursuite d'un intérêt général, ils ne peuvent être ni pertinents, ni proportionnés à cet objectif.

1. La nécessité du fichage des citoyens

587. Les différents systèmes d'information créés par les pouvoirs publics contribuent à renforcer la lutte contre la pandémie de la Covid-19. Compte tenu de l'ampleur exceptionnelle de la crise sanitaire, les pouvoirs publics avaient le devoir de prendre des mesures de protection de la santé de la population en ne laissant « de côté aucun outil

²¹⁴¹ ANDRIANTSIMBAZOVINA (J.), *L'état d'urgence sanitaire et les libertés*, Droit de la famille, 2020, n°06, étude n°19, § 1.

²¹⁴² CE, Ass., 26 octobre 2011, n° 317827, *Association pour la promotion de l'image*, Rec. Lebon, 2011, p. 505, concl. J. Boucher ; AJDA, 2011, n° 36, p. 2036, note R. Grand ; LPA, 2011, no 248, p. 10, note F. Chaltiel ; AJDA, 2012, n° 01, p. 35, chron. M. Guyomar et X. Domino.

²¹⁴³ SAUVE (J.-M.), *Le principe de proportionnalité, protecteur des libertés*, Les Cahiers Portalis, vol. 5, 2018, n°01, p. 15.

²¹⁴⁴ *Ibid.*

²¹⁴⁵ MERLAND (G.), *loc. cit.*

permettant d'endiguer la maladie »²¹⁴⁶. C'est ainsi que ces systèmes d'information ont été inscrits dans une stratégie politique globale, objectivée par le législateur et appliquée par le pouvoir exécutif. Autrement dit, ils constituent les outils pratiques de la mise en œuvre de la politique de protection de la santé publique. Ces traitements, « *nécessaires pour des motifs d'intérêt public dans le domaine de la santé publique* »²¹⁴⁷, participent donc à l'objectif de valeur constitutionnelle de protection de la santé.

Bien que le motif d'intérêt général apparaisse évident, son existence ne suffit pas à légitimer la mise en œuvre de ces systèmes d'information. Certainement, toute limitation aux droits fondamentaux doit être effectivement nécessaire à un motif d'intérêt général²¹⁴⁸. Dès lors que les systèmes d'information de lutte contre la menace sanitaire restreignent les droits au respect de la vie privée et à la protection des données personnelles, leur nécessité pour la protection de la santé publique doit être réellement démontrée. La justification de la nécessité du traitement est une étape fondamentale dans la mesure où son affirmation permet de concéder une réduction éventuelle des droits fondamentaux des personnes concernées. L'appréciation de cette nécessité doit donc être rigoureusement analysée et scrupuleusement contrôlée. Préalablement à l'instauration des systèmes d'information de lutte contre la menace sanitaire, Lucie Cluzel-Métayer s'est alors interrogée de savoir s'ils étaient nécessaires et, à tout le moins, utiles au combat contre le virus²¹⁴⁹. Afin de pertinemment répondre à cette question, François Pellegrini et Hélène Skrzypniak indiquent que « *pour être proportionnée, une mesure doit être nécessaire ; pour être nécessaire, elle doit être utile et, pour être utile, la mesure doit être efficace* »²¹⁵⁰. Il en advient que les systèmes d'information relatifs à la lutte contre la crise sanitaire doivent d'abord être nécessaires à l'objectif de santé publique poursuivi et, conséquemment, à l'atteinte aux droits fondamentaux qu'ils emportent. Seulement, « *comment apprécier la « nécessité » d'un traitement de données à caractère personnel en présence d'une situation de pandémie inédite où tout le monde semble*

²¹⁴⁶ CNIL, Délibération n° 2020-046 du 24 avril 2020, *loc. cit.*

²¹⁴⁷ Article 9.2 i) du RGPD.

²¹⁴⁸ Cons. Const., décision n° 79-107 DC, 12 juillet 1979, Rec. p. 31 ; RD publ., 1979, p. 1728 ; Article 52.1 de la Charte des droits fondamentaux de l'union européenne ; Article 8.2 de la convention européenne des droits de l'homme.

²¹⁴⁹ CLUZEL-METAYER (L.), *La datasurveillance de la Covid-19*, *op. cit.*, p. 918.

²¹⁵⁰ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 33

naviguer à vue ? »²¹⁵¹. L'évaluation de la nécessité d'un traitement de données médicales à des fins de lutte contre une menace sanitaire requiert d'examiner son utilité d'une part, et son efficacité d'autre part.

D'abord, un traitement de données à caractère personnel est considéré comme utile lorsque son usage est avantageux pour quelqu'un, qu'il satisfait un besoin ou répond à une demande sociale²¹⁵². Ensuite, un traitement de données à caractère personnel est réputé efficace lorsqu'il produit l'effet attendu dans de bonnes conditions²¹⁵³. Finalement, un traitement de données à caractère personnel s'avère nécessaire lorsque son existence ou son action est indispensablement requise pour répondre à une situation ou pour atteindre une fin²¹⁵⁴. Il en ressort que tout système d'information déployé pour lutter contre une pandémie doit effectivement satisfaire à cet objectif de protection de la santé publique. Réciproquement, l'atteinte aux droits à la vie privée et à la protection des données des personnes concernées, par la mise en œuvre du traitement, doit inévitablement permettre de répondre à l'objectif de santé publique poursuivi. Certainement, « *l'atteinte portée à la vie privée par ces traitements n'est admissible que si cette politique constitue la réponse appropriée pour ralentir la propagation de l'épidémie* »²¹⁵⁵. Préalablement à l'instauration de chaque traitement envisagé, il convient donc d'étudier leur pertinence pour l'intérêt de la protection de la santé publique et, en l'occurrence, pour la lutte contre la propagation du SARS-CoV-2.

588. Concrètement, l'appréciation de la nécessité des systèmes d'information – et donc de leur utilité et de leur efficacité – doit s'appuyer sur des critères tangibles. La nécessité des finalités déterminées pour chacun des traitements doit alors être évaluée certes juridiquement, mais, principalement, à l'aune d'expertises scientifiques et techniques. C'est ainsi que la spécification des systèmes d'information de lutte contre le virus de la Covid-19 a été décidée

²¹⁵¹ METALLINOS (N.), *op. cit.*, § 30.

²¹⁵² Définition de l'adjectif « utile » proposée par le CNRTL. Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 28 octobre 2021.

²¹⁵³ Définition de l'adjectif « efficace » proposée par le CNRTL. Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 28 octobre 2021.

²¹⁵⁴ Définition de l'adjectif « nécessaire » proposée par le CNRTL. Disponible en ligne sur le site [www.cnrtl.fr]. Consulté le 28 octobre 2021.

²¹⁵⁵ CNIL, Délibération n° 2020-051 du 8 mai 2020, *loc. cit.*

à l'appui des expertises du Centre européen de prévention et de contrôle des maladies²¹⁵⁶ et du « Conseil scientifique Covid-19 »²¹⁵⁷. En effet, l'édification d'outils politiques de lutte contre une menace sanitaire commande d'en appréhender les particularités. Lorsque la menace est constituée par un virus, les moyens d'action et l'urgence de leur déploiement diffèrent selon le son mode de transmission, sa contagiosité et sa gravité. Une étude scientifique relative à la sévérité du SARS-CoV-2 a révélé que la méthode de remaniement des protéines de fusion propres à ce virus, lorsqu'elles interagissent avec les cellules hôtes, lui confère un avantage en termes d'infectiosité, de transmissibilité, d'immunité et, *in fine*, de virulence par rapport aux coronavirus précédents²¹⁵⁸. De surcroît, sa propagation est accrue en raison de sa transmission par aérosols aéroportés. Ces caractéristiques scientifiques, et celles relatives aux différents variants, semblent avoir été prises en compte par les pouvoirs publics lors de l'évaluation de l'utilité des dispositifs de *contact tracing* et des Passes sanitaire et vaccinal²¹⁵⁹. Globalement, il en ressort que « *les technologies numériques, les applications mobiles et les échanges de données de santé représentent des atouts essentiels pour comprendre le mode de propagation du virus et lutter plus efficacement contre la covid-19* »²¹⁶⁰. Si l'utilité du traitement des données médicales des citoyens dans un contexte pandémique ne fait en théorie aucun doute, la réalité de son efficacité pour la protection de la santé publique se révèle plus épineuse à démontrer. Pour autant, la nécessité d'une atteinte aux droits fondamentaux des personnes concernées implique son efficience.

²¹⁵⁶ Règlement (CE) n°851/2004 du Parlement européen et du Conseil du 21 avril 2004 instituant un Centre européen de prévention et de contrôle des maladies, *JOUE* L 142/1, 30 avril 2004.

²¹⁵⁷ Décret du 3 avril 2020 portant nomination des membres du comité de scientifiques constitué au titre de l'état d'urgence sanitaire déclaré pour faire face à l'épidémie de covid-19, *JORF* n°82, 4 avril 2020, texte n° 19 ; Article L. 3131-19 du code de la santé publique.

²¹⁵⁸ KUMAR (A.), PRASOON (P.), KUMARI (C.), PAREEK (V.), FAIQ (M. A.), NARAYAN (R. K.), KULANDHASAMY (M.), KANT (K.), *SARS-CoV-2-specific virulence factors in COVID-19*, *Journal of Medical Virology*, March 2021, p. 1343 to p. 1350.

²¹⁵⁹ Conseil Scientifique Covid-19, Sortie progressive de confinement prérequis et mesures phares, Avis, 20 avril 2020 ; Conseil Scientifique Covid-19, Un nouvel ensemble numérique pour lutter contre le SARS-CoV-2, Avis, 20 octobre 2020 ; Conseil Scientifique Covid-19, Utilisation d'un pass sanitaire lors de grands rassemblements, Avis, 3 mai 2021 ; Conseil Scientifique Covid-19, Réagir maintenant pour limiter une nouvelle vague associée au variant Delta, Avis, 6 juillet 2021 ; Conseil Scientifique Covid-19, Fin de la période estivale et pass sanitaire rentrée de septembre 2021, Note d'alerte, 20 août 2021.

²¹⁶⁰ DE GROVE-VALDEYRON (N.), *Les applications de traçage contre la covid-19 : l'exception française dans le contexte européen*, RGDM, 2020, n°76, p. 133.

589. Alors, l'efficacité d'un traitement de données médicales contre une menace sanitaire doit être factuellement mesurée²¹⁶¹ en fonction des résultats de son effet par rapport à l'objectif attendu et en considération des autres moyens associés à la stratégie politique y afférent. A titre d'exemple, l'efficacité des dispositifs de *contact tracing* et des Passes sanitaire et vaccinal dépend directement de l'accessibilité aux tests rapides d'orientation diagnostique antigéniques, de la disponibilité des vaccins contre le SARS-CoV-2 et du comportement des personnes concernées. En vérité, le fichage des citoyens et des résidents français par les dispositifs Contact Covid et TousAntiCovid serait-il efficace si la majorité refusait de se prêter au *contact tracing* ? Certainement pas²¹⁶². Par conséquent, Aurèle Pawlotsky s'interroge de savoir si « *l'efficacité de l'utilisation des données personnelles dans un objectif de lutte contre la pandémie n'étant pas clairement établie, est-il bien raisonnable d'y avoir recours au prix d'une très forte restriction des libertés et droits fondamentaux des individus ?* »²¹⁶³. Il est vrai que l'efficacité des systèmes d'information de lutte contre une menace sanitaire ne peut être véritablement appréciée qu'au moyen de contrôles effectués *a posteriori*²¹⁶⁴. L'évaluation de l'efficacité de ces traitements nécessite donc une étude de performance rétrospective, pragmatique et vigoureuse. Seulement, le législateur étant peu rationaliste, comment garantir la véridicité du contrôle ultérieur de l'efficacité des atteintes aux droits au respect à la vie privée et à la protection des données personnelles ? Dans un contexte exceptionnel de crise sanitaire, des mécanismes doivent être indispensablement instaurés pour apprécier factuellement la nécessité de ces traitements extrêmement sensibles en toute indépendance²¹⁶⁵. En effet, le contrôle de l'utilité du traitement justifie l'atteinte qu'il porte aux droits et libertés de la personne concernée pendant que le contrôle de son efficacité légitime sa continuation. Si, conjuguées, l'utilité et l'efficacité forment la nécessité, l'intégrité de leur évaluation est gage d'équité dans un Etat de droit.

²¹⁶¹ « *Le principe de nécessité suppose le besoin de procéder à une évaluation factuelle combinée de l'efficacité de la mesure aux fins de l'objectif poursuivi et de déterminer si cette mesure est moins intrusive par rapport aux autres moyens de réaliser le même objectif.* », CEPD, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, p. 5.

²¹⁶² Cf. Paragraphes 589 et 611.

²¹⁶³ PAWLITSKY (A.), *op. cit.*, § 12.

²¹⁶⁴ Cf. Paragraphe 594.

²¹⁶⁵ Cf. Paragraphe 621.

590. Compte tenu de ce qui précède, les systèmes d'information nécessaires à la lutte contre une menace sanitaire ne peuvent poursuivre que des finalités légitimes à cet objectif de protection de la santé publique et suffisamment déterminées et explicites²¹⁶⁶. La spécification des finalités de ces systèmes d'information permet donc de figer leur nécessité au sein des actes législatifs et réglementaires qui les autorisent. Effectivement, les caractéristiques des traitements de données médicales à des fins de lutte contre une menace sanitaire, mis en œuvre pour le compte de l'Etat, doivent être détaillées au sein d'une disposition normative²¹⁶⁷. Cette cristallisation juridique de la nécessité des finalités de ces traitements en favorise le contrôle *ex ante* à leur mise en œuvre et *a posteriori*. La spécification des finalités permet de connaître l'objectif du traitement et de délimiter le périmètre de l'exploitation des données personnelles. Cette inscription permet donc de vérifier, à tout moment, que l'objectif de l'opération de traitement autorisée ne concourt activement qu'à l'objectif à valeur constitutionnelle de protection de la santé publique. La spécification des finalités du traitement permet de référencier sa nécessité. En effet, « *il importe dès lors de déterminer de façon suffisamment précise l'objectif d'intérêt général afin de pouvoir évaluer la nécessité de la mesure* »²¹⁶⁸. En outre, une définition claire des finalités de traitement nécessaires à la protection de la santé publique s'avère indispensable au respect du principe de proportionnalité²¹⁶⁹. Assurément, les finalités des opérations de traitement strictement nécessaires à la lutte contre la pandémie de la Covid-19 doivent être suffisamment déterminées pour pouvoir être mises en balance avec les conséquences engendrées pour les citoyens et les résidents fichés. Ainsi l'importance de l'ingérence dans leur vie privée peut être justement évaluée.

591. *Ex ante*, l'utilité des systèmes d'information portant atteinte aux droits et libertés des personnes concernées, dans l'intérêt de la protection de la santé publique, doit être examinée dès leur conception. Il appartient donc aux pouvoirs publics d'intégrer l'appréciation de l'utilité d'un traitement pour la lutte contre une menace sanitaire à l'occasion de l'élaboration

²¹⁶⁶ Article 5.1 b) du RGPD.

²¹⁶⁷ Article 35 de la loi Informatique et Libertés modifiée.

²¹⁶⁸ CEPD, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, p. 4.

²¹⁶⁹ Cf. Paragraphe 600.

du projet de loi ou de décret qui l'édifie. Cette approche devant être empirique²¹⁷⁰, il appartient aux pouvoirs publics de solliciter différents conseils pour cette évaluation. Dans le cadre des systèmes d'information de lutte contre la pandémie de la Covid-19, le pouvoir exécutif a été guidé par les avis indépendants du Conseil scientifique Covid-19 en amont de la construction des projets de loi et de décret les instituant. Une fois le projet d'acte normatif élaboré, le Gouvernement a bénéficié de l'avis du Conseil d'Etat préalablement à la présentation du projet de loi ou du projet de décret devant le Conseil des ministres²¹⁷¹. En effet, les traitements de données médicales destinés à la lutte contre une menace sanitaire, qu'ils soient ou non autorisés par la loi, doivent être créés par décret en Conseil d'Etat lorsqu'ils sont mis en œuvre pour le compte de l'Etat²¹⁷². Cela signifie que les actes réglementaires ayant déterminé les caractéristiques et les finalités de ces traitements sont systématiquement soumis à l'avis de la juridiction administrative suprême. C'est ainsi que le Conseil d'Etat a pu étudier la légalité, l'opportunité et, conséquemment, la nécessité des finalités des traitements SI-DEP, Contact Covid²¹⁷³, TousAntiCovid et des Passes sanitaire²¹⁷⁴ et vaccinal²¹⁷⁵ préalablement à leur adoption par le Gouvernement et, le cas échéant, à leur examen par le Parlement. Par surcroît, l'ensemble des projets de décret en Conseil d'Etat mettant en œuvre ces systèmes d'information ne peuvent être pris qu'après l'avis motivé de la CNIL²¹⁷⁶. A cette occasion, l'autorité de contrôle est chargée de vérifier la nécessité de chacun des dispositifs de lutte contre la menace sanitaire et, spécifiquement, l'utilité de chacune de leurs finalités pour cet objectif de santé publique²¹⁷⁷. Tandis que ces processus de conseil promeuvent la considération de l'utilité de l'atteinte aux droits fondamentaux des personnes concernées, ni le Gouvernement ni le Parlement ne sont tenus par les avis du Conseil scientifique Covid-19, du Conseil d'Etat et de la CNIL.

²¹⁷⁰ Cf. Paragraphe 588.

²¹⁷¹ Article 39 alinéa 2 de la Constitution.

²¹⁷² Article 31 II de la loi Informatique et Libertés modifiée.

²¹⁷³ CE, Avis n° 400104, *op. cit.*, cons. 16 à cons. 19.

²¹⁷⁴ CE, Avis n° 403629 du 19 juillet 2021 sur un projet de loi relatif à la gestion de la crise sanitaire, cons. 10 à cons. 21.

²¹⁷⁵ CE, Avis n° 404676 du 26 décembre 2021 sur un projet de loi renforçant les outils de gestion de la crise sanitaire et modifiant le code de la santé publique, cons. 4 à cons. 18.

²¹⁷⁶ Article 31 II de la loi Informatique et Libertés modifiée.

²¹⁷⁷ Voir notamment : CNIL, Délibération n° 2020-051 du 8 mai 2020, *loc. cit.* ; CNIL, Délibération n° 2020-056 du 25 mai 2020, *loc. cit.* ; CNIL, Délibération n° 2020-135 du 17 décembre 2020, *loc. cit.* ; CNIL, Délibération n° 2021-067 du 7 juin 2021, *loc. cit.* ; CNIL, Délibération n° 2021-097 du 6 août 2021, *loc. cit.*

592. Toutefois, l'article 34 de la Constitution annonce que les règles concernant « *les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » relèvent du domaine de la loi. Le Conseil d'Etat a alors précisé que « *le recours à une loi est cependant nécessaire dans l'hypothèse où le traitement envisagé ne peut être mis en œuvre sans modification d'une disposition législative qui y fait obstacle ainsi que dans celle où le traitement conduit à fixer des règles concernant les droits civiques et les garanties fondamentales accordées aux citoyens* »²¹⁷⁸. De surcroît, lorsqu'un Etat membre met en œuvre le droit de l'Union²¹⁷⁹, toute limitation aux droits au respect à la vie privée et à la protection des données personnelles tels que consacrés par la Charte des droits fondamentaux de l'Union européenne « *doit être prévue par la loi et respecter le contenu essentiel desdits droits* »²¹⁸⁰. Bien que les pouvoirs de restriction de certaines libertés publiques soient concentrés entre les mains de l'administration en période d'urgence sanitaire²¹⁸¹, les traitements de données médicales qui commandent des aménagements légaux, ou qui contreviennent à des droits fondamentaux, demeurent de la compétence du législateur.

Lors du contrôle éventuel de la constitutionnalité des lois adoptées par le Parlement²¹⁸², les sages de la rue Montpensier doivent scrupuleusement vérifier que les finalités de lutte contre la crise sanitaire, assignées aux systèmes d'information autorisés par la loi, sont bien nécessaires à l'objectif de valeur constitutionnelle de protection de la santé²¹⁸³. A cette occasion, le Conseil constitutionnel a le pouvoir de déclarer l'inconstitutionnalité d'une disposition législative par rapport au bloc de constitutionnalité. Ce contrôle permet, à la fois, de réguler l'activité des pouvoirs publics et de protéger le respect des droits et des libertés des personnes concernées. Certainement, « *la fonction essentielle du Conseil constitutionnel est la protection des droits fondamentaux contre le*

²¹⁷⁸ CE, Avis n° 400104, *op. cit.*, cons. 18.

²¹⁷⁹ Et plus particulièrement l'article 23 du RGPD.

²¹⁸⁰ Agence des Droits Fondamentaux de l'Union Européenne, *Application de la Charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale, Orientations*, 2019, p. 72.

²¹⁸¹ Article L.3131-15 du code de la santé publique.

²¹⁸² Article 61 alinéa 2 de la Constitution.

²¹⁸³ Voir : Cons. Const. décision n° 2020-800 DC du 11 mai 2020.

législateur »²¹⁸⁴. A cet égard, le travail des juges constitutionnels consiste principalement à interpréter les dispositions législatives afin de les confronter à la Constitution et de déduire s'il y a violation de la seconde par les premières²¹⁸⁵. Pierre Esplugas-Labatut explique que « dans ce travail, le Conseil utilise [notamment] comme technique de contrôle des objectifs à valeur constitutionnelle »²¹⁸⁶. Alors, « l'objet pour le Conseil constitutionnel est de justifier, par un processus de conciliation entre un droit fondamental et un objectif à valeur constitutionnelle, soit une limitation de ce droit, soit une protection accrue »²¹⁸⁷. Le contrôle de la nécessité des systèmes d'information pour la réalisation de l'objectif à valeur constitutionnel de protection de la santé publique constitue une garantie essentielle pour la préservation des droits fondamentaux des individus. Assurément, les sages de la rue Montpensier s'assurent que l'atteinte portée par le législateur aux droits et libertés des personnes concernées était effectivement utile à l'objectif constitutionnel de protection de la santé publique.

593. Seulement, tous les systèmes d'information créés afin de lutter contre une menace sanitaire n'ont pas à être autorisés par le législateur et, consécutivement, contrôlés par le Conseil constitutionnel²¹⁸⁸. A titre d'illustration, si les traitements SI-DEP, Contact Covid et le dispositif des Passes sanitaire et vaccinal ont été autorisés par le législateur, c'est parce que les premiers atteignent au droit au respect de la vie privée en raison de l'extension légale du partage du secret professionnel médical pendant que les derniers contrevenaient à la liberté d'aller et venir, à la liberté de se réunir ainsi qu'au droit d'expression collective des idées et des opinions²¹⁸⁹. En revanche, il apparaît que l'application TousAntiCovid, mise en œuvre par le ministre chargé de la santé, ne relevait pas du domaine de la loi. En effet, son utilisation

²¹⁸⁴ ESPLUGAS-LABATUT (P.), *Le Conseil constitutionnel*, Dalloz, 9^{ème} ed, novembre 2020, p. 73.

²¹⁸⁵ ESPLUGAS-LABATUT (P.), *op. cit.*, p. 102.

²¹⁸⁶ *Ibid.*

²¹⁸⁷ *Ibid.*

²¹⁸⁸ Voir : CE, 2^e et 7^e ch., 6 novembre 2019, n°434376, Rec. Lebon T. ; JCP A, 2019, n° 46, act. 710, M. Meyer ; Revue Communication Commerce électronique, 2020, n° 04, comm. 37, A. Debet.

²¹⁸⁹ Cons. Const., Décision n° 2021-824 DC du 5 août 2021, cons. 37 : D., 2021, n° 29, p. 1548 ; AJDA 2021, n° 44, p. 2610, note M. Verpeaux ; AJ fam., 2021, n° 09, p. 448, obs. A. Dionisi-Peyrusse.

ne heurte aucun obstacle législatif d'une part, et les caractéristiques techniques de ce traitement permettent de limiter l'atteinte aux droits et libertés des utilisateurs d'autre part²¹⁹⁰.

C'est ainsi que le traitement TousAntiCovid a été autorisé par un acte réglementaire et a échappé au contrôle du Conseil constitutionnel. Bien que l'expertise numérique de l'Institut national de recherche en sciences et technologies du numérique a permis de concevoir un dispositif respectueux de la protection des données personnelles dès la conception du traitement²¹⁹¹, il n'en demeure pas moins que « *l'utilisation des fonctionnalités des applications pour smartphones [...] est susceptible de porter atteinte à l'exercice de certains droits fondamentaux tels que le droit au respect de la vie privée et familiale* »²¹⁹². « *Toute ingérence dans ces droits devant être conforme aux exigences prévues par la loi* »²¹⁹³, la Commission européenne recommandait alors aux Etats membres d'autoriser ces applications mobiles de *contact tracing* par une norme législative. De cette manière, les garanties nécessaires à la protection des droits fondamentaux des utilisateurs auraient pu être définies par la représentation nationale d'une part, et la nécessité de sa mise en œuvre pour la protection de la santé publique aurait pu être contrôlée, en toute indépendance, par les juges constitutionnels d'autre part. Dès lors que les conséquences d'un traitement pour les droits fondamentaux des personnes concernées ne sont pas pleinement maîtrisables, sa création et l'évaluation de son utilité devraient, par précaution, revenir au législateur. En période d'exception comme en temps ordinaires, « *la soumission de l'État moderne à l'État de droit devrait impliquer de soumettre les mesures restrictives des libertés à un contrôle de nécessité et de proportionnalité* »²¹⁹⁴.

²¹⁹⁰ Voir : CE, Ass., 26 octobre 2011, n°317827, *Association pour la promotion de l'image*, Rec. Lebon, 2011, p. 505, concl. J. Boucher ; AJDA, 2011, n° 36, p. 2036, note R. Grand ; LPA, 2011, no 248, p. 10, note F. Chaltiel ; AJDA, 2012, n° 01, p. 35, chron. M. Guyomar et X. Domino.

²¹⁹¹ L'application TousAntiCovid s'appuie sur le protocole ROBust and privacy-presERving proximity Tracing (dit protocole ROBERT) spécifié par l'Institut national de recherche en sciences et technologies du numérique (INRIA) qui intervient en qualité de sous-traitant de ce traitement.

²¹⁹² Recommandation (UE) 2020/518 de la Commission du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées, JOUE L 114/7, 14 avril 2020, cons. 17.

²¹⁹³ Recommandation (UE) 2020/518 de la Commission du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées, JOUE L 114/7, 14 avril 2020, cons. 17.

²¹⁹⁴ ANDRIANTSIMBAZOVINA (J.), *op. cit.*, § 14.

594. *A posteriori*, l'efficacité des systèmes d'information portant atteinte aux droits et libertés des personnes concernées, dans l'intérêt de la protection de la santé publique, réclame d'être évaluée régulièrement. D'abord, l'utilité de ces dispositifs dépend de l'évolution de la situation sanitaire et de l'état des connaissances sur l'origine de la menace. Ensuite, l'appréciation de l'efficacité de ces dispositifs suppose l'examen de leur contribution à la lutte contre la crise sanitaire. A cet égard, le législateur a instauré un *Comité de contrôle et de liaison Covid-19* par la loi prorogeant l'état d'urgence sanitaire²¹⁹⁵. Concrètement, ce comité est « chargé d'associer la société civile et le Parlement aux opérations de lutte contre la propagation de l'épidémie »²¹⁹⁶. A ce titre, il lui appartient de régulièrement évaluer, « grâce aux retours d'expérience des équipes sanitaires de terrain, l'apport réel des outils numériques à leur action, et de déterminer s'ils sont, ou pas, de nature à faire une différence significative dans le traitement de l'épidémie »²¹⁹⁷. Le Comité de contrôle et de liaison Covid-19 a donc rendu des avis ainsi que des points de vigilance relatifs à l'efficacité des différents traitements de données médicales déployés pour lutter contre la pandémie du SARS-CoV-2²¹⁹⁸. En complément, la CNIL a été chargée d'émettre des avis publics trimestriels afin de contrôler périodiquement l'utilité et l'efficacité de ces traitements²¹⁹⁹. De la même façon, il incombe au Gouvernement d'adresser au Parlement un rapport détaillé sur les systèmes d'information mobilisés dans la lutte contre le virus de la Covid-19 « comprenant des indicateurs d'activité, de performance et de résultats quantifiés adaptés aux priorités retenues, tous les trois mois à compter » du 12 mai 2020 « et jusqu'à la disparition des

²¹⁹⁵ Article 11 VIII de la loi n°2020-546 du 11 mai 2020, *loc. cit.*

²¹⁹⁶ Article 11 VIII de la loi n°2020-546 du 11 mai 2020, *loc. cit.*

²¹⁹⁷ Article 11 VIII 1° de la loi n°2020-546 du 11 mai 2020, *loc. cit.*

²¹⁹⁸ CCL Covid-19, Avis du 28 juillet 2021 portant sur le projet de loi n° 4386 relatif à la gestion de la crise sanitaire ; CCL Covid-19, Point de vigilance : Pass sanitaire Covid-19, 20 avril 2021 ; CCL Covid-19, Avis du 9 février 2021 sur les systèmes d'information et campagne de vaccination ; CCL Covid-19, Avis du 15 septembre 2020 : Pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie ; CCL Covid-19, Avis du CCL du 19 octobre 2020 sur les évolutions nécessaires des outils numériques citoyens de lutte contre la Covid-19 ; CCL Covid-19, Avis du 15 Décembre 2020 sur le projet de décret modifiant le décret n°2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid ».

²¹⁹⁹ CNIL, Délibération n° 2020-087 du 10 septembre 2020 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 ; CNIL, Délibération n° 2021-004 du 14 janvier 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 ; CNIL, Délibération n° 2021-062 du 27 mai 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 ; CNIL, Délibération n° 2021-139 du 21 octobre 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19.

systemes d'information développés aux fins de lutter contre la propagation de l'épidémie de covid-19 »²²⁰⁰. En outre, il revient au Conseil scientifique Covid-19 d'adresser des avis au Premier ministre, au Président de l'Assemblée nationale et au Président du Sénat sur l'efficacité de ces dispositifs²²⁰¹. Ultérieurement à la mise en œuvre des traitements aux fins de protection de la santé publique, le contrôle de leur efficacité contre la crise sanitaire n'est effectué qu'à partir de procédés consultatifs. Pourtant, en l'absence de nécessité, l'atteinte aux droits fondamentaux résultant du traitement des données médicales des personnes concernées devient illicite et, *de jure*, disproportionnée.

595. *A posteriori*, l'inefficacité de l'atteinte aux droits fondamentaux des personnes concernées dans l'intérêt public de la lutte contre une menace sanitaire ne peut être dénoncée, à l'initiative du justiciable, que par la juridiction administrative suprême. Les systèmes d'information mis en œuvre pour le compte de l'Etat et concrétisés par le pouvoir exécutif²²⁰² peuvent faire l'objet d'un recours devant le Conseil d'Etat. En effet, le juge administratif a le pouvoir de suspendre ou d'annuler certaines mesures du Gouvernement. A cet égard, il lui appartient « *de faire une balance entre, d'une part, les exigences liées à la protection de la santé, qui se traduisent par des mesures attentatoires aux libertés publiques [...] et les exigences liées à la protection de ces mêmes libertés* »²²⁰³. Seulement, comment la juridiction administrative saurait-elle impartialement se prononcer en qualités de juge suprême et de conseil ? Le contrôle de la légalité des actes réglementaires s'en trouverait-il biaisé ? En guise de réponse, Jean-Denis Combrexelle s'attache à rappeler que « *la vision d'un juge qui devrait être un contre-pouvoir en charge de définir des politiques publiques alternatives à celles du Gouvernement ne correspond pas aux règles fondamentales de la démocratie et de la République* »²²⁰⁴. Par ailleurs, le recours d'un justiciable représente l'occasion, pour la juridiction administrative, de vérifier l'opportunité de son conseil pour l'administration. En outre, lors d'un recours devant le Conseil d'Etat, le justiciable jouit du droit de contourner la théorie de la loi-écran²²⁰⁵ afin de soulever une question prioritaire de constitutionnalité

²²⁰⁰ Article 11 IX de la loi n°2020-546 du 11 mai 2020, *loc. cit.*

²²⁰¹ Article 1 VII de la loi n°2021-689 du 31 mai 2021, *loc. cit.*

²²⁰² Article 31 II de la loi Informatique et Libertés modifiée.

²²⁰³ COMBREXELLE (J.-D.), *Le juge, l'état d'urgence sanitaire et les libertés*, La revue des juristes de sciences po, juin 2021, n°21, Dossier thématique n°09, § 4.

²²⁰⁴ COMBREXELLE (J.-D.), *op. cit.*, § 3.

²²⁰⁵ CE, Section, 6 novembre 1936, *Arrighi et Dame Coudert*, Rec. Lebon, 1936, p. 966.

relative à l'absence de nécessité de l'atteinte aux droits fondamentaux garantis par la Constitution²²⁰⁶. Toutefois, encore faut-il que le traitement de données médicales dont l'atteinte aux droits fondamentaux est injustifiée trouve son assise dans la loi²²⁰⁷ et que le Conseil d'Etat décide, ensuite, de la déférer devant les juges constitutionnels.

Si pour être proportionnée, une mesure doit être indispensablement utile et efficace, il appartient au législateur de concilier, avec équilibre, l'objectif à valeur constitutionnelle de protection de la santé publique avec les droits et les libertés fondamentaux reconnus aux personnes concernées. La proportionnalité a pour effet d'encadrer la marge de manœuvre du législateur dans l'objectivation de ce droit-créance. Nonobstant la gravité de la menace sanitaire, toute atteinte à l'autodétermination informationnelle des citoyens à l'égard de leurs données médicales ne peut donc qu'être proportionnée au droit à la protection de la santé publique.

2. La proportionnalité et la pertinence du fichage des citoyens

596. La démonstration de l'utilité et de l'efficacité d'un traitement de données médicales, pour lutter contre une menace sanitaire, ne suffit pas à légitimer sa mise en œuvre lorsqu'il est prévu par la législation. Alors, « *une fois que la mesure législative [ayant autorisé un traitement de données personnelles] a été jugée nécessaire, il convient de l'examiner à l'aune du principe de proportionnalité* »²²⁰⁸. Ainsi, tout traitement de données personnelles ingérant dans le droit fondamental à la protection des données personnelles et portant atteinte à la vie privée des personnes concernées peut être mis en œuvre à condition que les risques qu'il engendre soient proportionnés à sa finalité²²⁰⁹ ou limités par l'instauration de garanties appropriées²²¹⁰.

²²⁰⁶ Article 61-1 de la Constitution.

²²⁰⁷ Article 11 de la loi n°2020-546 du 11 mai 2020, *loc. cit* ; Article 1 de la loi n° 2021-689 du 31 mai 2021, *loc. cit*.

²²⁰⁸ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 11.

²²⁰⁹ Cf. Paragraphe 600.

²²¹⁰ Cf. Paragraphe 603.

Si le niveau d'acceptabilité de l'atteinte aux droits fondamentaux des personnes concernées par le traitement de leurs données personnelles est davantage étudié sous le prisme du droit de l'Union, c'est parce que le principe de proportionnalité en constitue un principe général. Lors d'un discours prononcé à l'Institut Portalis d'Aix-en-Provence, Jean-Marc Sauvé a rappelé que ce principe de proportionnalité a d'abord été « consacré par la Cour administrative suprême de Prusse dès 1882 »²²¹¹ pour ensuite découler de « l'interprétation des articles 19 et 20 de la Loi fondamentale allemande de 1949 »²²¹². Dorénavant, la *proportionnalité* fait notamment l'objet d'une « utilisation renforcée par l'article 52 de la Charte des droits fondamentaux de l'Union européenne, qui la mentionne expressément sous forme de principe »²²¹³. Bien que le principe de proportionnalité soit largement employé en droit de l'Union, ainsi que par l'ensemble des juridictions nationales des Etats membres, ce principe d'application hétérogène ne connaît aucune définition normative. Rhita Boustia a alors tenté de lui offrir une définition générale. A la lumière des jurisprudences constitutionnelles des pays de l'Union, elle a remarqué que « deux exigences découlent de cette optique finaliste ou téléologique. Tout d'abord, le moyen doit être nécessaire à l'objectif qu'il prétend poursuivre. Ensuite, les conséquences néfastes de la mise en œuvre de ce moyen (ici, l'atteinte aux droits fondamentaux) doivent « correspondre » à l'importance de cet objectif ; autrement dit, plus l'atteinte est grave, plus l'objectif doit être important »²²¹⁴. Plus simplement, selon Jean-Marc Sauvé, le principe de proportionnalité équivaut à « un principe de conciliation permettant d'équilibrer les rapports entre les droits fondamentaux et les objectifs d'intérêt général poursuivis par les autorités étatiques »²²¹⁵. En d'autres termes, « le principe de proportionnalité permet d'opérer une mise en balance, métaphore de la justice, et de réaliser ainsi un équilibre entre chacun des termes de l'équation »²²¹⁶. Cette conciliation est systématique dans l'exécution des objectifs à valeur constitutionnelle²²¹⁷. Il en ressort que dans le contexte d'une menace sanitaire grave, « la mise en œuvre de mesures aux fins de garantir la santé publique ne peut intervenir que dans

²²¹¹ SAUVE (J.-M.), *op. cit.*, p. 10.

²²¹² *Ibid.*

²²¹³ BOUSTA (R.), *Contrôle constitutionnel de proportionnalité. La spécificité française à l'épreuve des évolutions récentes*, Revue française de droit constitutionnel, Vol. 88, 2011, n°04, p. 913.

²²¹⁴ BOUSTA (R.), *op. cit.*, p. 915.

²²¹⁵ SAUVE (J.-M.), *op. cit.*, p. 12.

²²¹⁶ SAUVE (J.-M.), *op. cit.*, p. 10.

²²¹⁷ Cf. Paragraphe 592.

le cadre d'un strict contrôle de proportionnalité au regard des risques sanitaires encourus et des circonstances de temps et de lieu [...] ces exigences s'appliquant de fait aux traitements de données à caractère personnel sous-jacents »²²¹⁸.

597. Dorénavant, Jean-Marc Sauvé a constaté que « *le principe de proportionnalité ne revêt pas qu'une fonction contentieuse permettant au juge d'arbitrer a posteriori entre des principes antinomiques ; il s'applique plus largement à l'ensemble de l'action publique et s'érige en principe de portée générale* »²²¹⁹. En particulier, le principe de proportionnalité a rapidement été intégré au sein du droit à la protection des données²²²⁰ et a directement trouvé un écho dans les principes essentiels édictés à l'article 5 du RGPD. Aussi, le législateur européen annonce 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* »²²²¹. Cette exigence de proportionnalité commande d'être prise en compte dès la conception du traitement de façon à réduire les risques d'atteinte aux droits et libertés des personnes concernées par le traitement de leurs données personnelles. Il en advient que tout traitement de données personnelles doit constituer un moyen strictement nécessaire pour aboutir à la finalité qu'il poursuit. La conformité du traitement au droit à la protection des données personnelles est donc conditionnée par l'application, par le responsable de traitement, du principe de proportionnalité. De la même façon, lorsque le traitement, parce qu'il attente aux droits fondamentaux des personnes concernées, est autorisé par la loi, « *il est de la responsabilité du législateur d'évaluer la proportionnalité* »²²²² de cette mesure législative. Evidemment, « *même le législateur doit le respecter, lorsqu'il édicte les lois* »²²²³ qui tendent à restreindre les droits fondamentaux des individus. Plus qu'un simple mécanisme de contrôle juridictionnel, le principe de proportionnalité s'impose à tout organisme – public ou privé – qui envisage un traitement de données à caractère personnel, *a fortiori* lorsqu'il emporte une réduction des droits à la protection de ces données et au respect de la vie privée.

²²¹⁸ METALLINOS (N.), *op. cit.*, § 7.

²²¹⁹ SAUVE (J.-M.), *op. cit.*, p. 11.

²²²⁰ Convention n° 108 du Conseil de l'Europe sur la protection des données, 28 janvier 1981.

²²²¹ Considérant 4 du RGPD.

²²²² CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 4.

²²²³ SAUVE (J.-M.), *loc. cit.*

598. Alors qu'aucune disposition normative ne définit le principe de proportionnalité, sur quels critères reposent la réalisation d'un test de proportionnalité entre l'atteinte à un droit fondamental et les motifs qui la justifie ? Grâce à l'impulsion des instances européennes, « *les pratiques nationales tendent aujourd'hui à converger dans un mouvement général d'élévation de ce standard de contrôle* »²²²⁴. A cet effet, le Contrôleur européen de la protection des données ainsi que l'Agence des droits fondamentaux de l'Union européenne ont établi une méthodologie fondée sur les jurisprudences de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme. Si Romain Perray avait constaté « *la similitude qui existe entre les différents tests de proportionnalité quelles que soient les dispositions qui les prévoient* »²²²⁵, les Etats membres de l'Union européenne disposent désormais de lignes directrices pour assurer la proportionnalité à laquelle doivent satisfaire toute mesure supposant un traitement de données à caractère personnel entraînant une limitation des droits au respect de la vie privée et à la protection des données personnelles²²²⁶. En vertu d'une approche matérielle de la proportionnalité, il est alors concrètement possible d'évaluer si le traitement massif des données médicales de la majorité de la population d'un Etat est raisonnablement pondérée à l'objectif de lutte contre une menace sanitaire.

599. Le test de proportionnalité, élaboré par le contrôleur européen de la protection des données, se fonde sur quatre conditions cumulatives et chronologiques. Cela signifie que les traitements de données attentatoires aux droits fondamentaux des personnes concernées doivent successivement satisfaire à chacune des étapes de l'évaluation de la proportionnalité. A défaut, l'atteinte qu'il porte aux droits fondamentaux des personnes concernées est réputée disproportionnée. Or, une limitation aux droits au respect à la vie privée et à la protection des données personnelles n'est admissible que dans la mesure où elle respecte l'ensemble de ces exigences.

²²²⁴ SAUVE (J.-M.), *op. cit.*, p. 18.

²²²⁵ PERRAY (R.), *DONNÉES À CARACTÈRE PERSONNEL Principes fondamentaux relatifs aux traitements de données à caractère personnel. – Minimisation*, JurisClasseur Communication, Fasc. 932-30, 19 Juillet 2021, § 21 et § 22.

²²²⁶ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019.

600. En premier lieu, le test de proportionnalité entre un traitement de données personnelles et l'atteinte portée aux droits fondamentaux repose sur l'évaluation de la légitimité et de l'efficacité du traitement. La légitimité s'attache à l'importance des objectifs poursuivis par le traitement alors que son efficacité s'intéresse à son adéquation pour y satisfaire. Bien que cette première étape est similaire à l'évaluation de la nécessité du traitement²²²⁷, il s'agit d'apprécier *in concreto* les mesures permettant au responsable de traitement de réaliser effectivement un objectif impérieux pour l'intérêt général. Le législateur qui autorise le traitement doit d'abord définir l'importance du problème à résoudre ainsi que son degré d'urgence, pour ensuite vérifier que les finalités concrètes du traitement y répondent fondamentalement²²²⁸. Autrement dit, le problème doit être résolu par le biais du moyen. Dans l'hypothèse d'une menace sanitaire grave, les pouvoirs publics doivent urgemment la contenir afin de protéger la santé publique. Cet objectif présente donc une valeur constitutionnelle d'intérêt général qui le légitime. Il appartient ensuite au législateur de s'informer exactement sur les caractéristiques du problème de façon à déterminer les moyens à déployer pour y faire face.

Compte tenu de la révolution numérique engagée par les pouvoirs publics, la création de systèmes d'information est apparue comme une solution essentielle dans la lutte contre la pandémie de la Covid-19. En effet, « *le numérique non seulement a permis d'assurer la continuité de la vie sociale, mais encore il a été largement mobilisé pour lutter activement contre la propagation du virus* »²²²⁹. Notamment, les traitements à des fins d'identification des chaînes de contamination permettent efficacement de lutter contre la propagation d'un virus. Par conséquent, ils concourent directement à l'objectif à valeur constitutionnelle de protection de la santé publique, repris à l'article 35 de la Charte des droits fondamentaux de l'Union européenne. L'atteinte aux droits à la vie privée et à la protection des données constitue alors un besoin social impérieux et adéquat à la lutte contre la menace sanitaire. Certainement, au-delà de la santé, c'est la vie humaine qui est en jeu. L'absence de traitement de données médicales à des fins de *contact tracing* représenterait un dommage pour la société dans la mesure où les personnes à risque de contamination, asymptomatiques ou en période

²²²⁷ Cf. Paragraphes 587 s.

²²²⁸ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 18 à p. 19.

²²²⁹ CLUZEL-METAYER (L.), *La datasurveillance de la Covid-19*, loc. cit.

d'incubation de la maladie, favoriseraient la circulation du virus en entretiendraient le contexte épidémique ou pandémique. Chacune des finalités de ces traitements doivent concrètement poursuivre l'objectif observé comme légitime au risque de créer un « *détournement de la fonction législative* »²²³⁰ et, subséquemment, un détournement de la finalité du traitement. Le cas échéant, l'atteinte aux droits fondamentaux des personnes concernées irait au-delà de ce qui est nécessaire à la réalisation de l'objectif défini, et deviendrait donc disproportionnée.

601. En deuxième lieu, le test de proportionnalité consiste à évaluer « *l'incidence réelle de la mesure sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel* »²²³¹. En d'autres termes, « *la mesure ne doit pas faire porter une charge disproportionnée et excessive sur les personnes concernées par la limitation par rapport à l'objectif recherché* »²²³². Il convient alors de déterminer le niveau d'ingérence du traitement des données personnelles pour les droits fondamentaux des personnes concernées. A travers le RGPD, le législateur européen exige des responsables de traitement qu'ils limitent au maximum les risques pour les intérêts, les droits et les libertés des personnes concernées. Parmi les moyens adéquats pour parvenir à l'objectif poursuivi, doit donc être choisi celui limitant le moins les droits fondamentaux des intéressés²²³³. D'ailleurs, la proportionnalité des risques pour les droits des personnes concernées induits par le traitement de leurs données personnelles est contrôlée à l'occasion de l'AIPD²²³⁴ ; et les mesures correctives pour y faire face doivent être élaborées. Autrement dit, il ne doit pas exister de mesures alternatives moins attentatoires aux droits fondamentaux des citoyens fichés.

²²³⁰ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 18.

²²³¹ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 22.

²²³² Agence des Droits Fondamentaux de l'Union Européenne, *Application de la Charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale*, *op. cit.*, p. 76.

²²³³ BOUSTA (R.), *op. cit.*, p. 920.

²²³⁴ Cf. Paragraphe 567.

Pour réduire l'incidence du traitement sur les droits fondamentaux, la portée de la mesure ayant autorisé le traitement doit d'abord être suffisamment délimitée²²³⁵. Cette stricte limitation des moyens correspond aux différents principes de limitation et de minimisation consacrés à l'article 5 du RGPD. En vertu de leur application, « *les bases de données - SI-DEP et Contact-covid - tout comme l'application StopCovid, mises en place au niveau national, ont indéniablement bénéficié d'une approche « privacy by design » : elles ont été conçues ab initio dans le but de minimiser les atteintes à la vie privée* »²²³⁶. Si le traitement des données médicales des citoyens et des résidents français à des fins de lutte contre une menace sanitaire constitue une atteinte considérable au droit au respect de la vie privée, leur accès est strictement limité aux catégories de professionnels légalement autorisés et nommément habilités sous peine de sanctions pénales²²³⁷. En ce sens, le Conseil d'Etat avait attiré l'attention du Gouvernement « *sur la nécessité de garantir par des mesures particulièrement rigoureuse le respect de la vie privée et la restriction de ces accès aux plus strictes nécessités de la sécurité sanitaire* »²²³⁸. Bien que le législateur ait pris le soin de limiter ces accès, il n'empêche que le nombre de personnes concernées et le nombre d'opérationnels effectuant ces traitements est corrélatif à l'envergure d'une pandémie. Si la portée de l'atteinte est juridiquement circonscrite, un nombre important de professionnels accèdent à un nombre considérable de données médicales personnelles. Il en ressort que l'ampleur de la menace sanitaire retentit sur la portée de l'atteinte à la vie privée des personnes concernées. A l'évidence, « *le traitement centralisé de telles masses de données très sensibles et identifiantes peut être considéré comme largement disproportionné par rapport au problème à résoudre* »²²³⁹. Seulement, plus l'étendue d'une menace sanitaire est grave, plus la mise en œuvre de moyens pour parvenir à l'objectif est impérieuse. La régulation de la limitation de l'atteinte aux droits à la vie privée et à la protection des données personnelles ne peut donc être que relative.

²²³⁵ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 23.

²²³⁶ CLUZEL-METAYER (L.), *La datasurveillance de la Covid-19*, *op. cit.*, p. 919.

²²³⁷ Cf. Paragraphes 562 et 563.

²²³⁸ CE, Avis n° 400104, *loc. cit.*

²²³⁹ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 23.

Ensuite, l'évaluation de l'incidence commande d'analyser en quoi le traitement restreint les droits fondamentaux des personnes concernées. L'impériosité de la lutte contre une menace sanitaire grave réduit l'autodétermination informationnelle des personnes concernées à l'égard de leurs données intimes. En raison de la particularité du contexte de leur production²²⁴⁰, la réutilisation des données médicales nominatives emporte un degré d'intrusion particulièrement fort dans l'intimité de la vie privée des patients. En l'occurrence, les données médicales réutilisées à des fins de lutte contre la propagation du SARS-CoV-2 ont été produites à l'occasion d'actes médicaux de diagnostic tels qu'un examen de dépistage virologique ou immunologique ou à l'occasion d'actes médicaux de prévention tels que la vaccination. Ces traitements de données médicales concernant des personnes placées en état de vulnérabilité tendent à affecter les fondements de la relation médicale²²⁴¹. Alors que les données médicales méritent une protection renforcée eu égard à leur sensibilité, les droits reconnus aux personnes concernées sont réduits à peau de chagrin lorsque le traitement mis en œuvre pour le compte de l'Etat²²⁴² est nécessaire pour des motifs d'intérêt général dans le domaine de la santé publique²²⁴³. L'atteinte à la protection des données et, intrinsèquement, à la vie privée apparaît donc amplement caractérisée. La gravité de cette intrusion, jugée nécessaire pour lutter contre une menace sanitaire, doit être prise en compte dans l'évaluation de l'incidence de la mesure.

Finalement, l'intensité de l'incidence du traitement nécessite d'évaluer les « *effets préjudiciables potentiels de la mesure au-delà du point de vue de la protection de la vie privée et doit donc inclure les risques existant pour d'autres droits fondamentaux* »²²⁴⁴. Alors qu'à première vue les traitements mis en œuvre pour lutter contre une menace sanitaire ne restreignent que les droits à la vie privée et à la protection des données, leurs résultats peuvent, incidemment, impacter les libertés fondamentales des personnes concernées²²⁴⁵. Dans une situation épidémique, les personnes à risque de contamination identifiées *via* le *contact tracing* ont le devoir d'auto-restreindre leur liberté d'aller et venir par l'application

²²⁴⁰ Cf. Paragraphe 15.

²²⁴¹ Cf. Paragraphe 572.

²²⁴² Base légale du traitement conformément à l'article 6.1 e) du RGPD.

²²⁴³ Autorisation de traiter des données sensibles conformément à l'article 9.1 i) du RGPD.

²²⁴⁴ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 23.

²²⁴⁵ Cf. Paragraphes 611 et 612.

d'une mesure d'isolement. Pareillement, l'instauration des Passes sanitaire et vaccinal limite la liberté de circulation à la production de données médicales. Si les traitements à des fins de lutte contre une menace sanitaire grave, *a fortiori* lorsqu'il s'agit d'un virus, se révèlent indispensables pour protéger la santé publique de la société, il en ressort que l'atteinte qu'ils engendrent pour les droits et les libertés des personnes concernées est forte. Toutefois, la confrontation entre les moyens et la fin apparaît-elle équilibrée ?

602. En troisième lieu, le test de proportionnalité « *sert d'instrument pour mettre en balance des intérêts opposés selon des critères rationnels* »²²⁴⁶. Il s'agit alors de confronter les inconvénients engendrés pour la vie privée et la protection des données des personnes concernées avec les bénéfices du traitement pour l'objectif de lutte contre la menace sanitaire en faveur de la protection de la santé publique. L'application du principe de proportionnalité « *doit conduire à une véritable mise en balance des différents intérêts en présence et non à la prédominance systématique des droits fondamentaux sur l'intérêt général* »²²⁴⁷. Cependant, « *l'état d'urgence sanitaire vise à préserver la santé et la vie, deux droits fondamentaux qui semblent avoir une préséance sur les autres libertés* »²²⁴⁸. La sauvegarde de la santé publique et, consécutivement, de la vie humaine saurait-elle pondérer l'entorse aux droits à la vie privée et à la protection des données ?

Alors que la limitation des droits et libertés fondamentaux peut être considérée comme grave, la gravité de l'objectif poursuivi semble contrebalancer les éléments en conflit, et ainsi justifier la mise en œuvre de traitements de données médicales à des fins de lutte contre une menace sanitaire. Tout bien pesé, les charges imposées aux personnes fichées apparaissent mesurées par rapport aux bénéfices apportés par l'objectif visé. En effet, la protection de la santé publique profite à l'ensemble des membres de la société. En fin de compte, la réduction temporaire des droits à la vie privée et à la protection des données personnelles en faveur de la restauration de la santé publique et des libertés semble raisonnablement équilibrée. De surcroît, le législateur européen a pris le soin de préciser que « *le traitement des données à caractère personnel devrait être conçu pour servir*

²²⁴⁶ CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 31.

²²⁴⁷ SAUVE (J.-M.), *op. cit.*, p. 19.

²²⁴⁸ ANDRIANTSIMBAZOVINA (J.), *op. cit.*, § 5.

l'humanité »²²⁴⁹. A ce titre, il a consacré la possibilité de déroger au traitement des données médicales « *lorsque l'intérêt public le commande, notamment [...] à des fins de sécurité, de surveillance et d'alerte sanitaire, de prévention ou de contrôle de maladies transmissibles et d'autres menaces graves pour la santé* »²²⁵⁰. Tandis que l'atteinte au droit à la protection des données est globalement tolérée dans l'hypothèse d'une menace sanitaire grave, la proportionnalité de chaque traitement doit être évaluée, au cas par cas, en fonction des caractéristiques propres à chacun des traitements envisagés ainsi que des circonstances de temps et de lieu. Au demeurant, la conciliation entre le risque pour la santé de la population causé par la catastrophe sanitaire et le respect des droits fondamentaux n'apparaît pas disproportionnée lorsque le respect de l'essence desdits droits est garanti, notamment grâce à l'instauration de mesures appropriées²²⁵¹.

603. En quatrième lieu, lorsque le traitement des données médicales est nécessaire pour la protection de la santé publique, les responsables de traitement ont l'obligation de prendre des « *mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernées* »²²⁵². Ces garanties correspondent aux mesures techniques et organisationnelles appropriées pour garantir le respect des exigences du RGPD ainsi que les droits et libertés des personnes fichées. Assurément, « *la Charte européenne des droits fondamentaux n'a prévu aucune exception à l'application du droit à la protection des données dans un contexte de crise ou d'urgence* »²²⁵³. Bien au contraire, Maximilien Lanna souligne que « *les principes de protection mis en œuvre par le RGPD jouent en théorie le rôle de garde-fou dans la mise en œuvre de traitements de données personnelles et ceux-ci s'opposent à ce que les données soient utilisées de façon disproportionnée* »²²⁵⁴. La proportionnalité d'un traitement de données médicales attentatoires aux droits fondamentaux provient donc, en partie, du respect des principes essentiels du droit à la protection des données personnelles. Certainement, les traitements de données médicales à des fins de lutte

²²⁴⁹ Considérant 4 du RGPD.

²²⁵⁰ Considérant 52 du RGPD.

²²⁵¹ Agence des Droits Fondamentaux de l'Union Européenne, *Application de la Charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale*, Orientations, 2019, p. 76.

²²⁵² Article 9.2 i) du RGPD.

²²⁵³ METALLINOS (N.), *op. cit.*, § 31.

²²⁵⁴ LANNA (M.), *op. cit.*, § 8.

contre une menace sanitaire limitent significativement le droit à la protection des données personnelles – en ce qu’ils restreignent l’autodétermination informationnelle des personnes fichées – mais doivent impérativement être conçus *by design*²²⁵⁵ et *by default*²²⁵⁶. Bien que les droits des personnes fichées sur leurs données personnelles se trouvent manifestement dérisoires, la substance du droit à la protection des données personnelles apparaît, en tout état de cause, préservée. Afin d’assurer le respect des dispositions du RGPD dans le cadre de la pandémie de la Covid-19, « *les interventions récentes, aussi bien de la Commission européenne que du CEPD, sonnent comme une injonction aux autorités publiques non seulement de se conformer au droit de la protection des données personnelles dans leur utilisation des technologies contre le coronavirus, mais de l’utiliser comme un vecteur essentiel de transparence à l’égard de la population et de confiance de la population à leur égard* »²²⁵⁷. En définitive, « *le principe de proportionnalité a partout le même objet : [...] éviter les atteintes qui, par leur caractère excessif ou trop radical, seraient de nature à porter atteinte à la substance même des droits et des libertés* »²²⁵⁸.

604. A l’instar de la nécessité, le principe de proportionnalité doit être apprécié *ex ante*. Evidemment, la proportionnalité est une notion évolutive qui nécessite une évaluation dynamique et continue à la lumière de l’efficience des finalités du traitement pour l’objectif de santé publique poursuivi. C’est pourquoi le principe de proportionnalité doit être couplé à un principe de réalité²²⁵⁹. D’abord, « *la proportionnalité d’une mesure considérée peut être appréciée à différents égards* »²²⁶⁰ : elle peut être temporelle, spatiale ou concerner des catégories d’individus particuliers. Par exemple, le Passe vaccinal s’adresse, entre autres, à des catégories de professionnels particulièrement exposés à des risques de contamination. Aussi, la proportionnalité d’une mesure doit être appréciée en fonction de l’évolution concrète de la gravité de la menace qui a conduit à l’instauration de traitements attentatoires aux droits fondamentaux des personnes concernées. A titre d’illustration, la substitution

²²⁵⁵ La *privacy by design* signifie que la protection des données doit être appliquée dès la conception du traitement de données à caractère personnel.

²²⁵⁶ La *privacy by default* signifie que la protection des données doit être définie, par défaut, conformément aux dispositions du RGPD.

²²⁵⁷ GAVANON (I.), LE MAREC (V.), *loc. cit.*

²²⁵⁸ SAUVE (J.-M.), *op. cit.*, p. 13.

²²⁵⁹ COMBREXELLE (J.-D.), *op. cit.*, § 5.

²²⁶⁰ LEPAGE (A.), *op. cit.*, § 248.

réciproque des Passes sanitaire et vaccinal dépend de la situation sanitaire évaluée en fonction de la circulation virale et des indicateurs sanitaires tels que le taux de vaccination, le taux de positivité aux tests de dépistage, le taux d'incidence ou encore le taux de saturation des lits de réanimation²²⁶¹. En application du principe de proportionnalité, « *le législateur doit [donc] pouvoir suspendre la mesure limitant les droits à la vie privée et à la protection des données à caractère personnel une fois que ce niveau [de menace] diminue* »²²⁶². A cet effet, le législateur devrait déterminer un niveau de menace ainsi qu'un degré d'urgence afin d'en assurer le contrôle. Dès lors que les facteurs de la menace atteindraient les seuils définis, et que le risque ne saurait être suffisamment caractérisé par rapport à la situation sanitaire, les traitements attentatoires aux droits fondamentaux des personnes fichées devraient concomitamment cesser. Certainement, « *une mesure d'interdiction peut être justifiée si elle est provisoire, mais devenir disproportionnée lorsqu'elle est définitive* »²²⁶³. Afin de garantir la temporalité de l'atteinte, les traitements de données médicales pour lutter contre la menace sanitaire doivent être fixés pour une durée déterminée ou, à tout le moins, pour une durée déterminable. Indéniablement, « *si les gouvernements étendent leurs pouvoirs de suivi et de surveillance, alors ces pouvoirs doivent être limités dans le temps et ne doivent pas se prolonger au-delà de la durée nécessaire pour lutter contre le COVID-19* »²²⁶⁴. Dans le cadre d'un contexte exceptionnel, l'atteinte à l'autodétermination informationnelle doit demeurer exceptionnelle.

²²⁶¹ Article 1^{er} II-A de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

²²⁶² CEPD, *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019, p. 18.

²²⁶³ LEPAGE (A.), *loc. cit.*, § 248.

²²⁶⁴ Amnesty International, Déclaration conjointe de la société civile, Le recours aux technologies de surveillance numérique pour combattre la pandémie doit se faire dans le respect des droits humains, 2 avril 2020. Disponible en ligne sur le site [www.amnesty.org]. Consulté le 18 octobre 2021.

B) La temporalité des atteintes portées aux droits fondamentaux de la personne fichée

« La pandémie de COVID-19 ne saurait servir d'excuse à une surveillance illimitée dans le temps. »²²⁶⁵.

605. La temporalité du traitement doit être calquée sur la temporalité de la gravité de la menace sanitaire. Les caractéristiques de la menace sanitaire, couplées aux risques qu'elles présentent pour la santé de la population, sont les éléments qui légitiment l'instauration de systèmes d'information nécessaires pour y faire face, et qui équilibrent l'atteinte portée aux droits fondamentaux des personnes concernées. La durée de ces systèmes d'information doit donc être déterminée en fonction de la résolution de l'objectif visé. Autrement dit, « le maintien du dispositif doit être limité à la durée strictement nécessaire à la réponse à la situation sanitaire exceptionnelle, compte tenu des paramètres épidémiologiques pertinents disponibles, et devra, en tout état de cause, prendre fin dès que cette nécessité disparaîtra »²²⁶⁶. Les atteintes aux droits fondamentaux des personnes concernées doivent être appropriées aux circonstances de la crise sanitaire, ce qui implique qu'il doit y être mis fin dès l'instant où elles ne sont plus indispensables à la satisfaction de cette finalité. Dans le contexte de la lutte contre le SARS-CoV-2, les pouvoirs publics ont alors limité les différents systèmes d'information pour la durée strictement nécessaire à la lutte contre la pandémie de la Covid-19 et, au plus tard, jusqu'au terme du régime de sortie de l'état d'urgence sanitaire²²⁶⁷. La temporalité du régime provisoire de l'état d'urgence sanitaire est censée garantir le caractère éphémère de ces traitements exceptionnels de données médicales.

606. Seulement, la déterminabilité de l'état d'urgence sanitaire, et du régime de sortie de crise, repose sur l'aléa d'une situation sanitaire qui ne semble pouvoir être pleinement maîtrisable. Par conséquent, la durée des systèmes d'information de lutte contre la menace sanitaire en devient vaguement déterminable. En effet, les traitements SI-DEP, Contact Covid et TousAntiCovid auraient initialement dû prendre fin en janvier 2021. Néanmoins,

²²⁶⁵ Amnesty International, Déclaration conjointe de la société civile, Le recours aux technologies de surveillance numérique pour combattre la pandémie doit se faire dans le respect des droits humains, 2 avril 2020. Disponible en ligne sur le site [www.amnesty.org]. Consulté le 18 octobre 2021.

²²⁶⁶ CNIL, Délibération n° 2021-054 du 12 mai 2021, *op. cit.*, cons. 19 et cons. 20.

²²⁶⁷ Article 1 de la loi n°2021-1465 du 10 novembre 2021 portant diverses dispositions de vigilance sanitaire, *JOFR* n°263, 11 novembre 2021, texte n°1.

l'application du régime de l'état d'urgence sanitaire ayant été régulièrement prorogée, la caducité de ces systèmes d'information n'a cessé d'être reportée. C'est ainsi que l'existence du dispositif TousAntiCovid²²⁶⁸ et des systèmes SI-DEP et Contact Covid a été repoussée jusqu'au terme de ce régime, soit au 31 juillet 2022. Sauf à ce qu'ils soient à nouveau prolongés, ces traitements – en théorie provisoires – auront duré pendant plus de deux années.

Pareillement, alors que le Passe sanitaire instauré par la loi du 31 mai 2021²²⁶⁹ devait être limité à la seule période estivale de l'année 2021, sa subsistance – additionnée à la création d'un Passe vaccinal pour les personnes âgées de plus de seize ans²²⁷⁰ – a été étendue jusqu'au 31 juillet 2022²²⁷¹. La persistance de ces Passes aura, à tout le moins, perduré pendant près d'une année. Néanmoins, un amendement adopté par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République a permis d'apporter un cadre plus contraignant à l'utilisation de ces justificatifs sanitaires. L'utilisation de ces Passes « *ne pourra ainsi être mis en œuvre que si la situation sanitaire le justifie au regard de la circulation virale ou de ses conséquences sur le système de santé, appréciées en tenant compte des indicateurs sanitaires tels que le taux de vaccination, le taux de positivité des tests de dépistage, le taux d'incidence ou le taux de saturation des lits de réanimation* »²²⁷². Par suite, du 15 novembre 2021 au 31 juillet 2022, « *le pouvoir réglementaire devra apprécier la nécessité du passe [sanitaire et du passe vaccinal] sous le contrôle du juge* »²²⁷³.

²²⁶⁸ Article 1 du décret n° 2021-1584 du 7 décembre 2021 modifiant le décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « TousAntiCovid », *JORF* n°285 du 8 décembre 2021, texte n° 23.

²²⁶⁹ Article 1 de la loi n° 2021-689 du 31 mai 2021, *loc. cit.*

²²⁷⁰ Article 1 de la loi n° 2022-46 du 22 janvier 2022 renforçant les outils de gestion de la crise sanitaire et modifiant le code de la santé publique, *JORF* n°19, 23 janvier 2022, texte n° 01.

²²⁷¹ Article 2 de la loi n° 2021-1465 du 10 novembre 2021, *loc. cit.*

²²⁷² Exposé sommaire de l'amendement n°344 présenté par Jean-Pierre Pont au sujet de l'article 2 du Texte n° 4574, adopté par la commission, sur le projet de loi portant diverses dispositions de vigilance sanitaire le mercredi 20 octobre 2021.

²²⁷³ Exposé sommaire de l'amendement n°344 présenté par Jean-Pierre Pont au sujet de l'article 2 du Texte n° 4574, adopté par la commission, sur le projet de loi portant diverses dispositions de vigilance sanitaire le mercredi 20 octobre 2021.

In fine, l'ensemble des traitements de données médicales à des fins de lutte contre la menace sanitaire pourraient théoriquement être prorogés jusqu'à la caducité du régime – transitoire – de sortie de l'état d'urgence sanitaire²²⁷⁴.

607. Indépendamment de la pérennisation des dispositions du régime de l'état d'urgence sanitaire²²⁷⁵, les systèmes d'information à des fins de lutte contre la propagation du SARS-CoV-2 doivent être interrompus dès lors qu'ils ne se révèlent plus strictement nécessaires à cet objectif. Si le terme du régime d'exception permet approximativement de borner l'existence de ces systèmes d'information, leur longévité ne doit pas être liée à cette temporalité maximale. C'est pourquoi la CNIL insiste « *pour que la nécessité de ces traitements de données à caractère personnel soit périodiquement réévaluée au vu de l'évolution de l'épidémie et des connaissances scientifiques* »²²⁷⁶. Etant donné que « *les mesures présentées comme « exceptionnelles » en temps de crise sont souvent légitimées et généralisées par la suite* »²²⁷⁷, l'application des principes de nécessité et de proportionnalité s'avère absolument capitale et doit être minutieusement respectée au risque de tomber dans une normalisation des mesures – exceptionnelles – de restriction des droits fondamentaux et des libertés individuelles. Toutefois, si la gravité de la situation sanitaire justifie la nécessité et la proportionnalité d'un régime particulièrement attentatoire aux droits et libertés à tous les niveaux, il est loisible d'imaginer que les outils inscrits au sein de la stratégie sanitaire globale le sont *de facto*. En définitive, et sans compter « *la permanence des dangers et des périls graves qui menacent la vie de la Nation* »²²⁷⁸, les traitements de données médicales des individus pour lutter contre une menace sanitaire grave tendent à s'installer, pour une période illimitée, dans notre société.

608. Compte tenu de ce qui précède, Bruno Py est soucieux de savoir « *si le Covid-19 n'est pas jugulé, si le virus devient récurrent comme la grippe saisonnière, si d'autres virus se manifestent demain, la dérogation [au secret des données médicales] deviendra-t-elle*

²²⁷⁴ Article 2 de la loi n° 2021-1465 du 10 novembre 2021, *loc. cit.*

²²⁷⁵ HENNETTE-VAUCHEZ (S.), *La démocratie en état d'urgence : quand l'exception devient permanente*, Éditions du Seuil, 2022.

²²⁷⁶ CNIL, Délibération n°2020-051 du 8 mai 2020, *op. cit.*, p. 11.

²²⁷⁷ PAWLITSKY (A.), *op. cit.*, § 11.

²²⁷⁸ ANDRIANTSIMBAZOVINA (J.), *op. cit.*, § 5.

*pérenne ? »*²²⁷⁹. Plus globalement, Caroline Zorn signale que « *la question importante est celle d'une pérennisation de ces fichiers géants au-delà de la période d'urgence sanitaire »*²²⁸⁰. Dans l'hypothèse où le degré de menace serait si faible qu'il permettrait de recouvrer les temps ordinaires d'un régime de droit commun, l'identification des personnes infectées et, consécutivement, le *contact tracing* pourraient être réalisés par le biais de la procédure de déclaration des maladies à signalement obligatoire²²⁸¹. Assurément, des dispositifs de surveillance sanitaire intégrant des données médicales nominatives existent déjà dans notre environnement juridique de droit commun²²⁸².

Historiquement, dès la médecine hippocratique, « *la surveillance a d'abord concerné les maladies contagieuses. L'identification des cas et leur isolement de la population non malade a constitué une première démarche pour contrôler les épidémies »*²²⁸³. Dans cette lignée, « *à la fin du XIX^e et au début du XX^e siècle émerge le concept d'hygiène publique, avec la nécessité de protéger les communes des maladies transmissibles, de déclarer les maladies pour exercer une surveillance des malades et des risques épidémiques pour la population »*²²⁸⁴. Dès le milieu du XX^e siècle, la surveillance sanitaire « *a été ensuite étendue à l'ensemble du champ de la pathologie incluant les maladies chroniques, des risques et des expositions aux dangers incluant ceux liés à l'environnement »*²²⁸⁵. Incontestablement, « *l'élément commun à toutes les déclinaisons possibles de la surveillance est son lien direct avec l'action publique »*²²⁸⁶ ; et l'importance des choix en matière de politique de santé publique font que « *de plus en plus d'informations sur l'état de santé de la population sont nécessaires »*²²⁸⁷. Quand bien même la crise sanitaire connexe à la pandémie du SARS-CoV-2 est sans précédent, la surveillance sanitaire des individus et des maladies est loin d'être inédite. Cependant, en raison du développement des technologies de l'information et du numérique, les épidémiologistes Jean-Claude Désenclos et Gilles Brücker préviennent que

²²⁷⁹ PY (B.), *Les épidémies et le secret professionnel*, loc. cit.

²²⁸⁰ ZORN (C.), *État d'urgence pour les données de santé (II) : sidep et contact covid*, loc. cit.

²²⁸¹ Si le SARS-CoV-2 était additionné à la liste des maladies à signalement obligatoire.

²²⁸² Cf. Paragraphe 557.

²²⁸³ DESENCLOS (J.-C.), BRÜCKER (G.), *op. cit.*, p. 79.

²²⁸⁴ *Ibid.*

²²⁸⁵ *Ibid.*

²²⁸⁶ *Ibid.*

²²⁸⁷ DESENCLOS (J.-C.), BRÜCKER (G.), *op. cit.*, p. 93.

« si l'intérêt de la surveillance en santé publique est avant tout de nature collective, l'accès de plus en plus large à des informations à caractère individuel peut aller à l'encontre de l'intérêt des personnes, d'où une nouvelle dimension éthique et déontologique de la surveillance et des systèmes d'information en santé publique »²²⁸⁸. Alors, si le traitement des données médicales des membres de la société est consubstantiel à la protection de la santé publique, il apparaît indispensable d'en concevoir la régulation par-delà les sciences juridiques dont, essentiellement, une redéfinition de l'éthique de la santé publique²²⁸⁹.

609. En tout état de cause, les données personnelles collectées à des fins de lutte contre une menace sanitaire ne peuvent être traitées et conservées que « pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées »²²⁹⁰. A titre d'exemple, les historiques de contacts utiles au *contact tracing* via l'application TousAntiCovid ne peuvent être exploités que pendant la période de contagiosité de l'utilisateur décrétée à 15 jours²²⁹¹. Le Gouvernement a ainsi limité « cette durée à ce qui est strictement nécessaire à l'objectif poursuivi. »²²⁹². Au-delà de ce délai scientifiquement affirmé, leur conservation ne présenterait aucune utilité pour la rupture des chaînes de contamination ; elle deviendrait *de jure* illicite. En dépit de l'extensibilité de la persistance des traitements à des fins de lutte contre une menace sanitaire grave, la durée de conservation des données médicales personnelles des personnes fichées doit être rigoureusement limitée. Malgré un risque d'accoutumance de la population à des mesures de contrôle permanentes²²⁹³, la détermination de la durée au-delà de laquelle les données minimisées doivent être supprimées apporte une garantie contre un fichage globalisé. Au demeurant, si le fichage des membres de la société est corrélatif à la gravité de la menace sanitaire, une coalition citoyenne à son encontre permettrait d'expédier le caractère temporaire de ces fichages exceptionnels. En effet, lorsque la menace sanitaire a pour origine un virus, le comportement de la population peut, selon son mode de transmission, significativement

²²⁸⁸ DESENCLOS (J.-C.), BRÜCKER (G.), *op. cit.*, p. 94.

²²⁸⁹ Cf. Paragraphe 612 s.

²²⁹⁰ Article 5.1 e) du RGPD.

²²⁹¹ Article 3 du décret n°2020-650 du 29 mai 2020, *loc. cit.*

²²⁹² PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 33.

²²⁹³ BOULANGER (A.), *loc. cit.* ; GORI (R.), *Le soin et la démocratie à l'épreuve du totalitarisme sanitaire*, Cliniques méditerranéennes, 2021, n° 103, p. 23 à p. 39.

contribuer à l'endiguer²²⁹⁴. En tant qu'acteurs de la préservation de la santé publique, les membres de la société pourraient, par surcroît, participer à la conception des systèmes d'information nécessaires pour combattre les menaces sanitaires, en gouverner les usages et en encadrer les limites. Dans un contexte de crise sanitaire, la démocratie exige d'être renforcée. En effet, « *la santé publique ne peut plus être l'affaire des seules autorités, elle doit devenir la responsabilité de l'ensemble des acteurs sociaux* »²²⁹⁵.

Paragraphe 2 : L'affermissement de la démocratie sanitaire en faveur de la santé publique

*« La pandémie de la Covid-19 a fait surgir au grand jour la dimension collective de la santé humaine, ce que l'on appelle la santé publique, ainsi que les dilemmes éthiques qu'elle peut soulever. »*²²⁹⁶.

610. La base légale et la finalité des systèmes d'information instaurés pour lutter contre une menace sanitaire tendent à restreindre les droits des personnes concernées sur leurs données médicales²²⁹⁷. En dépit du caractère contraignant des traitements favorables à la protection de la santé publique, il n'en demeure pas moins que leur succès repose indispensablement sur leur acceptation sociale et, consécutivement, sur les actions individuelles et collectives des membres de la société. Evidemment, « *la santé publique ne concerne pas que la société considérée comme objet d'une politique publique ; elle devra aussi son succès à l'attitude de ceux qui composent cette société* »²²⁹⁸. Seulement, il existerait des tensions entre la nature collective de la santé publique et les libertés individuelles de la population à laquelle elle s'adresse. Il est vrai qu'« *une politique de santé publique peut apparaître rapidement comme une politique contraignante pour l'individu, voire «*

²²⁹⁴ Voir : INSERM, *Covid-19 : Suivre l'évolution des connaissances et des comportements de la population*, 30 mars 2020. Disponible en ligne sur le site [www.inserm.fr]. Consulté le 5 novembre 2021.

²²⁹⁵ GRAVEL (S.), DOUCET (H.), BATTAGLINI (A.), LAUDY (D.), BOUTHILLIER (M.-E.), BOUCHERON (L.), FOURNIER (M.), *Éthique et santé publique : Quelle place pour l'autonomie ?*, Responsabilité sociale et éthique de la recherche, Vol. 12, 2010, n° 01, § 19.

²²⁹⁶ CCNE, *Éthique et santé publique*, Avis 137, 20 mai 2021, actu. 02 septembre 2021, p. 6.

²²⁹⁷ Cf. Paragraphe 33.

²²⁹⁸ CCNE, *Éthique et santé publique*, op. cit., p. 13.

liberticide », au nom d'un objectif qu'il ne souhaite parfois ne pas voir se réaliser »²²⁹⁹. Pourtant, la santé publique comporte intrinsèquement une dimension sociale et l'individualisme ne permet guère de soutenir la défense d'une cause commune. C'est pourquoi « *la société tout entière doit être associée à un processus dont l'efficacité dépendra de sa mobilisation* »²³⁰⁰. Les citoyens seraient alors additionnés aux débiteurs du droit-crédence à la protection de la santé publique (A) et devraient, à ce titre, participer à la construction des dispositifs qui en permettent l'objectivation (B). Les citoyens adhèreraient plus favorablement aux traitements de leurs données médicales à des fins de lutte contre une menace sanitaire si leur déploiement était conçu et gouverné par la démocratie sanitaire.

A) *La coopération citoyenne pour la prévention des menaces sanitaires*

611. La crise sanitaire provoquée par la pandémie de la Covid-19 a démontré que l'assouvissement de la protection de la santé publique reposait sur la population pour laquelle la politique de santé était élaborée. Les différents outils déployés pour lutter contre la propagation du SARS-CoV-2, qu'il s'agisse des masques chirurgicaux, des tests antigéniques à orientation rapide, des enquêtes sanitaires, ou encore des dispositifs numériques, ont été créés afin d'être employés par la population à laquelle ils s'adressent. En effet, « *il ne suffit pas de penser les politiques de santé en direction de la société ; il est aussi nécessaire de construire les comportements individuels et collectifs qui, la pandémie et le confinement l'ont montré, sont au cœur de la santé publique* »²³⁰¹. Autrement dit, la capacité d'agir des individus « *dans le collectif et dans la société contribuent à mettre en œuvre une politique de santé publique* »²³⁰².

Il en ressort qu'indépendamment de leur utilité²³⁰³, l'efficacité des systèmes d'information élaborés par les pouvoirs publics résulte principalement des actions individuelles et collectives²³⁰⁴. A titre d'exemple, l'efficacité des dispositifs de *contact*

²²⁹⁹ CCNE, *Éthique et santé publique*, op. cit., p. 13.

²³⁰⁰ CCNE, *Éthique et santé publique*, op. cit., p. 14.

²³⁰¹ CCNE, *Éthique et santé publique*, op. cit., p. 13.

²³⁰² CCNE, *Éthique et santé publique*, op. cit., p. 8.

²³⁰³ Cf. Paragraphe 591.

²³⁰⁴ Cf. Paragraphe 611.

tracing, indispensables à la réduction des chaînes de contamination, dépend de la participation des citoyens. D'abord, l'efficacité du traitement Contact Covid s'appuie sur des enquêtes sanitaires volontaires. En effet, « *le patient peut refuser de révéler l'identité des personnes avec lesquelles il a été en contact, tandis que la personne contactée peut refuser de participer à l'enquête* »²³⁰⁵. Ensuite, le succès de l'application TousAntiCovid dépend de son téléchargement et de son utilisation par les citoyens connectés. Des enquêtes statistiques ont révélé que « *pour être efficace, une application de traçage doit être utilisée par un nombre important de la population estimé, selon les sources, entre 20% et 60%* »²³⁰⁶. S'il apparaît que 84% de la population française était équipée d'un smartphone en 2021²³⁰⁷, « *une efficacité optimale suppose que ce soient les personnes les plus exposées qui adhèrent en nombre à l'application* »²³⁰⁸.

De la même façon, la recherche sur le virus et les moyens de lutter contre sa propagation s'appuie sur une participation citoyenne. En effet, sa mise en œuvre suppose que les personnes concernées ne s'opposent pas à l'intégration de leurs données médicales pseudonymisées au sein du SNDS ainsi qu'à leur réutilisation pour un projet d'intérêt public spécifique²³⁰⁹.

Si les citoyens ne concouraient pas au traitement de leurs données médicales au moyen des systèmes d'information de lutte contre la Covid-19, ces dispositifs deviendraient inefficaces ; s'ils devenaient inefficaces, ils ne seraient pas nécessaires ; s'ils n'étaient pas nécessaires, ils ne pourraient être proportionnés aux atteintes portées aux droits fondamentaux des personnes concernées. Dans l'hypothèse où les membres de la société ne permettraient pas le traitement de leurs données médicales pour lutter contre la menace sanitaire, les systèmes d'information déployés à cet effet ne pourraient donc être licitement mis en œuvre.

²³⁰⁵ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 38.

²³⁰⁶ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 33.

²³⁰⁷ Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, *Enquête sur la diffusion des technologies de l'information et de la communication dans la société française*, Baromètre du numérique, ed. 2021,

²³⁰⁸ PELLEGRINI (F.), SKRZYPNIAK (H.), *op. cit.*, p. 34.

²³⁰⁹ Article 13 du décret n°2020-551 du 12 mai 2020, *loc. cit.*

612. Si un pan de la santé publique repose sur le traitement des données médicales de la population²³¹⁰, et que la réussite de la santé publique dépend des comportements des individus, alors les individus devraient coopérer à la lutte contre les menaces sanitaires par la mise à disposition de leurs données médicales. Ainsi, le succès de la santé publique ne devrait pas uniquement reposer sur la restriction de l'autodétermination informationnelle des personnes concernées, mais résulter d'une mobilisation consciente à une cause commune. Seulement, il existerait des tensions systémiques entre l'objectif à valeur constitutionnelle de protection de la santé publique et les droits et libertés fondamentaux des individus²³¹¹.

Lexicalement, la santé publique, parce qu'elle concerne « *l'ensemble de la population* »²³¹², serait antinomique avec la notion d'individualité. Pourtant, si « *la santé publique a pour objectif de préserver et d'améliorer la santé, prise dans toutes ses dimensions, de la population présente sur le territoire* »²³¹³, c'est qu'elle s'adresse à chaque individualité incluse dans la collectivité. Cependant, si la santé, parce qu'elle est publique, constitue autant un fait social qu'un fait biologique²³¹⁴, sa mise en œuvre nécessite une coopération communautaire. Assurément, « *une bonne santé publique appelle la collaboration des citoyens* »²³¹⁵. Il en résulte que « *la santé publique doit désormais se concevoir avec le recours à la participation citoyenne, exercée à titre individuel ou collectif* »²³¹⁶. Tandis que « *le principe de proportionnalité [...] ne saurait conduire à méconnaître les intérêts généraux dont l'État et les collectivités publiques ont la charge et qui sont, avec les libertés et les droits fondamentaux, les piliers du vivre-ensemble* »²³¹⁷, la protection de la santé publique devrait être objectivée en collaboration avec les membres de la société et en considération de leurs valeurs. La réduction des tensions juridiques entre l'autodétermination informationnelle des personnes concernées et la nécessité d'un partage

²³¹⁰ Cf. Paragraphes 548 et 608.

²³¹¹ GRAVEL (S.), DOUCET (H.), BATTAGLINI (A.), LAUDY (D.), BOUTHILLIER (M.-E.), BOUCHERON (L.), FOURNIER (M.), *op. cit.*, § 2 ; CCNE, *Éthique et santé publique*, *op. cit.*, p. 7.

²³¹² Définition de l'adjectif « public » proposée par le CNRTL. Disponible sur le site [www.cnrtl.fr]. Consulté le 07 novembre 2021.

²³¹³ CCNE, *Éthique et santé publique*, *op. cit.*, p. 9.

²³¹⁴ CCNE, *Éthique et santé publique*, *op. cit.*, p. 10

²³¹⁵ GRAVEL (S.), DOUCET (H.), BATTAGLINI (A.), LAUDY (D.), BOUTHILLIER (M.-E.), BOUCHERON (L.), FOURNIER (M.), *op. cit.*, § 13.

²³¹⁶ CCNE, *Éthique et santé publique*, *op. cit.*, p. 23.

²³¹⁷ SAUVE (J.-M.), *op. cit.*, p. 21.

collectif de leurs données médicales pour la préservation de la santé publique nécessite une conciliation éthique spécifique.

Alors qu'en éthique médicale « *la priorité doit être accordée à l'autonomie de l'individu, [...] la santé publique ne peut y reconnaître la même importance, celle-ci étant responsable de promouvoir la santé des populations* »²³¹⁸. Bien qu'ils puissent être repris, les principes éthiques d'autonomie, de justice, de bienfaisance et non-malfaisance propres à la bioéthique n'apparaissent pas adaptés aux particularités de la santé publique. Suite à la pandémie de la Covid-19, le Conseil consultatif national d'éthique a alors ébauché trois « *nouveaux repères éthiques, spécifiques à la santé publique* »²³¹⁹ qui ont vocation à dessiner un cadre applicable à la gestion de toute menace sanitaire, qu'elle soit ponctuelle ou durable, urgente ou latente.

613. Premièrement, la coopération citoyenne pour la prévention des menaces sanitaires devrait être fondée sur la conciliation entre l'autonomie individuelle et la responsabilité collective. Ainsi, l'exploitation des données médicales personnelles dans la gestion d'une crise sanitaire devrait davantage procéder d'une responsabilisation que d'une contrainte. Certainement, « *si parfois il peut y avoir des limites imposées à l'autodétermination d'individus, la thèse centrale [soutenue par Jonathan Mann] consiste plutôt à affirmer les conséquences néfastes sur la santé des atteintes aux droits* »²³²⁰ fondamentaux des personnes concernées. A l'inverse, la préservation de leur autodétermination informationnelle encouragerait l'acceptabilité sociale des politiques de santé publique non coercitives. De surcroît, « *responsabiliser et susciter un engagement personnel peuvent conduire à changer les attitudes* »²³²¹. Conjointement, la responsabilisation et l'autonomisation des individus promeuvent « *la participation citoyenne* »²³²² à la santé publique. Néanmoins, la préservation de l'autonomie des individus n'empêche le paternalisme des pouvoirs publics afin

²³¹⁸ GRAVEL (S.), DOUCET (H.), BATTAGLINI (A.), LAUDY (D.), BOUTHILLIER (M.-E.), BOUCHERON (L.), FOURNIER (M.), *op. cit.*, § 27.

²³¹⁹ CCNE, *Éthique et santé publique*, *op. cit.*, p. 6.

²³²⁰ GRAVEL (S.), DOUCET (H.), BATTAGLINI (A.), LAUDY (D.), BOUTHILLIER (M.-E.), BOUCHERON (L.), FOURNIER (M.), *op. cit.*, § 43.

²³²¹ CCNE, *Éthique et santé publique*, *op. cit.*, p. 18.

²³²² GRAVEL (S.), DOUCET (H.), BATTAGLINI (A.), LAUDY (D.), BOUTHILLIER (M.-E.), BOUCHERON (L.), FOURNIER (M.), *op. cit.*, § 43.

d'augmenter les conséquences positives pour la santé publique²³²³. Partant, la responsabilisation des personnes concernées pourrait induire des comportements favorables pour la santé publique qui seraient exprimés à travers leur autodétermination informationnelle. Alors, les citoyens sensibilisés aux enjeux liés à une menace sanitaire pour la santé publique contribueraient davantage à la défense d'une cause collective en toute indépendance. Par l'exercice de leur autodétermination informationnelle, les citoyens pourraient alors affirmer leur volonté de participer à la protection de la santé publique par la communication de leurs données médicales à des fins de lutte contre une menace sanitaire.

A titre d'illustration, tout à chacun pourrait spontanément aider à la surveillance de la pandémie à l'échelle de la France métropolitaine en participant à un recueil hebdomadaire de données épidémiologiques par l'Internet et de façon anonyme *via* le dispositif Covidnet.fr. Ce projet de datasurveillance a été créé en janvier 2012 par l'Inserm, l'université de la Sorbonne et Santé publique France afin de suivre l'évolution du virus de la grippe avant d'être étendu à la surveillance du SARS-CoV-2. Ce dispositif s'appuie sur la participation volontaire de la population qui n'aurait pas été prise en charge par le système de santé et qui, *de facto*, n'aurait pas été comptabilisée grâce aux méthodes de datasurveillance ordinaires. L'autodétermination informationnelle des personnes concernées coïnciderait donc avec l'objectif à valeur constitutionnelle de protection de la santé publique, et favoriserait même son efficacité. Toutefois, « *assumer sa responsabilité implique d'avoir pris conscience des risques liés à certains comportements et de faire les meilleurs choix pour préserver sa santé et celle des autres* »²³²⁴. L'acceptabilité sociale de la santé publique et la responsabilisation de la population passent donc par l'information. Pour dire les choses autrement, Caroline Lequesne Roth explique que « *volonté et consentement doivent nécessairement entrer en résonance avec les principes de transparence et de responsabilité* »²³²⁵.

614. C'est pourquoi le deuxième principe éthique en matière de santé publique repose sur l'équité dans l'accès aux ressources et, principalement, à l'information. Si « *la santé publique, parce qu'elle est populationnelle, doit faire l'objet d'une diffusion*

²³²³ CCNE, *Éthique et santé publique*, *op. cit.*, p. 19.

²³²⁴ CCNE, *Éthique et santé publique*, *op. cit.*, p. 18.

²³²⁵ LEQUESNE ROTH (C.), *loc. cit.*

populationnelle »²³²⁶, il n'en demeure pas moins que l'ensemble des membres de la société n'est pas en mesure d'en appréhender l'enseignement. C'est pourquoi la communication relative aux enjeux de la santé publique doit allier les principes de transparence, de complexité et de clarté. En effet, il ne s'agit pas de vulgariser l'information au point de vider les enjeux de toute leur substance, ni de diffuser une information qui ne puisse être saisie que par la proportion de la population déjà encline à adopter un comportement vertueux pour la santé publique. L'autonomisation et la responsabilisation des citoyens et des résidents français commandent alors d'offrir à tous un accès proportionné à l'information relative à la santé publique. Cela signifie que l'ampleur et l'intensité des campagnes d'information devraient être déterminées en fonction du niveau de défaveur sociale des sous-groupes de la société²³²⁷. En outre, il apparaît globalement nécessaire d'acculturer l'ensemble de la population à la santé publique « *extrêmement tôt, à des âges où l'on est prêt à adhérer à une logique de pensée de prévention* »²³²⁸. Par-delà l'enseignement scolaire, l'instruction de la santé publique devrait être intégrée dans l'éducation populaire afin d'être diffusée, à tous les niveaux, par « *tous ceux qui sont professionnellement en contact avec les personnes et les familles : élus locaux, responsables associatifs, enseignants, travailleurs sociaux, professionnels de santé, etc.* »²³²⁹. En l'occurrence, le manque de clarté associée à la contradiction des explications gouvernementales relatives aux stratégies de lutte contre la pandémie de la Covid-19 ont conduit à une méfiance des membres de la société. Seulement, comment expliquer un nouveau phénomène que l'on ne maîtrise pas ?

Selon le CCNE, la communication sur la santé publique devrait également inclure la relativité et les limites du savoir relatif aux sciences médicales²³³⁰. L'ouverture des données statistiques et des modèles épidémiologiques à l'appui desquels les décisions publiques ont été fondées devrait être systématisée afin d'éclairer la politique de santé et d'alimenter le

²³²⁶ CCNE, *Éthique et santé publique, op. cit.*, p. 29.

²³²⁷ CCNE, *Éthique et santé publique, op. cit.*, p. 21.

²³²⁸ ANSOBORLO (M.), BELART (A.), FAUSSAT (C.), FLORENCE (A.-M.), DE LAFFOREST (S.), DIOT (P.), *Pourquoi et comment donner un nouvel élan à la santé publique en France ?*, La Presse Médicale Formation, Vol. 2, 2021, n°01, Partie 2, p. 4.

²³²⁹ DESCHAMPS (J.-P.), FERRON (C.), ALLA (F.), DOUILLER (A.), *L'éducation pour la santé, parent pauvre de la politique de santé ?*, Santé Publique, Vol. 25, Supp 2013, n° 02, p. 81.

²³³⁰ CCNE, *Éthique et santé publique, op. cit.*, p. 15.

débat démocratique²³³¹. Le cas échéant, « *cette publication devrait s'accompagner d'une communication forte expliquant les biais et hypothèses du modèle, afin d'éviter une mauvaise compréhension du public* »²³³². Si la communication permettait de gagner la confiance, les citoyens ne résisterait pas au traitement de leurs données médicales pour un motif d'intérêt général. Selon la position du Comité européen de la protection des données, l'autonomisation des individus et la transparence des pouvoirs publics des Etats membres « *permettent d'espérer une Union fédératrice de ses peuples autour de valeurs respectueuses des droits et libertés fondamentaux, facteurs de création et de dynamisme* »²³³³. Il en ressort que le CEPD prône également le « *concept rousseauiste de contrat social fondé sur l'adhésion citoyenne aux contraintes du vivre-ensemble* »²³³⁴.

615. Troisièmement, la coopération pour la prévention des menaces sanitaires devrait être fondée sur la solidarité des citoyens en leur qualité d'acteurs de la santé publique. En ce sens, le CCNE souligne que la santé publique « *ne repose pas seulement sur des principes appliqués à la « population », mais sur les comportements collectifs eux-mêmes* »²³³⁵. Afin de développer le pouvoir d'agir de chaque citoyen, le CCNE propose d'inscrire la santé publique parmi les choses communes à co-construire de façon participative²³³⁶. A cet effet, cette chose publique commune serait intégrée au processus démocratique de sorte que les citoyens puissent directement édifier les valeurs de la santé publique, en orienter les politiques et en créer les outils d'objectivation pratiques. La rénovation de la démocratie sanitaire deviendrait ainsi le levier de l'action collective, de la confiance, de l'acceptabilité et de l'efficacité des dispositifs de santé publique²³³⁷. Compte tenu de la durabilité de la crise sanitaire liée à la pandémie de la Covid-19 et de la gravité des risques sanitaires émergeant de la crise environnementale, de l'effondrement de la biodiversité et de l'imbrication des

²³³¹ BOTHOREL (E.), COMBES (S.), VEDEL (R.), *Pour une politique publique de la donnée*, décembre 2020, p. 43 et p. 47.

²³³² BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, p. 47.

²³³³ GAVANON (I.), LE MAREC (V.), *loc. cit.*

²³³⁴ *Ibid.*

²³³⁵ CCNE, *Éthique et santé publique*, *op. cit.*, p. 21

²³³⁶ *Ibid.*

²³³⁷ ANSOBORLO (M.), BELART (A.), FAUSSAT (C.), FLORENCE (A.-M.), DE LAFFOREST (S.), DIOT (P.), *op. cit.*, p. 3.

écosystèmes du vivant, il apparaît urgent de prévenir ces menaces et d'anticiper la gestion de nouvelles crises grâce à la coopération citoyenne et, notamment, au moyen du numérique.

S'il est évident que les technologies du numérique ne constituent pas la solution à chaque problème, et qu'il convient de veiller au risque d'accoutumance et de banalisation des dispositifs attentatoires à la vie privée²³³⁸, le numérique est devenu un élément central de l'exercice de la santé publique dans les sociétés contemporaines²³³⁹. Dès à présent, l'application de la démocratie de la santé publique exige que les outils numériques permettant la gestion des menaces sanitaires fondés sur le traitement des données médicales des citoyens soient conçus et gouvernés en collaboration avec les membres de la société.

B) La coconstruction citoyenne des dispositifs numériques de lutte contre les menaces sanitaires

616. L'objectivation de la santé publique nécessite de mettre en place un ensemble cohérent de mesures et de moyens en mobilisant des compétences multidisciplinaires²³⁴⁰ tout en enrôlant la participation citoyenne. La santé publique, parce qu'elle s'exprime à travers la capacité d'agir de chacun des membres de la société, apparaît consubstantiellement démocratique. Bien que la France ait principalement opté pour une conception verticale des systèmes d'information de lutte contre la pandémie de la Covid-19, les dispositifs numériques mis en œuvre pour le compte de l'Etat devraient être développés en collaboration avec la société civile. Alors que « *les choix que réaliseront nos dirigeants dans les outils de gestion numérique de la crise constitueront, même sous le sceau de l'exceptionnalité, un jalon de la gouvernance numérique des outils de demain* »²³⁴¹, Caroline Lequesne Roth forme également « *le vœu que le gouvernement inscrive le service numérique de santé publique dans la permanence démocratique d'une technologie responsable* »²³⁴². En application des principes éthiques de la santé publique, la coconstruction citoyenne des dispositifs numériques de gestion des menaces sanitaires améliorerait la compréhension, la confiance ainsi que

²³³⁸ CNIL, Délibération n° 2021-097 du 6 août 2021, *loc. cit.*

²³³⁹ CCNE, *Éthique et santé publique, op. cit.*, p. 11 à p. 12.

²³⁴⁰ CCNE, *Éthique et santé publique, op. cit.*, p. 9.

²³⁴¹ LEQUESNE ROTH (C.), *loc. cit.*

²³⁴² *Ibid.*

l'acceptabilité du traitement des données médicales des personnes fichées. Si la France affirmait son indépendance technologique²³⁴³, cette souveraineté numérique devrait donc revêtir un caractère populaire.

617. Tandis que pour lutter contre le virus de la Covid-19 « *le gouvernement français a fait le choix d'adopter des dispositifs centralisés et contrôlés par des autorités publiques* »²³⁴⁴, les nouveaux outils numériques de gestion des menaces sanitaires devraient être décentralisés et contrôlés par la démocratie sanitaire. Si tout professionnel compétent dans le domaine du numérique est libre de mettre en œuvre un traitement de données médicales à des fins d'intérêt public dans le domaine de la santé publique indépendamment des pouvoirs publics²³⁴⁵, les traitements mis en œuvre pour le compte de l'Etat devraient être coconstruits avec la société civile. Cette décentralisation pourrait être consécutive à un appel d'offre ou naître d'une initiative individuelle ou collective. Le cas échéant, un partenariat entre l'administration et le coconstructeur du système d'information devrait être conclu dès sa conception et préalablement à son autorisation par décret en Conseil d'Etat²³⁴⁶.

Bien que le développement du dispositif numérique soit le fruit d'une coopération citoyenne impliquant des acteurs du secteur privé, les codes sources de ce programme informatique devraient, au nom de la démocratie sanitaire, faire l'objet d'une diffusion automatique en raison de leur motif d'intérêt général pour la santé publique²³⁴⁷. Alors que la notion de données et de codes sources d'intérêt général commence à être reconnue par la législation²³⁴⁸, la crise sanitaire en est apparue comme un accélérateur. D'une part, l'ouverture des codes sources des dispositifs numériques de santé publique affirmerait les principes de transparence et de complexité. Certainement, cette communication encouragerait l'explicabilité des logiques sous-jacentes au traitement des données intimes des personnes fichées par leurs coconstructeurs. Si la loi des algorithmes et leurs impacts sur la société étaient expliqués en toute clarté, les membres de la société coopéreraient plus

²³⁴³ Cf. Paragraphe 619.

²³⁴⁴ CLUZEL-METAYER (L.), *La datasurveillance de la Covid-19, op. cit.*, p. 920.

²³⁴⁵ Article 9.2 i) du RGPD.

²³⁴⁶ Article 31 II de la loi Informatique et Libertés modifiée.

²³⁴⁷ Voir : BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, Partie 5.

²³⁴⁸ Section 2 de la loi n°2016-1321 du 7 octobre 2016, *loc. cit.*

sereinement à la prévention des menaces sanitaires au moyen du traitement de leurs données médicales. D'autre part, cette ouverture emporterait un droit à la réutilisation des codes sources. L'innovation des technologies numériques serait alors stimulée par la contribution des actions individuelles et collectives. La coconstruction horizontale des dispositifs de lutte contre les menaces sanitaire par l'administration et les citoyens ainsi que la diffusion de leur langage de programmation constitueraient donc un cercle vertueux pour la santé publique.

618. Toutefois, la coconstruction citoyenne des dispositifs numériques de lutte contre les menaces sanitaires exige, au préalable, la réutilisation des données médicales pseudonymisées intégrées dans le domaine commun informationnel. Certainement, le développement des dispositifs numériques en santé, leur entraînement et leur performance nécessitent des jeux de données médicales pseudonymisées « *réelles, [et] représentatives des situations opérationnelles d'emplois* »²³⁴⁹. En effet, « *des données reconstituées peuvent entraîner des biais dans l'algorithme affectant la qualité du développement et in fine la confiance mise dans l'outil* »²³⁵⁰.

Alors que le patient ne peut empêcher l'intégration de ses données médicales dans la base principale du SNDS²³⁵¹, le législateur a néanmoins concédé le droit, pour les personnes fichées au sein des outils SI-DEP et Contact Covid, de s'opposer à l'intégration de leurs données médicales et de santé au sein de ce système²³⁵². Pourtant, ces informations représentent un enjeu incontournable pour la recherche sur le SARS-CoV-2 ainsi que pour le développement des dispositifs pratiques de lutte contre sa propagation. En effet, « *plus l'on aura de données sur le phénomène, sur les patients et leurs contacts, plus la compréhension et la lutte contre le virus seront efficaces* »²³⁵³. La question de l'ouverture de ces données pseudonymisées en raison de leur motif d'intérêt général pour la santé publique se pose alors naturellement²³⁵⁴. Toute information répondant à la définition que nous concédons à la chose anthropomorphe devrait intégrer le domaine commun informationnel afin d'être

²³⁴⁹ BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, p. 125.

²³⁵⁰ *Ibid.*

²³⁵¹ Article R.1461-9 II 1° du code de la santé publique.

²³⁵² Article 7 de la loi n°2021-689 du 31 mai 2021, *loc. cit.*

²³⁵³ CLUZEL-METAYER (L.), *La datasurveillance de la Covid-19, op. cit.*, p. 918

²³⁵⁴ Voir : BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, Partie 5.

réutilisée, de façon pseudonymisée, pour tout projet présentant un motif d'intérêt public. Une mise à disposition simplifiée des choses anthropomorphiques par la création d'un domaine commun informationnel consoliderait la souveraineté numérique, laquelle se révèle être gage d'éthique et de sécurisation juridique.

619. Lucie Cluzel-Métayer n'a pas manqué de remarquer que « *la lutte contre le coronavirus a manifestement accentué ce phénomène de dépendance numérique des États* »²³⁵⁵. Cette souveraineté numérique doit être appliquée du recueil des données médicales nécessaires à la conception du dispositif numérique jusqu'à l'hébergement du serveur et des données qu'ils traitent²³⁵⁶. Seulement, des chercheurs privilégient la réutilisation de données de santé étrangères²³⁵⁷ pendant que les autorités administratives recourent aux services d'hébergement proposés par des sociétés établies en dehors de l'Union européenne²³⁵⁸. Eu égard à ces constatations, le Gouvernement révélait, en décembre 2020, qu'il souhaitait voir émerger des initiatives françaises innovantes et conformes à nos valeurs et choix de société²³⁵⁹. Il en advient que la souveraineté du numérique en santé dépend de la participation citoyenne à la santé publique. La nouvelle éthique de la santé publique devrait alors comprendre les principes éthiques propres au numérique. En effet, si la coconstruction citoyenne des dispositifs de lutte contre les menaces sanitaires permettait de réduire la méfiance à l'égard de l'exploitation des données médicales des membres de la société, l'inclusion de l'éthique du numérique en santé soutiendrait davantage la coopération citoyenne pour la santé publique. Les acteurs numériques de la santé publique devraient alors

²³⁵⁵ CLUZEL-METAYER (L.), *La datasurveillance de la Covid-19*, *op. cit.*, p. 920.

²³⁵⁶ MARTIAL-BRAZ (N.), *Nos données de santé en danger... Quand l'arbre de la crise sanitaire cache la forêt de la perte de souveraineté !*, In *Le droit face au coronavirus, Comment une pandémie inédite à mis à l'épreuve notre système juridique*, LexisNexis, 2021, p. 829 à p. 831.

²³⁵⁷ BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, p. 39.

²³⁵⁸ CJUE, 16 juillet 2020, *Data Protection Commissioner c/ Facebook Ireland Ltd, Maximillian Schrems*, aff. C-311/18 : JCP G, 2020, n° 41, 1116, note N. Martial-Braz ; Dalloz actu., 2020, obs. C. Crichton ; D., 2020, p. 2432, note C. Castets-Renard ; AJ contrat, 2020, p. 436, obs. T. Douville ; Dalloz IP/IT, 2020, p. 640, obs. B. Bertrand et J. Sirinelli ; RTD eur., 2021, p. 175, obs. B. Bertrand ; LPA, 2020, n° 243, p. 08, A. Rolin ; CE, ord., 19 juin 2020, n° 440916, Inédit Rec. Lebon ; AJDA, 2020, n° 23, p. 1262, note M.-C. De Montecler ; RLDI, 2020, n° 172, 5904, obs. L. Costes ; Arrêté du 9 octobre 2020 modifiant l'arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé ; CE, ord., 13 octobre 2020, n° 444937, Inédit Rec. Lebon ; JCP A, 2021, n° 21, chron. 2163, J.-C. Videlin ; JCP A, 2021, n° 03, chron. 2019, L. Paravano et J.-L. Sauron ; Dalloz IP/IT, 2020, n° 11, p. 590, obs. N. Maximin ; AJDA, 2021, n° 13, p. 741, note L. Cluzel-Métayer ; RLDI, 2020, n° 176, comm. F. Zannotti et P. Navarro ; Dalloz IP/IT, 2021, n° 02, p. 103, obs. O. De Maison Rouge.

²³⁵⁹ BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, p. 132.

s'engager à respecter des valeurs dont « *la confidentialité et l'intégrité des données de santé, la sécurité et la transparence de leurs traitements informatiques, le respect de l'information du patient, le développement de solutions visant à réduire les fractures numériques, mais également la sobriété numérique et la réduction de l'impact environnemental des systèmes d'information de santé dans un objectif d'engagement pour le développement durable de l'ensemble des acteurs de l'écosystème* »²³⁶⁰. Si les concepteurs des futurs dispositifs numériques étaient tenus au respect de ces règles, il appartiendrait également à leurs utilisateurs d'adhérer à ce socle de principes.

620. En effet, l'ensemble des dispositifs numériques de lutte contre une menace sanitaire n'auront pas vocation à être utilisés par les membres de la société. Les systèmes d'information développés grâce à la mobilisation citoyenne seraient principalement destinés aux pouvoirs publics, aux professionnels de santé ou à l'administration hospitalière. Des outils algorithmiques pourraient les aider à « *repérer plus précocement et de prendre des décisions de gestion de risques épidémiques* »²³⁶¹, à analyser le suivi épidémiologique afin de modéliser des scénarii sanitaires, à anticiper l'afflux hospitalier massif afin de mobiliser les professionnels de santé, ou encore à répartir les patients dans les services adéquats en fonction d'une analyse de risque sémiologique afin de sécuriser le protocole sanitaire. D'ailleurs, dès le mois de mars 2020, des initiatives citoyennes ont point.

D'abord, le dispositif *OpenCovid* porté par Thomas Landrain consiste en une « *organisation informelle issue de la société civile dont l'objet est de consolider des données et de proposer des outils de visualisation concernant l'épidémie de COVID19 en France* »²³⁶². Cette plateforme de recherche participative est ouverte à toute personne désirant élaborer des solutions pour lutter contre la pandémie de la Covid-19 quelle que soit sa profession ou sa qualification. Egalement, l'ingénieur en informatique Guillaume Rozier a créé le dispositif *CovidTracker* permettant de suivre l'évolution de la pandémie du SARS-CoV-2 en France et dans le monde grâce à des graphiques élaborés à partir des données issues de Santé publique

²³⁶⁰ Agence du numérique en santé, *Pourquoi éthique et numérique ?*. Disponible en ligne sur le site [esante.gouv.fr]. Consulté le 05 novembre 2021.

²³⁶¹ CCNE, *Numérique & Santé Quels enjeux éthiques pour quelles régulations ?*, 19 novembre 2018, p. 25.

²³⁶² BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, p. 44.

France, de l'Institut National de la Statistique et des Études Économiques et du *Center for Systems Science and Engineering* de l'Université John Hopkins²³⁶³.

Au demeurant, ces initiatives citoyennes, développées indépendamment de la stratégie sanitaire étatique, ne disposent pas d'une gouvernance établie démocratiquement. Il semble alors fondamental de préciser que les solutions numériques contre la menace sanitaire devraient être implémentées en réponse à la politique de santé orientée démocratiquement. En ce sens, le CCNE considère que la réalisation des objectifs de la santé publique implique de constituer une politique publique impliquant une participation sociale²³⁶⁴. Egalement, la conception de ces dispositifs numériques devraient être gouvernée selon des référentiels juridiques, éthiques et techniques élaborés démocratiquement. Il apparaît donc urgent de définir le cadre d'un développement technologique raisonnable plutôt que de créer des dispositifs numériques à la hâte au risque d'engendrer une méfiance de la population et des effets négatifs sur la santé publique.

621. Bien que les traitements mis en œuvre pour le compte de l'Etat soient pilotés par les pouvoirs publics, l'exercice de la démocratie sanitaire exigerait que les dispositifs numériques puissent être développés horizontalement sous l'égide de la société civile. Or, « *la consultation de l'ensemble de la société lors de la crise sanitaire liée à la Covid-19 s'est révélée insuffisante, défailante* »²³⁶⁵. Pourtant, « *la société aurait probablement gagné en confiance tant dans les responsables de la politique de santé que dans la médecine, si elle avait été associée aux réflexions, aux doutes, puis aux orientations et décisions pendant cette période* »²³⁶⁶. A l'avenir, une représentation de la citoyenneté devrait coconstruire, avec les pouvoirs publics, un cahier des charges détaillant l'ensemble des principes devant être appliqués à chaque outil numérique. Ainsi, les règles à respecter par les concepteurs issus de la société civile seraient déterminées par la société civile elle-même. Ces instructions pourraient notamment adapter la lecture des critères de nécessité et de proportionnalité des traitements attentatoires aux droits à la vie privée et à la protection des données en fonction d'une graduation de la gravité de la menace sanitaire. Ce cahier des charges pourrait

²³⁶³ Disponible sur le site [covidtracker.fr].

²³⁶⁴ CCNE, *Éthique et santé publique*, op. cit., p. 4.

²³⁶⁵ CCNE, *Éthique et santé publique*, op. cit., p. 27.

²³⁶⁶ *Ibid.*

également déterminer les principes éthiques du numérique en santé publique de façon à ce qu'ils soient impérieusement appliqués dès la conception des traitements et par défaut. Avant d'être adoptée par le gouvernement et, le cas échéant, débattue par la représentation nationale, l'autorisation des dispositifs numériques élaborés par la société civile pourrait être soumise à l'avis consultatif de la représentation citoyenne à l'instar du Comité de contrôle et de liaison Covid-19²³⁶⁷ ou de l'hypothétique *Comité citoyen pour la protection de l'intérêt public de l'innovation médicale*²³⁶⁸.

622. Par ailleurs, la société civile devrait définir les limites socialement acceptables aux atteintes aux droits fondamentaux dans l'espoir de privilégier l'autodétermination informationnelle et l'autonomisation de la participation citoyenne à la santé publique. L'ensemble des membres de la société devrait alors contribuer à la détermination des actions d'éducation à la santé publique dans l'intention particulière de prendre en compte les diversités, de résorber les inégalités et, subséquemment, de responsabiliser chacun à la préservation de notre bien commun par la mise à disposition de sa chose anthropomorphique.

²³⁶⁷ Cf. Paragraphe 594.

²³⁶⁸ Cf. Paragraphe 540.

Conclusion du chapitre

623. Le traitement des données médicales nominatives, pseudonymisées ou anonymisées d'une population touchée par une menace sanitaire semble incontournable à la préservation de la santé publique. Il permet, entre autres, d'observer son évolution afin d'adapter la stratégie sanitaire, d'identifier les personnes physiques affectées afin d'adapter des mesures de prévention individuelles et collectives ou de sécuriser des espaces où le risque sanitaire serait atténué. A titre exceptionnel, les technologies de l'information et de la communication constituent un outil performant pour examiner et partager, en un temps record, une quantité considérable d'informations relatives à la quasi-totalité des membres de la société. Toutefois, il importe de tenir compte de la multiplicité des risques induits par le fichage généralisé des choses anthropomorphiques d'une population. Leur exploitation porte une véritable atteinte à l'intimité de la vie privée des personnes fichées et comporte des dangers sécuritaires inhérents au numérique. Par surcroît, l'embuche la plus redoutable réside dans le basculement insidieux et progressif vers une datasurveillance banalisée et pérennisée. L'existence de ces risques engendre naturellement des craintes emportant la méfiance, et parfois la défiance, des personnes fichées. Pourtant, le droit à la protection des données personnelles s'attache à encadrer ces traitements de données médicales personnelles consubstantiels à la gestion des menaces sanitaires qui sont, au demeurant, autorisés légalement. Si la datasurveillance constitue une pratique essentielle à la santé publique, la systématisation du fichage populationnel ne devrait jamais être considérée comme une solution universelle à tous les maux.

624. Tandis que la gravité du contexte sanitaire légitime une restriction légale des droits ordinairement reconnus aux personnes concernées sur leurs données médicales, une proportion de leur autodétermination informationnelle tend à subsister. Cela signifie que les citoyens peuvent, dans une certaine mesure, adhérer comme déclinier le traitement de leur données médicales aux fins d'affronter la menace sanitaire. Néanmoins, l'efficacité des systèmes d'information mis en œuvre pour la braver et, consécutivement, le succès de la stratégie de santé publique à laquelle ils sont intégrés dépendent directement de la mobilisation de l'ensemble des membres de la société. Assurément, la préservation de la santé d'une population procède de la participation des individus aux stratégies et aux outils

de santé publique décidés politiquement. Seulement, comment espérer leur assentiment compte tenu des inquiétudes soulevées et des inconvénients présentés ?

L'acceptabilité de la datasurveillance face à une menace sanitaire nécessite l'affermissement du concept de la démocratie sanitaire. Malgré l'urgence et la gravité d'une situation sanitaire, la société civile devrait être invitée à coconstruire la politique de santé publique d'une part, et responsabilisée à l'accomplissement de cette cause commune d'autre part. Véritablement, « *avec la démocratie en santé, au lieu d'avoir une santé publique contrainte, on peut avoir une santé publique qui est expliquée, mobilisée et faite ensemble* »²³⁶⁹. De surcroît, l'innovation numérique demeurerait davantage au service de l'humanité si elle était contenue par un processus démocratique. Toutefois, si l'exercice de la démocratie sanitaire ainsi que la participation citoyenne à la santé publique présupposent la responsabilisation des citoyens, la responsabilité de chacun à l'égard de la santé de tous ne constituerait-elle pas un devoir ? Autrement dit, n'existerait-il pas un devoir de concours à la lutte contre les menaces sanitaires ? A l'évidence, « *les données personnelles sont vues comme une ressource pour répondre directement aux défis sanitaires* »²³⁷⁰. Alors, dans l'hypothèse où l'autodétermination informationnelle des citoyens était conservée, ils auraient le devoir de favoriser le traitement de leurs données médicales nominatives ou pseudonymisées au profit de ce motif d'intérêt général. Toutefois, l'instauration et l'efficacité d'un tel devoir impliqueraient d'en déterminer, délicatement, la valeur et la portée.

²³⁶⁹ ANSOBORLO (M.), BELART (A.), FAUSSAT (C.), FLORENCE (A.-M.), DE LAFFOREST (S.), DIOT (P.), *op. cit.*, p. 3.

²³⁷⁰ CNIL, Audition commission des lois Assemblée nationale Propos liminaires de Madame Marie-Laure Denis, Présidente de la CNIL, mercredi 8 avril 2020, p. 2.

Conclusion du titre

625. Les données médicales des uns servent à la promotion de la santé de tous. En effet, les données médicales représentent le matériau principal de la protection et de l'amélioration de la santé publique. C'est alors qu'un principe d'altruisme de la donnée médicale émergerait à l'appui d'une nouvelle ère de la politique publique de la donnée. Ce principe consiste, pour les personnes concernées, à partager sciemment leurs données personnelles avec des tiers pour des projets d'intérêt général²³⁷¹. Spécifiquement, il s'agirait, pour les patients, de partager leurs données médicales avec les acteurs conduisant des projets concourant à la santé publique. En raison de leur utilité pour cet objectif public, les données médicales des patients comporteraient intrinsèquement un caractère d'intérêt général qui participerait à les ériger en choses communes. Alors, c'est à partir de cette chose anthropomorphique commune que les membres de la société coconstruiraient et entretiendraient ensemble un autre commun : la santé publique²³⁷².

L'exploitation des données médicales présente donc un enjeu considérable pour l'intérêt de la collectivité. C'est d'ailleurs pour cette raison que la notion générale et abstraite de l'intérêt public permet de déroger aux principes essentiels du droit à la protection des données personnelles²³⁷³. En effet, le législateur européen autorise le traitement des données médicales des personnes concernées, sans requérir leur consentement, lorsque « *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* »²³⁷⁴. Il en résulte que l'intérêt de la collectivité l'emporterait sur les intérêts particuliers des individus, quand bien même ils seraient concernés par le

²³⁷¹ BOTHOREL (E.), COMBES (S.), VEDEL (R.), *op. cit.*, p. 181.

²³⁷² Voir : REBOUL-MAUPIN (N.), *Santé et biens communs : vers un nouveau droit vivant des biens !*, In Mélanges en l'honneur de Gérard Mémeteau, *Droit médical et éthique médicale : regards contemporains*, LEH, 2015, p. 581 à p. 592.

²³⁷³ Voir : CJUE, 21 juin 2012, aff. C-84/11, *Marja-Liisa Susisalo, Olli Tuomaala, Merja Ritala* : Europe, 2012, n° 8-9, comm. 321, note A. Rigaux ; RTD Eur., 2013, n° 03, p. 679, note F. Benoît-Rohmer ; CJUE, 6 septembre 2012, aff. C-544/10, *Deutsches Weintor eG c/ Land Rheinland-Pfalz* : Europe, 2012, comm. 430, obs. S. Roset ; RD rur, 2013, n° 412, comm. 61, F. Barthe ; RD rur. 2013, n° 413, comm. 88, N. Olszak.

²³⁷⁴ Article 9.2 i) du RGPD.

traitement d'informations intimement sensibles. Pour cause, la notion d'intérêt général « *est censée désigner l'ordre public, l'intérêt du peuple ou bien la priorité des décisions administratives sur les intérêts privés, sectoriels, les droits individuels et les contrats entre particuliers* »²³⁷⁵. Finalement, l'association des principes d'altruisme et de réciprocité des individus envers la société consoliderait un devoir auquel ils ne pourraient véritablement renoncer. Assurément, le droit à la protection des données ne laisse que peu de marge à l'autodétermination informationnelle des patients concernés par la réutilisation de leurs données médicales pour un motif d'intérêt public dans le domaine de la santé.

626. Néanmoins, quelle serait la portée d'un devoir de concours à la santé publique dans les quelques cas où le patient conserve son autodétermination informationnelle à l'égard de ses données médicales personnelles ? A l'inverse des devoirs moraux, les devoirs juridiques constituent des obligations légales. Les résonances d'un devoir juridique sur les conduites des individus dépendent de l'effectivité de la règle de droit qui l'édifie, c'est-à-dire son respect par ses destinataires²³⁷⁶. La fonction de la règle de droit étant « *de servir de modèle idéal à l'action humaine* »²³⁷⁷, l'application d'une règle de droit par ses destinataires passe notamment par la « *reproduction d'un modèle soit pour éviter une sanction, soit pour obtenir certains effets* »²³⁷⁸. Pendant que l'accomplissement du devoir de concours à la santé publique par la mise à disposition de ses données médicales personnelles peut potentiellement faire l'objet d'une récompense²³⁷⁹, le manquement à son exécution devrait-il entraîner une sanction ? Si les membres de la société sont individuellement responsables de l'amélioration de la santé collective, cette responsabilité n'implique-t-elle pas d'assumer les conséquences de ses actes ?

²³⁷⁵ CRETOIS (P.), ROZA (S.), *loc. cit.*

²³⁷⁶ Voir : MINCKE (C.), *Effets, effectivité, efficacité et efficacité du droit : le pôle réaliste de la validité*, Revue interdisciplinaire d'études juridiques, vol. 40, 1998, n°01, p. 115 à p. 151.

²³⁷⁷ MINCKE (C.), *op. cit.*, p. 127.

²³⁷⁸ MINCKE (C.), *op. cit.*, p. 129.

²³⁷⁹ Cf. Paragraphe 463.

La santé publique constitue un bien social qui bénéficie à l'ensemble de la société et qui requiert d'être défendu par le plus puissant de tous les droits²³⁸⁰. C'est pourquoi le législateur a déjà érigé la santé publique en valeur sociale à protéger²³⁸¹. Cela n'empêche que le « *mauvais positionnement du pouvoir incriminateur en matière médicale aboutit trop souvent à une impuissance du droit pénal, là où pourtant se nouent parfois des drames sanitaires et où le droit pénal devrait jouer le rôle qui doit être le sien pour protéger les valeurs sociales* »²³⁸². Seulement, l'incrimination de la soustraction au concours de la santé publique apparaîtrait-elle nécessaire à la protection de la santé publique et proportionnée à la limitation du droit à la protection des données personnelles ? Censément, l'effectivité de ce devoir devrait davantage résider dans les conséquences positives attachées à la communication de sa chose anthropomorphique au profit de la coconstruction de notre bien commun universel.

²³⁸⁰ Voir : BEAUSSONIE (G.), *La notion de valeur sociale protégée*, In KUREK (C.), PAPIILLON (S.), MISTRETTA (P.), *L'empreinte des valeurs sociales protégées en droit pénal*, Dalloz, août 2020, p. 6.

²³⁸¹ Aux articles 511-1 à 511-28 du code pénal.

²³⁸² MISTRETTA (P.), *Valeur sociale protégée et santé*, In KUREK (C.), PAPIILLON (S.), MISTRETTA (P.), *L'empreinte des valeurs sociales protégées en droit pénal*, Dalloz, août 2020, p. 106.

Conclusion de la deuxième partie

627. La réutilisation des données médicales du patient est une condition *sine qua non* à l'amélioration de la santé publique par les recherches dans le domaine de la santé ainsi qu'à la protection de la santé publique par la datasurveillance des menaces sanitaires. Les données médicales sont alors très prisées en raison de leur utilité pour la collectivité et de la valeur économique qu'elles génèrent par l'intermédiaire de leur traitement. C'est ainsi que les éléments immatériels du corps humain du patient sont devenus la cible privilégiée des cybercriminels. Eu égard à la convoitise de ces informations intimement confidentielles, l'encadrement de leur traitement par le droit à la protection des données personnelles n'apparaît plus suffisant. En effet, il s'avère nécessaire de protéger la donnée médicale parce qu'elle existe en tant que chose indépendamment de son utilisation éventuelle. Cette garantie suppose donc qu'un statut particulier lui soit légalement consacré : celui d'une chose anthropomorphique.

628. Ce statut aurait vocation à réguler l'utilisation – gracieuse – de cette information d'intérêt général ainsi qu'à protéger l'intimité de la vie privée et la dignité de la personne physique qui en est à l'origine. L'intégration de la chose anthropomorphique du patient parmi les choses communes n'empêche qu'il demeure titulaire du secret médical quand elle est nominative et qu'il en garde le contrôle lorsqu'elle fait l'objet d'une pseudonymisation. Le statut spécifique à la chose anthropomorphique favorise donc sa mise à disposition au profit de la collectivité sans que l'impériosité de sa protection ne puisse être opposée à la protection de la santé publique, à l'innovation sanitaire, ni à la valorisation des résultats subséquents à son traitement. Vraisemblablement, « *vouloir empêcher le recueil des données, c'est bloquer l'innovation, et donc freiner l'économie numérique* »²³⁸³.

629. L'édification d'un statut de la chose anthropomorphique conforme aux valeurs des droits civils consacrés par le droit français, et repris par le droit européen, devient indispensable à l'heure où la création d'un espace européen des données de santé est discutée

²³⁸³ PEUGEOT (V.), *Données personnelles : sortir des injonctions contradictoire*, 13 avril 2014. Article disponible en ligne sur le site [www.vecam.org]. Consulté le 4 février 2021.

au sein de la Commission européenne²³⁸⁴. Si l'accès à un volume exponentiel de données médicales des citoyens européens devenait bientôt possible, ce regroupement essentiel pour le bien commun entraînerait *necessario* de larges tentations mercantiles. C'est pourquoi « *la mise en place d'un espace européen des données de santé que l'Union appelle de ses vœux ne pourra se faire que dans le respect [...] des choix souverains des Etats quant à la collecte et au traitement de ces données sensibles* »²³⁸⁵.

²³⁸⁴ Commission européenne, *Une stratégie européenne pour les données*, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, 19 février 2020, p. 35 à p. 36.

²³⁸⁵ DE GROVE-VALDEYRON (N.), *op. cit.*, p. 144.

CONCLUSION GENERALE

630. Ces travaux ont révélé que le patient ne disposait que d'une faible maîtrise de sa donnée médicale. Bien que la chose anthropomorphique soit une émanation du corps humain du patient, elle semble systématiquement lui échapper. Pour cause, la chose anthropomorphique constitue un instrument sanitaire globalisé. En effet, elle représente tant l'outil du professionnel de santé nécessaire à la prévention, aux diagnostics et aux soins du patient que le matériau utile à l'innovation en santé et à la protection de la santé publique. Il appert que l'usage de la chose anthropomorphique profite tant à la santé individuelle du patient qu'à la santé collective de la population. Le traitement de la donnée médicale apparaît donc comme un impératif sanitaire entraînant une réduction de l'autodétermination informationnelle du patient et une diminution des droits qui lui sont effectivement reconnus à l'égard des éléments immatériels de son corps humain. Certainement, le patient ne peut intervenir pour modifier ni pour effacer une réalité : la réification de son corps humain et, subséquent, de son état de santé à un instant donné.

631. L'autodétermination médicale du patient doit donc être distinguée de son autodétermination informationnelle. En effet, la personne physique qui consent à être prise en charge médicalement ne peut librement décider de la génération et de l'analyse des éléments immatériels de son corps humain. Assurément, ces traitements constituent essentiellement l'objet de la prise en charge médicale, ils en sont consubstantiels. Le patient doit alors favoriser le traitement de ses données médicales et livrer toute information pertinente pour l'exécution des services de soins de santé dont il bénéficie.

En revanche, la réutilisation des données médicales du patient à des fins d'intérêt public dans le domaine de la santé ne présente, à première vue, aucune utilité pour la dispensation des actes sanitaires auxquels il a consenti. Seulement, le patient étant membre de la collectivité, l'exploitation de ses données médicales pour l'amélioration et la protection de la santé publique lui profite *in fine*. Il existe donc un lien indirect entre l'exploitation des données médicales du patient au profit d'un intérêt sanitaire général et son propre état de santé. De la même façon que le patient ne peut s'opposer à l'utilisation de ses données médicales dans le cadre de sa prise en charge sanitaire, le législateur a restreint les possibilités de s'opposer à la réutilisation de ses données médicales pour un motif d'intérêt public

important pour la santé publique²³⁸⁶. De surcroît, le responsable de traitement n'est pas tenu de faire droit à la demande d'opposition dès lors qu'il existe des motifs légitimes et impérieux importants pour le traitement qui prévalent sur les intérêts, les droits et les libertés de la personne concernée²³⁸⁷. Si la donnée médicale est, par nature, l'une des informations les plus intimes concernant un individu, son intérêt particulier pour la santé de tous et de chacun la dresse en une chose commune sacralisée.

632. La chose anthropomorphique étant capitale à la prise en charge médicale du patient et à l'objectivation de la santé publique, ces travaux ont dévoilé que le patient avait davantage de devoirs que de droits à son égard. En conséquence, le patient serait responsable de la communication de ses données médicales pour le bien de sa santé individuelle comme pour le bien de la santé collective. Cependant, pour qu'un devoir juridique produise des effets efficients, « *la relation entre le comportement et la règle doit être consciente dans l'esprit du sujet concerné* »²³⁸⁸. L'instauration de devoirs incombant aux patients vis-à-vis de leurs données médicales présuppose inéluctablement la dispensation d'une éducation à la santé. Afin d'atteindre l'entièreté des membres de la société, cette éducation sanitaire doit indispensablement se montrer inclusive. Véritablement, si la responsabilité signifie que les individus aient à répondre de leurs actions ou de leurs omissions, encore est-il nécessaire qu'ils puissent en évaluer les bienfaits comme les méfaits.

633. En conclusion de ces travaux, nous pouvons affirmer que l'exercice, par le patient, d'une autodétermination informationnelle raisonnable et responsable implique généralement un renforcement de l'éducation et de la démocratie sanitaires couplés à une protection renforcée de la très particulière *chose anthropomorphique*. La considération normative de ces propositions académiques constitue une urgence à l'heure de la progression de la médecine numérique et algorithmique ainsi que de l'amplification des catastrophes sanitaires consécutives au dérèglement climatique. L'exploitation des données médicales des patients constituera alors un enjeu sanitaire pour lequel tout individu devrait se mobiliser. A l'avenir,

²³⁸⁶ Article 17.3 c) du RGPD.

²³⁸⁷ Article 21.1 du RGPD.

²³⁸⁸ MINCKE (C.), *op. cit.*, p. 118.

le citoyen saurait devenir l'acteur principal du concept *One Health*²³⁸⁹ qui « encourage une approche globale plus collaborative, multisectorielle et transdisciplinaire pour une meilleure santé »²³⁹⁰ des personnes, des animaux et de l'environnement. S'il n'y a qu'un monde, il n'y a qu'une seule Santé que chacun a le devoir de préserver. Assurément, la protection de la santé individuelle comme de la santé collective correspond à autant d'obligations individuelles et collectives²³⁹¹ à l'égard des *données médicales* qu'il appartient – maintenant – au législateur de consacrer²³⁹².

²³⁸⁹ Selon l'OMS, « *One Health est une approche de conception et de mise en œuvre de programmes, de politiques, de législation et de recherche dans laquelle de multiples secteurs communiquent et travaillent ensemble pour obtenir de meilleurs résultats en matière de santé publique. L'approche « Une seule santé » est essentielle pour faire face aux menaces pour la santé dans l'interface entre l'animal, l'homme et l'environnement.* ». Définition disponible sur le site [www.euro.who.int]. Consulté le 15 novembre 2021.

²³⁹⁰ AOMARI (M.), BRU (P.), EL GANI (H.), JABOT (M.), KABA (A.), LEMAIRE (L.), MOREAU (M.), MULLIEZ (H.), QUESNE (A.), TOUMELIN (M.), YAECHE (C.), sous la direction de QUESNE (A.), *Santé humaine, animale et environnementale : état des lieux et perspectives du concept One Health*, RGDM, n° 80, septembre 2021, p. 147.

²³⁹¹ Cons. Const., 20 mars 2015, décision n° 2015-458 QPC : : AJDA, 2015, n° 11, p. 611, note J.-M. Pastor ; JCP G, 2015, n° 22, p. 1055, note K. Foucher et V. Rachet-Darfeuille ; JCP G ; 2016, n° 36, p. 1607, chron. B. Mathieu et M. Verpeaux ; Dr. fam., 2015, n° 05, p. 03, note M. Lamarche ; RJPF, 2015, n° 05, p. 25, note A. Cheynet de Beaupré ; LPA, 2017, n° 21, p. 06, chron. M. Verpeaux.

²³⁹² JARRY-LACOMBE (B.), BERGERE (J.-M.), EUVE (F.), TARDIEU (H.), *Pour un numérique au service du bien commun*, Odile Jacob, 2022.

Index Alphabétique

Les chiffres renvoient aux numéros des paragraphes principaux.

A

ABUSUS, voir *ATTRIBUTS DE LA PROPRIETE*.

ACCES (droit d'–) :

- Majeur, **189 s, 196 s, 421, 511.**
- Majeurs protégés, **212 s.**
- Mineur :
 - Principe, **204 s.**
 - Secret gardé, **208, 209.**

ACQUISITION DE LA PROPRIETE, **382 s, 385 s.**

ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES, **567.**

ANONYMISATION :

- Définition, **366, 392 s.**
- Traitement aux fins (d' –), **367 s.**

ARCHIVES PUBLIQUES, **156 s, 506.**

ATTRIBUTS DE LA PERSONNALITE, **353.**

ATTRIBUTS DE LA PROPRIETE :

- ABUSUS, **390.**
- FRUCTUS, **442, 449 s.**

- USUS, **415, 439, 441, 445 s, 453.**

ATTRIBUTS DU CORPS HUMAIN, **354.**

AUTODETERMINATION INFORMATIONNELLE :

- Définition, **32, 330, 539.**

B

BASE DE DONNEES :

- Contenu :
 - Eléments, **440.**
 - Droit *sui generis* du producteur, **417 s, 426, 429 s.**
 - Redevance, **420, 423, 431.**

BASE LEGALE DU TRAITEMENT :

- Détermination, **19, 101.**
- CONSENTEMENT :
 - Définition, **580.**
- INTERETS LEGITIMES :
 - Définition, **113.**
- MISSION D'INTERET PUBLIC :
 - Définition, **112.**
- OBLIGATION LEGALE :
 - Définition, **103.**

BIEN MEUBLE INCORPOREL, **370, 382 s, 385 s, 392.**

C

CHOSE COMMUNE :

- Définition, **374**.

CHOSE SANS MAITRE, **370, 373, 392**.

COLLOQUE SINGULIER, **5, 320, 556**.

COMMERCE JURIDIQUE, **363, 383, 414**.

COMMISSION D'ACCES AUX DOCUMENTS ADMINISTRATIFS, **191**.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES :

- Autorisation, **22, 439, 496**.
- Avis, **567, 591, 594**.
- Recommandations, **103**.
- Recours, **192**.

CONTROLE DE CONSTITUTIONNALITE, **592**.

CREATION INTELLECTUELLE, **436, 437**.

D

DATASURVEILLANCE :

- *Contact tracing*, **555, 557, 570, 575, 580**.
- Suivi épidémiologique, **345, 557, 570, 608**.

- Surveillance sanitaire, **548, 608.**

DEMOCRATIE SANITAIRE, **96, 540 s, 615, 616, 620 s, 633.**

DEVOIR :

- DEVOIR DE COLLABORATION A LA PRISE EN CHARGE SANITAIRE, **319** :
 - Devoir de communication des données médicales, **319 s.**
 - Devoir de renseignement des données médicales, **307 s, 311 s.**
- DEVOIR DE CONCOURS A LA PROTECTION DE LA SANTE PUBLIQUE, **626** :
 - Devoir de concours à la recherche et à l'innovation dans le domaine de la santé, **531 s.**
 - Devoir de coopération citoyenne contre les menaces sanitaires, **612 s, 624.**
- DEVOIR DE RECTIFICATION DES DONNEES MEDICALES, **178.**

DIGNITE HUMAINE, **37, 52, 356 s, 372, 377, 393, 411, 628.**

DIRECTIVES ANTICIPEES, **82.**

DIRECTIVES SUR LE SORT DES DONNEES APRES LE DECES, **530.**

DOCUMENTS ADMINISTRATIFS :

- Accès :
 - Patient, voir *ACCES (droit d'—)*.
 - Tiers réutilisateurs :
 - Gratuité, **420.**
 - Principe, **421.**
 - Redevance, **420, 424, 425.**
- Définition, **191.**

DOMAINE COMMUN INFORMATIONNEL, **376, 441, 453, 464, 466 s, 506, 545 s, 618.**

DON :

- Mobilier, **362.**
- Organes et tissus, **176.**

DONNEES A CARACTERE PERSONNEL :

- Définition, **10.**

DONNEES ANONYMES :

- Définition, **11, 366.**

DONNEES DE RECHERCHE :

- Définition, **480 s.**

DONNEES GENETIQUES :

- Définition, **52.**

DONNEES MEDICALES :

- Composition, **49 s, 52 s.**
- Définition, **15, 355.**
- Régime juridique, **17 s, 356 s, 373 s, 441, 466.**
- Statut juridique, **352 s, 366 s, 466.**

DONNEES SENSIBLES :

- Définition, **12.**

DOSSIER MEDICAL :

- DOSSIER MEDICAL HOSPITALIER :
 - Accès, voir *ACCES (droit d'—)*.

- Constitution, **103.**
- Contenu, **57 s, 66.**
- Conservation, **151.**
- DOSSIER MEDICAL PARTAGE :
 - Accès :
 - Patient, **201.**
 - Professionnels, **288 s, 299.**
 - Clôture, **117.**
 - Contenu, **77 s.**
 - Conservation, **172, 177.**
 - Masquage, **325, 326.**
 - Ouverture, **116 s.**
- FICHE D'OBSERVATION PERSONNELLE :
 - Accès, voir *ACCES (droit d'—)*.
 - Constitution, **107 s.**
 - Contenu, **62 s, 66.**
 - Conservation, **152, 153.**

DROIT-CREANCE, 335, 341, 534.

DROITS DE L'AUTEUR :

- Droits extrapatrimoniaux, **405 s.**
- Droits moraux, **404.**

DROITS DE LA PERSONNALITE, 356 s, 391, 408.

DROITS DES PERSONNES CONCERNEES :

- Composants :
 - ACCES (droit d'–), voir indexation correspondante.
 - EFFACEMENT (droit d'–), voir indexation correspondante.
 - INFORMATION (droit d'–), voir indexation correspondante.
 - LIMITATION (droit à la –), voir indexation correspondante.
 - OPPOSITION (droit d'–), voir indexation correspondante.
 - PORTABILITE (droit à la –), voir indexation correspondante.
 - RECTIFICATION (droit de –), voir indexation correspondante.
- Délais de réponse, **131**.

E

ECHANGE DE DONNEES MEDICALES, voir *SECRET PROFESSIONNEL MEDICAL*.

EDUCATION SANITAIRE, **614, 633**.

EFFACEMENT (droit d'–),

- Données médicales, **143 s, 154 s, 168 s, 178**.
- Données de recherche, **506, 513, 514**.

ENTREPOT DE DONNEES DE SANTE, **491, 503 s**.

EQUIPE DE SOINS, **264**.

EQUITE, **462 s**.

ESPACE NUMERIQUE DE SANTE :

- Définition, **94**.

ETAT D'URGENCE SANITAIRE, **551, 606**.

ETHIQUE DE LA SANTE PUBLIQUE, **612 s.**

EXACTITUDE DES DONNEES (principe d'—) :

- Définition, **130 s.**
- Exemples, **135 s, 163, 167, 175, 308, 316, 505, 511 s.**

EXAMEN CLINIQUE :

- Anamnèse, **50**.
- Examen physique, **51**.
- Examens complémentaires, **52, 53**.

F

FAUTE :

- Exonération de responsabilité, **308, 314 s.**
- Présomption, **69**.

FINALITE, voir *PRINCIPES ESSENTIELS DU TRAITEMENT*.

FONDEMENT JURIDIQUE, voir *BASE LEGALE DU TRAITEMENT*.

FRACTURE NUMERIQUE, **118, 313, 574**.

FRUCTUS, voir *ATTRIBUTS DE LA PROPRIETE*.

H

HEALTH DATA HUB, voir *PLATEFORME NATIONALE DES DONNEES DE SANTE*.

HEBERGEUR DE DONNEES DE SANTE, **150, 154, 177, 199, 200, 619**.

HOSPITALISATION SOUS CONTRAINTE, **236 s.**

I

IDENTITOVIGILANCE, **60, 135**.

INDISPONIBILITE (de la chose), **362**.

INFORMATIONS D'INTERET GENERAL, **469, 625**.

INFORMATION MEDICALE (droit à l' –), **188, 230**.

INFORMATION (droit d' –) :

- Aménagement, **500**.
- Délais, **369, 489**.
- Dérogation, **496 s.**
- Mode de délivrance, **488**.
- Principe, **485 s.**

INTEGRITE :

- Corps humain, voir *DIGNITE HUMAINE*.
- Données médicales, **34, 128, 140, 398, 502, 512**.

INTERET PUBLIC :

- Définition, **541**.
- Evaluation, **439, 540**.
- Finalité, **346, 443, 460**.

INTEROPERABILITE INFORMATIQUE, **86, 94, 158, 536**.

L

LETTRE DE LIAISON, **295**.

LIMITATION DE LA CONSERVATION (principe de –), **150, 155 s, 170, 579, 611**.

LIMITATION DES FINALITES (principe de –) :

- Finalité initiale :
 - Définition, **474**.
- Finalité ultérieure :
 - Définition, **475**.
 - Critères de compatibilité, **476**.
 - Présomption de compatibilité, **368, 494**.

LIMITATION DU TRAITEMENT (droit à la –), **507, 515**.

M

MAJEUR PROTEGE, voir *ACCES (droit d'–)*.

MALADIE A DECLARATION OBLIGATOIRE, **557**.

MANDAT, **197.**

MARCHANDISATION DU CORPS HUMAIN, **371 s, 411 s, 445, 466.**

MARCHE ECONOMIQUE, **361.**

METHODOLOGIE DE REFERENCE :

- Principe, **439.**

MESURES TECHNIQUES ET ORGANISATIONNELLES, **55, 478, 565, 568.**

MINEUR, voir *ACCES (droit d'–)*.

MINIMISATION DES DONNEES (principe de –) :

- Définition, **43.**
- Exemples, **59, 67 s, 266 s, 490.**

N

NECESSITE DU TRAITEMENT, **587 s.**

NON-PROFESSIONNELS DE SANTE, **261.**

NOTES PERSONNELLES, **71 s.**

O

OBJECTIF A VALEUR CONSTITUTIONNELLE, **329, 592.**

OBLIGATION MORALE, **337.**

ŒUVRE DE L'ESPRIT, **397 s.**

ŒUVRE PLURALE, **457 s.**

OPPOSITION (droit d' –) :

- – à l'alimentation du DMP, **123 s.**
- – à la communication des données médicales, **278 s, 284 s, 296 s.**
- – à la création des dossiers de soins, **104, 107.**
- – à la création du DMP, **117.**
- – à la réutilisation des données médicales à des fins de recherche, **521 s, 524 s.**
- – à la réutilisation des données médicales à des fins de lutte contre une menace sanitaire, **570 s, 575, 578, 580, 581.**

OUBLI (droit à l'–), voir *DROITS DES PERSONNES CONCERNEES*.

P

PARTAGE DE DONNEES MEDICALES, voir *SECRET PROFESSIONNEL MEDICAL*.

PARTURIENTE, **49.**

PERSONNE DE CONFIANCE, **81, 82.**

PLATEFORME NATIONALE DES DONNEES DE SANTE, **427, 504, 536.**

PORTABILITE (droit à la –), **300.**

PREUVE :

- Charge de la preuve, **69.**
- Etablissement de la preuve, **68.**

- Falsification, **141**.
- Moyen de preuve, **137, 152, 172**.

PRINCIPES ESSENTIELS DU TRAITEMENT :

- EXACTITUDE DES DONNEES (principe d'–), voir indexation correspondante.
- LIMITATION DES FINALITES (principe de –), voir indexation correspondante.
- LIMITATION DE LA CONSERVATION (principe de –), voir indexation correspondante.
- MINIMISATION DES DONNES (principe de –), voir indexation correspondante.
- SECURISATION DES DONNEES (principe de –), voir *MESURES TECHNIQUES ET ORGANISATIONNELLES*.
- TRANSPARENCE (principe de –), voir indexation correspondante.

PROFESSIONNEL DE SANTE, **260**.

PROPORTIONNALITE DU TRAITEMENT, **596 s**.

PROTECTION DE LA SANTE :

- Collective :
 - Définition, **528**.
- Individuelle :
 - Définition, **329**.

PSEUDONYMISATION :

- DEFINITION, **421**.
- FONCTIONNEMENT, **478**.

R

RECHERCHES, ETUDES ET EVALUATIONS DANS LE DOMAINE DE LA SANTE, voir *RECHERCHE N'IMPLIQUANT PAS LA PERSONNE HUMAINE*.

RECHERCHE N'IMPLIQUANT PAS LA PERSONNE HUMAINE :

- Définition, **470, 473.**

RECIPROCITE (principe de –), **535.**

RECOMPENSE INDEMNITAIRE, **463 s.**

RECTIFICATION (droit de –) :

- – des données médicales, **137 s, 162 s.**
- – des données de recherche, **505, 512.**

RESPONSABLE DE TRAITEMENT :

- Définition, **122.**

RETICENCE DOLOSIVE, **308, 309.**

S

SANTE PUBLIQUE :

- Définition, **612.**

SECRET PROFESSIONNEL MEDICAL :

- Communication des données médicales, **257, 262, 274 :**
 - Echange, **275 s.**
 - Partage, **282 s, 555.**

- Dépositaires, **260, 261, 545, 557.**
- Principe, **24 s, 193, 556.**
- Sanction, **566.**
- Titulaire, **24 s, 193, 194, 251, 321, 388.**
- Violation, **196, 244, 269, 324, 558.**

SOUS-TRAITANCE, **363, 490.**

SOUVERAINETE NUMERIQUE, **619.**

SURVEILLANCE SANITAIRE : voir *DATA SURVEILLANCE.*

SYSTEME NATIONAL DES DONNEES DE SANTE :

- Définition, **157, 427.**

T

THEORIE DE L'ACCESSOIRE, **353.**

TRAITEMENT :

- Autorisation :
 - Principe, **29, 439.**
- Définition, **3.**
- Interdiction :
 - Principe, **17.**

TELESANTE :

- TELESOIN :
 - Définition, **65, 70.**
- TELEMEDECINE :
 - Actes :
 - Téléassistance médicale, **298.**
 - Téléconsultation médicale, **51, 306.**
 - Téléexpertise médicale, **298, 323.**
 - Télésurveillance médicale, **67.**
 - Définition, **65.**

TRANSPARENCE (principe de –) :

- Définition, **118, 483, 485.**
- Exemples, **278, 538, 574.**

U

USUS, voir *ATTRIBUTS DE LA PROPRIETE.*

USUFRUIT, **442, 444 s.**

Bibliographie

I. Ouvrages, Manuels, Traités et Cours

ARISTOTE, *Sur la justice, Éthique à Nicomaque*, Flammarion, 2008, 128 pp.

AUBERT (J.-L.), SAVAUX (E.), *Introduction au droit et thèmes fondamentaux du droit civil*, 18^e ed., Sirey, août 2020, 432 pp.

BENABOU (V.-L.), ROCHFELD (J.), *À qui profite le clic ? Le partage de la valeur à l'heure numérique*, Odile Jacob, 2015, 112 pp.

BENSAMOUN (A.), *Le règlement général sur la protection des données : aspects institutionnels et matériels*, Mare & Martin, 2020, 258 pp.

BENTHAM (J.), *Déontologie*, Chapitre II, éd. Posth. 1834.

BIOY(X.), LAUDE (A.), TABUTEAU (D.), *Droit de la santé*, 4^e ed., Presses universitaires de France, 2020, 768 pp.

BUFFELAN-LANORE (Y.), LARRIBAU-TERNEYRE (V.), *Droit civil. Les obligations*, Sirey, 17^e ed., octobre 2020, 1266 pp.

CARBONNIER (J.), *Droit civil*, Vol. 1, 14^e ed, Presses universitaires de France, 1982, 409 pp.

CATALA (P.), *Le droit à l'épreuve du numérique : jus ex machina*, Presses universitaires de France, 1998, 345 pp.

CHAGNOLLAUD DE SABOURET (D.), *Dictionnaire élémentaire du droit*, 2^e ed., Dalloz, août 2016, 766 pp.

COMPIEGNE (I.), *La société numérique en question(s)*, Editions Sciences Humaines, 2010, 130 pp.

CORNU (G.), *Vocabulaire juridique*, 13^e ed, PUF, 2020, 1136 pp.

CORNU (M.), ORSI (F.), ROCHFELD (J.), *Dictionnaire des biens communs*, 2^e ed, PUF, 2021, 1392 pp.

CNIL, *Les données génétiques*, La documentation française, 6 septembre 2017, 216 pp.

DALLE (D.), QUEMENER (M.), WIERRE (C.), *Quels droits face aux innovations numériques ? Législation, jurisprudences et bonnes pratiques du cyberspace - Défis et protections face aux dérives du numériques*, Gualino, 2020.

DE MONDEVILLE (H.), *La chirurgie*, Tome 1, ed. 1897-1898, Société des anciens textes français, Bibliothèque nationale de France. Disponible en ligne sur le site [<https://gallica.bnf.fr>]. Consulté le 30 décembre 2020.

DOUVILLE (T.), *Droit des données à caractère personnel*, Gualino, 2020, 432 pp.

DUJARDIN (V.), *La personne mineure*, LEH, 2005, 110 pp.

DUHAMEL (G.), *Paroles de médecin*, Du Rocher Monaco, 1946, 248 pp.

ESPLUGAS-LABATUT (P.), *Le Conseil constitutionnel*, Dalloz, 9^{ème} ed, novembre 2020, 224 pp.

FERAL-SCHUHL (C.), *La protection des données personnelles*, Dalloz, 2019, 240 pp.

FERRAUD-CIANDET (N.), *Droit de la télésanté et de la télé médecine*, Heures de France, 158 pp.

GHANTY (A.) et al., *Protection des données personnelles*, Francis Lefebvre, 2019, 298 pp.

GUINCHARD (S.), DEBARD (T.), *Lexique des termes juridiques 2021-2022*, 29^e ed., Dalloz, août 2021, 1120 pp.

HENNETTE-VAUCHEZ (S.), *La démocratie en état d'urgence : quand l'exception devient permanente*, Éditions du Seuil, 2022, 208 pp.

HENNETTE-VAUCHEZ (S.), ROMAN (D.), *Droits de l'Homme et libertés fondamentales*, 4^e ed., Dalloz, 2020, 870 pp.

HIRSCH (E.), *Une démocratie confinée. L'éthique quoi qu'il en coûte*, Érès, 2021, 344 pp.

JARRY-LACOMBE (B.), BERGERE (J.-M.), EUVE (F.), TARDIEU (H.), *Pour un numérique au service du bien commun*, Odile Jacob, 2022, 240 pp.

KANT (E.), *Critique de la raison pratique*, Théorème IV, Première partie, Trad. par François PICAUVET, PUF, 1965, 228 pp.

KAYSER (P.), *La protection de la vie privée*, 3^e ed., PUAM, 1995, 605 pp.

LECA (A.), LUNEL (A.), SANCHEZ (S.), *Histoire du droit de la santé*, LEH, 2014, 314 pp.

LOISEAU (G.), *Le droit des personnes*, 2^{ème} ed., Ellipses, 2020, 373 pp.

MEMETEAU (G.), GIRER (M.), *Cours de droit médical*, 5^e ed., LEH, 2016, 854 pp.

NETTER (E.), *Numérique et grandes notions du droit privé*, CEPRISCA, 2019, 510 pp.

OBERDORFF (H.), *Droits de l'homme et libertés fondamentales*, LGDJ, ed. 8, août 2021, 476 pp.

OSTROM (E.), *Gouvernance des biens communs, pour une nouvelle approche des ressources naturelles*, Révisé par Laurent Baechler, De Boeck, 2010, 301 pp.

PARANCE (B.), DE SAINT VICTOR (J.), *Repenser les biens communs*, CNRS éditions, 2014, 314 pp.

PÉQUIGNOT (H.), *Médecine et mode moderne : l'écran des techniques entre le médecin et le malade*, Paris, Les éditions de minuit, 1953, 163 pp.

PORTES (L.), *À la recherche d'une éthique médicale*, Paris, Masson & Cie, 1964, 210 pp.

PY (B.), *Le secret professionnel*, L'Harmattan, 2005, 138 pp.

REBOUL-MAUPIN (N.), *Droit des biens*, Dalloz, 8^e ed., septembre 2020, 872 pp.

SAINT PAU (J.-C.), *Droits de la personnalité*, LexisNexis, 2013, 1410 pp.

TERRE (F.), SIMLER (P.), *Droit civil. Les biens*, Dalloz, 10^e ed., septembre 2018, 880 pp.

THERON (S.), *Les soins psychiatriques sans consentement*, Paris, Dunod, 2017, 352 pp.

TRANCHANT (L.), ÉGEA (V.), *Droit des obligations*, Dalloz, 25^e ed., septembre 2020, 250 pp.

VIALLA (F.), *Les grandes décisions du droit médical*, LGDJ, 2^e ed. 2014, 896 pp.

VIVANT (M.), BRUGUIERE (J.-M.), *Droit d'auteur et droits voisins*, Dalloz, 4^e ed., janvier 2019, 1386 pp.

II. Ouvrages collectifs, Mélanges et Colloques

BARBE (V.), *La garantie du droit au respect de la vie privée face au fichier* », In EDDAZI (F.), MAUCLAIR (S.), *Le fichier*, Actes du colloque organisé les 26 et 27 novembre 2015 par le Centre de recherche juridique Pothier de l'Université d'Orléans, LGDJ, p. 87 et s.

BEAUSSONIE (G.), *La notion de valeur sociale protégée*, In KUREK (C.), PAPILLON (S.), MISTRETTA (P.), *L'empreinte des valeurs sociales protégées en droit pénal*, Actes du colloque organisé le 6 juin 2019 par l'Université Lyon 3, Dalloz, août 2020, p. 5 à p. 15.

BENABOU (V.-L.), « *Création* » collaborative et données, In ROBIN (A.), *La propriété intellectuelle en partage*, Actes du colloques organisé en 2019 par la Faculté de Droit de Montpellier, Dalloz, octobre 2020, p. 49 à p. 68.

BENSAMOUN (A.), *Droits fondamentaux et internet*, In CABRILLAC (R.), *Libertés et droits fondamentaux 2021*, Dalloz, 27^e ed., 2021, p. 312 à p. 335.

BERNAULT (C.), *Œuvres protégées. Règles générales (CPI, art. L. 112-1 et L. 112-2)*, JurisClasseur Civil, Fasc. 1135, Annexes V^o Propriété littéraire et artistique, mars 2017, actu. mars 2021

BINCTIN (N.), *Retour sur un cadre juridique complexe et en pleine évolution*, In Rapport du Think-tank Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018, p. 47 à p. 76.

BLOCH (L.), *Rapport de synthèse*, In BLOCH (L.), *Numérique et crise sanitaire*, Université de Bordeaux, LEH Édition, Actes et séminaires, février 2021, p. 45 à p. 49.

CASAUX-LABRUNEE (L.), *Le droit à la santé*, In CABRILLAC (R.), *Libertés et droits fondamentaux 2021*, Dalloz, 27^e ed., 2021, p. 935 à p. 962.

CLEMENT-FONTAINE (M.), *Un renouveau des biens communs : des biens matériels aux biens immatériels*, In Faculté de droit et des sciences sociales de Poitiers - Actes & Colloques (dir.), *Les modèles propriétaires*, Actes du colloque international organisé par le CECOJI en hommage au professeur Henri-Jacques Lucas, LGDJ, 2012, n°47, p. 51.

CLUZEL-METAYER (L.), *Le code face aux données*, In KOUBI (G.), CLUZEL-METAYER (L.), TAMZINI (W.), *Lectures critiques du code des relations entre le public et l'administration*, LGDJ, 2018, 240 pp.

CRETOIS (P.), ROZA (S.), *De l'intérêt général : Introduction*, In CRETOIS (P.), ROZA (S.), *De l'intérêt général*, Astéris, 2017, n°17, p. 4.

DE LAMBERTERIE (I.), *Qu'est ce qu'une donnée de santé ?*, In *Le droit des données de santé*, Actes du colloque de l'Association française de droit de la santé organisé à Paris le 25 mars 2004, RGDM, 2004, n° 04, p. 11 à p. 34.

DELFORGE (A.), *Les obligations générales du responsable du traitement et la place du sous-traitant*, In DE TERWANGNE (C.) et ROSIER (K.), *Le règlement général sur la protection des données (RGPD/GDPR)*, Analyse approfondie, Larcier, 2018, p. 371 à p. 406.

DESENCLOS (J.-C.), *Surveillance et veille sanitaire : concepts, définition et organisation*, In DABIS (F.), DESENCLOS (J.-C.), *Épidémiologie de terrain*, John Libbey Eurotext, 2^{ème} ed., février 2017, p. 84 à p. 98.

DESENCLOS (J.-C.), BRÜCKER (G.), *Surveillance*, In BOURDILLON (F.), BRÜCKER (G.), TABUTEAU (D.), *Traité de santé publique*, Lavoisier, 2016, p. 79 à p. 94.

DESGENS-PASANAU (G.), *Traçage des données mobiles : ne sacrifions pas la protection de nos données sur l'autel de la crise sanitaire*, In *Le droit face au coronavirus, Comment une pandémie inédite à mis à l'épreuve notre système juridique*, LexisNexis, 2021, p. 439 à p. 441.

DE TERWANGNE (C.), *Définitions clés et champ d'application du RGPD*, In DE TERWANGNE (C.) et ROSIER (K.), *Le règlement général sur la protection des données (RGPD/GDPR)*. Analyse approfondie, Larcier, 2018, p. 59 à p. 84.

DROSS (W.), *L'extension de la notion de bien à l'intérêt économique substantiel*, In LEVENEUR (L.), *Les nouveaux biens*, Dalloz, janvier 2020, p. 15 à p. 29.

ESPESSON-VERGEAT (B.), *Quel regard en droit européen sur l'innovation juridique en matière de santé ?*, In ESPESSON-VERGEAT (B.), *Innovation juridique et transversalité des politiques liées au numérique, à la santé et aux territoires*, Actes du colloque organisé le 28 septembre 2017 à la Faculté de droit de Saint-Etienne, LEH, 2018, p. 113 à p. 116.

FOEGLE (J.-P.), *Le "droit" à l'autodétermination informationnelle et les réseaux numériques*, In ENCINAS DE MUNAGORI (R.), BENSAMOUN (A.), BROSSET (E.), COHENDET (M.-A.), *Sciences et droits de l'homme*, Actes du colloque organisé le 22 octobre 2015 à l'Université Paris 1, Mare & Martin, 2017, p. 85 à p. 103.

JACOTOT (D.), *D'une relation bipartite à une relation multipartite. Essai sur le contrat médical*, In, LEONHARD (J.), PY (B.), VIALLA (F.), *Mélanges en l'honneur de Gérard Mémeteau. Droit médical et éthique médicale : regards contemporains*, LEH Édition, 2015, p. 505 à p. 514.

LANDREAU (I.), *Le RGPD, un pas dans la bonne direction ?*, In Rapport du Think-tank Génération Libre, *Mes data sont à moi. Pour une patrimonialité des données personnelles*, janvier 2018, p. 77 à p. 94.

LECA (A.), *Corpus id est persona ? Réflexions à propos de la situation juridique du corps humain*, In THOLOZAN (O.), *De jure corporis ou la réification du corps humain*, Les cahiers de droit de la santé, 2004, n°02, p. 37 à p. 79.

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 à p. 316.

LUCAS (J.), *Quelle déontologie pour les médecins à l'heure du numérique ?*, In POIROT-MAZÈRES (I.), *Santé, numérique et droit-s*, Presses de l'Université Toulouse 1 Capitole, 2018, p. 167 à p. 175.

MALLET-POUJOL (N.), *Droit à et droit sur l'information de santé*, In *Le droit des données de santé*, Actes du colloque de l'Association française de droit de la santé organisé à Paris le 25 mars 2004, RGDM, 2004, n° 04, p. 77 à p. 95.

MARCHAND (J.), *L'accès et la réutilisation des données publiques dans le cadre de la loi pour une République numérique*, In CHATRY (S.), GOBERT (T.), *Numérique. Nouveaux droits, nouveaux usages*, Actes du colloque organisé le 10 mars 2017 à l'Université de Perpignan Via Domitia, Mare & Martin, 2017, p. 35 à p. 49.

MARTIAL-BRAZ (N) :

- *Présentation de la loi française et articulation des textes français et européens*, In MARTIAL-BRAZ (N.), ROCHFELD (J.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, p. 11 à p. 27.
- *Données traitées – Données de santé*, In MARTIAL-BRAZ (N.), ROCHFELD (J.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, p. 85 à p. 99.
- *Base de traitement – Consentement*, In MARTIAL-BRAZ (N.), ROCHFELD (J.), *Droit des données personnelles. Les spécificités du droit français au regard du RGPD*, Dalloz, 2019, p. 143 à p. 159.
- *Création et économie collaborative : quelle régulation ?*, In ROBIN (A.), *La propriété intellectuelle en partage*, Actes du colloques organisé en 2019 par la Faculté de Droit de Montpellier, Dalloz, octobre 2020, p. 19 à p. 31.
- *Nos données de santé en danger... Quand l'arbre de la crise sanitaire cache la forêt de la perte de souveraineté !*, In *Le droit face au coronavirus, Comment une pandémie inédite à mis à l'épreuve notre système juridique*, LexisNexis, 2021, p. 829 à p. 831.

MAUREL (L.), *La reconnaissance du « domaine commun informationnel » : tirer les enseignements d'un échec législatif*, In ALIX (N.), BANCEL (J.-L.), CORIAT (B.),

SULTAN (F.), *Vers une République des biens communs ?*, Les liens qui libèrent, 2018, Chapitre 9.

MISTRETTA (P.), *Valeur sociale protégée et santé*, In KUREK (C.), PAPILLON (S.), MISTRETTA (P.), *L’empreinte des valeurs sociales protégées en droit pénal*, , Actes du colloque organisé le 6 juin 2019 par l’Université Lyon 3, Dalloz, août 2020, p. 95 à p. 107.

MOUNCIF-MOUNGACHE (M.), *La place de la santé dans le règlement sur les données personnelles*, In ESPESSON-VERGEAT (B.), *Innovation juridique et transversalité des politiques liées au numérique, à la santé et aux territoires*, Actes du colloque organisé le 28 septembre 2017 à la Faculté de droit de Saint-Etienne, LEH, 2018, p. 85 à p. 93.

MOUSSERON (J.-M.), RAYNARD (J.), REVET (T.), *De la propriété comme modèle*, In Mélanges offerts à André Colomer, 1993, p. 281 à p. 306.

PAULIN (B.), *Trois conseils sur le traitement des données de santé*, In *Droit des données personnelles*, Dalloz, 1^{ère} ed., novembre 2019, p. à p..

PAUVERT (B.), *Le droit des éléments et produits du corps – ou les enjeux d’une réification silencieuse* – In NICOLAS (G.), *Les éléments et produits du corps humain*, Les cahiers de droit de la santé, 2011, n°12, p. 11 à p. 26.

PELLEGRINI (F.), SKRZYPNIAK (H.), *Les libertés publiques face au traçage numérique*, In BLOCH (L.), *Numérique et crise sanitaire*, Université de Bordeaux, LEH Édition, Actes et séminaires, février 2021, p. 17 à p. 40.

PY (B.), *Secret professionnel*, In VIALLA (F.) *Les grandes décisions du droit médical*, LGDJ, 2^e ed. 2014, p. 305 à p. 318.

REBOUL-MAUPIN (N.), *Santé et biens communs : vers un nouveau droit vivant des biens !*, In Mélanges en l’honneur de Gérard Mémeteau, *Droit médical et éthique médicale : regards contemporains*, LEH, 2015, p. 581 à p. 592.

ROCHFELD (J.) :

- *Quel modèle pour construire des communs ?*, In PARANCE (B.), DE SAINT VICTOR (J.), CNRS, 2014, p. 112.
- *Contre l'hypothèse de la qualification des données personnelles comme des biens*, In NETTER (E.), CHAIGNEAU (A.), *Les biens numériques*, PUF, 2015, p. 221 à p. 236.

ROUVROY (A.), POULLET (Y.), *Le droit à l'autodétermination informationnelle et la valeur du développement personnel: une réévaluation de l'importance du droit à la protection de la vie privée pour la démocratie*, In BENYEKHFLEF (K.), TRUDEL (P.), *Etat de droit et virtualité*, Thémis, Montréal, p. 157 à p. 222.

TABUTEAU (D.), DOMINIQUE (M.), *Les droits des personnes malades*, In BOURDILLON (F.), *Traité de santé publique*. Lavoisier, 2016, p. 148 à p. 158.

TRUCHET (D.), *Le secret médical, obligation obsolète ou exigence actuelle*, In Mélanges en l'honneur de Michel Bélanger, *Modernité du droit de la santé*, LEH, 2017, p. 317 à p. 328.

VIALLA (F.) :

- *L'accès au dossier médical*, In VIALLA (F.) *Les grandes décisions du droit médical*, LGDJ, 2^e ed. 2014, p. 207 à p. 226.
- *Non progredi est regredi ?*, In BROSSET (E.), GAMBARDELLA (S.), NICOLAS (G.), *La santé connectée et « son » droit : approches de droit européen et de droit français*, Presses Universitaires d'Aix-Marseille, 2017, p. 47 à p. 56.

III. Thèses

ALLIOT (S.), *Essai de qualification de la notion de données à caractère personnel*, Nathalie MARTIAL-BRAZ (dir.), Thèse de Doctorat, Droit, Université de Franche-Comté, 2018.

BRASSELET (R.), *La circulation de la donnée à caractère personnel relative à la santé,* Bruno PY (dir.), Thèse de doctorat, Droit, Université de Lorraine, décembre 2018.

CAVALIER (M.), *La propriété des données de santé,* Marion GIRER (dir.), Thèse de doctorat, Droit, Université Lyon 3 Jean Moulin, décembre 2016.

CHAMBARDON (N.), *L'identité numérique de la personne humaine : contribution à l'étude du droit fondamental à la protection des données à caractères personnel,* Édith JAILLARDON (dir.), Thèse de Doctorat, Droit, Université Lyon II, 2018.

CHARDEAUX (M.-A.), *Les choses communes,* Thèse de Doctorat, Droit, Université Paris I, LGDJ, 2006, préf. LOISEAU (G).

DEBAETS (E.), *Le droit à la protection des données à caractère personnel. Recherche sur un droit fondamental,* Bertrand MATHIEU (dir.), Thèse de Doctorat, Droit, Université Paris I, 2014.

EL RHRIB-LOUH (H.), *L'autonomie médicale des personnes en situation d'incapacité,* Françoise DEKEUWER-DEFOSSEZ (dir.), Thèse de doctorat, Droit, Université de Lille, juin 2012.

EYNARD (J.), *Les données personnelles, quelle définition pour un régime de protection efficace ?,* Thèse de Doctorat, Droit, Université Toulouse 1, Michalon, 2013, 436 pp.

GUITTET (L.), *La transparence des données issues des bases médico-administratives. Pour une ouverture des bases de données respectueuse de la vie privée,* Guillaume ROUSSET (dir.), Thèse de Doctorat, Droit, Université Lyon III, 2019.

HAGE-CHAHINE (N.), *La distinction de l'obligation et du devoir en droit privé,* Yves LEQUETTE (dir.), Thèse de doctorat, Droit, Université Paris II, avril 2014.

KOUMPLI (C.), *Les données personnelles sensibles. Contribution à l'évolution du droit fondamental à la protection des données à caractère personnel*, Otto PFERSMANN (dir.), Thèse de Doctorat, Droit, Université Paris I, 2019.

LANNA (M.), *La protection des données à caractère personnel à l'épreuve de l'automatisation connectée*, Camille BROUELLE, Lucie CLUZEL-METAYER (dir.), Thèse de Doctorat, Droit, Université Paris II, 2019.

LE CLAINCHE (J.), *L'adaptation du droit des données à caractère personnel aux communications électroniques*, Jean FRAYSSINET (dir.), Thèse de Doctorat, Droit, Université Montpellier I, 2008.

LESAULNIER (F.), *L'information nominative*, Thèse de Doctorat, Droit, Pierre CATALA (dir.), Université Paris II, 2005.

LUTUN (A.), *Le Bigdata en santé, richesse et conditions d'accès*, Anne DEBET (dir.), Thèse de Doctorat, Droit, Université Paris V, 2021.

MERABET (S.), *Vers un droit de l'intelligence artificielle*, Thèse de doctorat, Droit, Université Aix-Marseille, Dalloz, 2020, 558 pp.

NIETO (A.), *La vie privée à l'épreuve de la relation de soin*, François VIALLA (dir.), Thèse de Doctorat, Droit, Université de Montpellier, 2017.

OCHOA (N.), *Le droit des données personnelles : une police administrative spéciale*, Catherine TEITGEN-COLLY (dir.), Thèse de Doctorat, Droit, Université Paris I, 2014.

OLECH (V.), *Le secret médical et les technologies de l'information et de la communication*, Bruno PY (dir.), Thèse de doctorat, Droit, Université de Lorraine, 2019.

PELISSIER (A.), *Possession et meubles incorporels*, Dalloz, janvier 2001, 384 pp.

TILMAN (L.), *L'utilisation des technologies de l'information et de la communication à l'hôpital face au droit*, Johanne SAISON-DEMARS (dir.), Thèse de doctorat, Droit, Université de Lille, septembre 2017.

WATRIN (L.), *Les données scientifiques saisies par le droit*, Thèse de Doctorat, Droit, Université Aix-Marseille, Institut Francophone pour la Justice et la Démocratie, 2019, 504 pp.

ZORN-MACREZ (C.), *Données de santé et secret partagé. Pour un droit de la personne à la protection de ses données de santé partagées*, Thèse de Doctorat, Droit, Université Nancy 2, Presses universitaires de Nancy, 2010, 502 pp.

IV. Articles et Publications assimilées

ALBIGES (C.), *Équité*, Répertoire de droit civil, octobre 2017, actu. janvier 2019.

ANDRIANTSIMBAZOVINA (J.), *L'état d'urgence sanitaire et les libertés*, Droit de la famille, 2020, n°06, étude n°19.

ANCIAUX (A.), **FARCHY (J.)**, *Données personnelles et droit de propriété : quatre chantiers et un enterrement*, Revue internationale de droit économique, Vol. XXIX, 2015, n° 03, p. 307.

ANSOBORLO (M.), **BELART (A.)**, **FAUSSAT (C.)**, **FLORENCE (A.-M.)**, **DE LAFFOREST (S.)**, **DIOT (P.)**, *Pourquoi et comment donner un nouvel élan à la santé publique en France ?*, La Presse Médicale Formation, Vol. 2, 2021, n°01, Partie 2, p. 2.

ANTIPPAS (J.), *Propos dissidents sur les droits dits « patrimoniaux » de la personnalité*, Répertoire de droit commercial, 2012, n°01, p. 35.

AOMARI (M.), BRU (P.), EL GANI (H.), JABOT (M.), KABA (A.), LEMAIRE (L.), MOREAU (M.), MULLIEZ (H.), QUESNE (A.), TOUMELIN (M.), YAECHÉ (C.), *Santé humaine, animale et environnementale : état des lieux et perspectives du concept One Health*, Revue générale de droit médical, 2021, n° 80, p. 145.

AUBY (J.-B.), *DONNÉES PUBLIQUES. – Droits d'accès. Étendue*, JurisClasseur Administratif, Fasc. 109-60, 24 avril 2018, actu. 20 janvier 2021.

AZRIA (E.), *Le soignant et la standardisation des pratiques médicales*, Laennec, t. 61, 2013, n°3, p. 32.

AZZI (T.), *Open data et propriété intellectuelle, État des lieux au lendemain de l'adoption de la loi pour une République numérique*, Recueil Dalloz, 2017, n° 11, p. 583 à p. 592.

BENABOU (V.-L.), *La loi pour une République numérique et la propriété intellectuelle*, Dalloz IP/IT, 2016, n° 11, p. 531 à p. 536.

BENSAMOUN (A.) :

- *Création et données : différence de notions = différence de régime ?*, Dalloz IP/IT, 2018, n° 02, p. 85 à p. 89.
- *Rapport de la CNIL sur l'intelligence artificielle : une réflexion éthique*, Revue pratique de la prospective et de l'innovation, 2018, n° 01, p. 33 à p. 37.
- *Ceci est... une œuvre d'art ! La question des créations générées par une intelligence artificielle*, L'Observatoire, 2020, n° 55, p. 104 à p. 106.

BENSAMOUN (A.), MARTIAL-BRAZ (N.), *StopCovid : sortir des postures ! Point de vue sur l'avis de la CNIL*, Dalloz IP/IT, 2020, n° 05, p. 280 à p. 283.

BERANGER (J.), BOUADI (R.), *Approche éthico-juridique de l'usage des données médicales à caractère personnel*, Les Cahiers du numérique, vol. 10, 2014, n°02, p. 93 à p. 23.

BERNAULT (C.), *Ouverture des données publiques et propriété intellectuelle*, Dalloz IP/IT, 2018, n° 02, p.103 à p. 106.

BIOY (X.), *Le corps humain et la dignité*, Cahiers de la recherche sur les droits fondamentaux, 2017, n°15, p. 11.

BLOUD-REY (C.), *Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ?*, Recueil Dalloz, 2013, n°42, p. 2795.

BOISVERT (Y.), *Crise de confiance et crise de légitimité : de l'éthique gouvernementale à l'éthique publique*, Éthique de l'administration et du service public, Vol. 4, 2002, n° 1.

BOSSI-MALAFOSSE (J.), *Le cadre juridique du partage d'informations dans les domaines sanitaire et médico-social : état des lieux et perspectives*, Médecine & Droit, janvier - février 2013, p. 5.

BOULANGER (A.), *L'impact du « passe sanitaire » sur les droits et libertés fondamentaux des personnes*, Revue Juridique Personnes et Famille, 2021, n° 10.

BOURCIER (D.), DE FILIPPI (P.), *Vers un droit collectif sur les données de santé*, Revue de droit sanitaire et social, 2018, n°03, p. 444.

BOURDAIRE-MIGNOT (C.), *2018 : l'année du DMP pour tous ?*, Revue générale de droit médical, 2018, n°66, p. 19.

BOURGEOIS (M.), COUSIN (G.), *Les apports de la loi pour une République numérique en matière de propriété intellectuelle*, La semaine juridique - entreprise et affaires, 2016, n° 49, p. 32 à p. 37.

BOURGEOIS (M.), THIBIERGE (L.), *Droit de la donnée : plaidoyer pour un régime général*, La semaine juridique Entreprise et Affaires, 2020, n°20, p. 39.

BOUSTA (R.), *Contrôle constitutionnel de proportionnalité. La spécificité française à l'épreuve des évolutions récentes*, Revue française de droit constitutionnel, Vol. 88, 2011, n°04, p. 913.

BRUN (P.), *Responsabilité du fait personnel*, Répertoire de droit civil, mai 2015, actu. octobre 2020.

BUCKI (E.), CASANOVAS (G.), LANGARD (S.), *Les règles d'échange et de partage d'informations : aux limites de la démarche empirique*, Revue droit & santé, 2017, n° 79, p. 658.

CAIRE (A.-B.), *Le corps gratuit : réflexions sur le principe de gratuité en matière d'utilisation de produits et d'éléments du corps humain*, Revue de droit sanitaire et social, 2015, n°05, p. 865.

CAPODANO (J.), *Dossier médical partagé (DMP) et secret professionnel : les nouveaux enjeux*, Revue droit & santé, 2017, n° 76, p. 233.

CARON (C.), *Utilisation de la « balance des intérêts » pour résoudre les conflits de droits fondamentaux*, Recueil Dalloz, 2004, n°23, p. 1633.

CARRIERE (C.), *Le droit au secret médical : de la personne à la chose en passant par la propriété*, RDS, 2007, n°20, p. 716.

CASES (A.-S.), *L'e-santé : l'empowerment du patient connecté*, Journal de Gestion et d'Économie Médicales, Vol. 35, 2017, n°4-5, p. 137.

CHARDEAUX (M.-A.), *Nommer la prérogative d'usage des choses communes*, Recueil Dalloz, 2019, n°40, p. 2195.

CHATRY (S.), *Droits des producteurs des bases de données*, JurisClasseur Civil, Fasc. 1650, Annexe V° propriété littéraire et artistique, 1^{er} décembre 2018, actu. 1^{er} juin 2021.

CLEMENT-FONTAINE (M.), *L'union du droit à la protection des données à caractère personnel et du droit à la vie privée*, Légipresse, 2018, n°356, p. 19 à p. 24.

CLUZEL-METAYER (L.) :

- *La loi pour une République numérique : l'écosystème de la donnée saisi par le droit*, Actualité juridique Droit administratif, 2017, n°06, p. 340.
- *La construction d'un service public de la donnée*, Revue française d'administration publique, 2018, n°167, p. 491.
- *La datasurveillance de la Covid-19*, Revue de droit sanitaire et social, 2020, p. 919.

CLUZEL-METAYER (L.), FRANCOIS (A.), *La protection des données personnelles à l'épreuve de la télémédecine*, Revue de droit sanitaire et social, 2020, n°01, p. 51.

COMBREXELLE (J.-D.), *Le juge, l'état d'urgence sanitaire et les libertés*, La revue des juristes de sciences po, juin 2021, n°21, Dossier thématique n°09.

CORGAS-BERNARD (C.), *Responsabilité civile médicale et nouvelles pratiques numériques : L'exemple de la télémédecine*, Les petites affiches, 2014, n°164, p. 27.

CORNU (M.) :

- *Création scientifique et statut d'auteur*, Hermès, La Revue, Vol. 57, 2010, n°02, p. 85.
- *Ouverture des données : les trompe-l'œil de la loi*, Dalloz IP/IT, 2016, n° 11, p. 515 à p. 519.

DANIS-FATOME (A.), *Ordre public et protection des données à caractère personnel*, AJ contrat, 2019, n°8 et n°9, p.366.

DARAGON (E.), *Etude sur le statut juridique de l'information*, Recueil Dalloz, 1998, n°07, p. 63.

DEBIES (E.), *Big data de santé et autodétermination informationnelle : quelle articulation possible pour une innovation protectrice des données personnelles ?*, Revue française d'administration publique, 2018, vol. 3 n° 167, p. 565-574.

DEBOST (V.-C.), GIRAUDEAU (N.), VERON (P.), VIALLA (F.), *La réforme du Code de déontologie médicale*, RGDM, 2012, n° 44, p. 231.

DE GROVE-VALDEYRON (N.), *Les applications de traçage contre la covid-19 : l'exception française dans le contexte européen*, Revue générale de droit médical, 2020, n°76, p. 133.

DEGUERGUE (M.), *Télémédecine et responsabilités*, Revue de droit sanitaire et social, 2020, n°01, p. 33.

DEKEUWER-DEFOSSEZ (F.), *L'autorité parentale à l'épreuve de la loi Kouchner*, Revue générale de droit médical, 2004, n° 12, p. 99 à p. 104.

DE LAMBERTERIE (I.), *Débat éthique et juridique relatif à l'accès aux données génétiques*, Revue internationale d'éthique sociétale et gouvernementale, Vol. 6, Éthique publique, 2004, n° 02.

DESCHAMPS (J.-P.), FERRON (C.), ALLA (F.), DOUILLER (A.), *L'éducation pour la santé, parent pauvre de la politique de santé ?*, Santé Publique, Vol. 25, Supp 2013, n° 02, p. 81.

DESCHANEL (C.), *L'instauration d'un droit de propriété des données personnelles : vrai danger ou fausse utilité ?*, Revue Lamy Droit de l'immatériel, 2019, n°156, p. 35.

DESTREGUIL (M.), *Plaidoyer en faveur d'une approche propriétaire des données personnelles*, Revue Juridique Personnes et Famille, 2019, n°03, p. 05.

DIEU (F.), *Hospitalisation sous contrainte et encadrement thérapeutique de l'information délivrée au malade*, Revue de droit sanitaire et social, 2009, n°04, p. 688.

DJOUDI (J.), *Occupation*, Répertoire de droit civil, juillet 2018.

DOUNOT (C.), *La démesure du « pass sanitaire »*, Recueil Dalloz, 2021 p. 1387.

DOUVILLE (T.) :

- *Les dangers de la collecte des données de santé par les tiers intéressés (gafam, assureurs...)*, Journal du Droit de la Santé et de l'Assurance Maladie, 2018, n° 20, p. 12.
- *Les droits des personnes concernées en cas de transmission de leurs données à caractère personnel*, Revue Lamy Droit de l'Immatériel, 2018, n° 153, p. 33.
- *L'émergence des cyber-risques*, Archives de philosophie du droit, Vol. 62, 2020, n°01, p. 289.

DOUVILLE (T.), HERVOCHON (C.), NOËL (E.), PAQUIER (Y.), *Les vulnérabilités numériques*, Cahiers de la recherche sur les droits fondamentaux, 2020, n°18, p. 111.

DUHAMEL (G.), *Les excès de l'étatisme et les responsabilités de la médecine*, Revue des Deux Mondes, 1934, n°02, p. 277 à p. 299.

FASSIN (D.), HENCKES (N.), KEMPF (R.) et al., *La démocratie à l'épreuve de l'épidémie*, Esprit, 2020 n° 10, p. 81 à p. 106.

GALLOUX (J.-C.), *Réflexions sur la catégorie des choses hors du commerce: l'exemple des éléments et des produits du corps humain en droit français*, Les Cahiers de droit, Vol. 30, 1989. n°4, p. 1011.

GAULLIER (F.), *Le principe de finalité dans le RGPD : beaucoup d'ancien et un peu de nouveau*, Communication Commerce électronique, avril 2018, n° 4.

GAVANON (I.), LE MAREC (V.), *Application de contact tracing : « un choix individuel gage de responsabilité collective » encadré par le CEPD*, Dalloz actualité, 21 avril 2020.

GAY (L.), *La notion de « droits-créances » à l'épreuve du contrôle de constitutionnalité*, Cahiers du conseil constitutionnel, juin 2004, n°16.

GERVIER (P.), *La limitation des droits fondamentaux constitutionnels par l'ordre public*, Les nouveaux cahiers du Conseil constitutionnel, octobre 2014, n°45.

GINGRAS (Y.), KHELFAOUI (M.), *L'effet SIGAPS : la recherche médicale française sous l'emprise de l'évaluation comptable*, Zilsel, février 2021, n°08, p. 144.

GIOCANTI (D.), *Les différentes acceptions des termes "dossier médical" et, dans ce contexte, situation du dossier hospitalier*, Revue générale de droit médical, 2010, n°37, p. 161.

GORI (R.), *Le soin et la démocratie à l'épreuve du totalitarisme sanitaire*, Cliniques méditerranéennes, 2021, n° 103, p. 23 à p. 39.

GRAVEL (S.), DOUCET (H.), BATTAGLINI (A.), LAUDY (D.), BOUTHILLIER (M.-E.), BOUCHERON (L.), FOURNIER (M.), *Éthique et santé publique : Quelle place pour l'autonomie ?*, Responsabilité sociale et éthique de la recherche, Vol. 12, 2010, n° 01.

GROSSHOLZ (C.), *Hôpitaux : régimes de responsabilité et de solidarité. La responsabilité pour faute*, Répertoire de la responsabilité de la puissance publique, Dalloz, février 2018, actu. juin 2021.

GRÜNDLE (T.), *Le juge et le droit à la protection de la santé*, RDSS, 2010, n°05, p.835.

HASSLER (T.), *La crise d'identité des droits de la personnalité*, Les petites affiches, n°244, 7 décembre 2004, p. 3.

HENNION (S.), *Le partage du secret professionnel à l'ère du numérique*, Revue de droit sanitaire et social, 2020, n°01, p. 129.

HERVEG (J.), VERHAEGEN (M.-N.), POULLET (Y.), *Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique : les conditions d'une alliance entre informatique, vie privée et santé*, Revue de droit de la santé, 2002, n°02, p. 56 à p. 85.

HO DINH (A.-M.), *Le « vide juridique » et le « besoin de loi ». pour un recours à l'hypothèse du non-droit*, L'Année sociologique, Vol. 57, 2007, n° 2, p. 419.

HOERNI (B.) & BENEZECH (M.), *Les devoirs des patients*, La Presse Médicale, Vol. 33, 2004, n°2, p. 80.

KAHN (A.), *Le secret médical : d'Hippocrate à internet*, Recueil Dalloz, 2009, n°39, p. 2623.

KEELING (M.), BELLEFLEUR (O.), *Le principe de réciprocité : comment peut-il éclairer la santé publique et les politiques publiques favorables à la santé ?*, Note documentaire, Centre de collaboration nationale sur les politiques publiques et la santé du Québec, 2014.

KUMAR (A.), PRASOON (P.), KUMARI (C.), PAREEK (V.), FAIQ (M. A.), NARAYAN (R. K.), KULANDHASAMY (M.), KANT (K.), *SARS-CoV-2-specific virulence factors in COVID-19*, Journal of Medical Virology, March 2021, p. 1343.

LALLET (A.), NGUYEN DUY (P.) :

- *Communication des documents administratifs*, Répertoire de contentieux administratif, juin 2019.
- *Diffusion et réutilisation des informations publiques : « Open data » - données ouvertes*, Répertoire de contentieux administratif, septembre 2020.

LANNA (M.), *Crise sanitaire - Les données personnelles de santé, nouvelle composante de la prévention sanitaire ?*, Droit Administratif, 2020, n° 6, étude 7.

LATINA (M.), *Contrat : généralités (Civ.)*, RDT civ., mai 2017, actu. février 2020.

LAUDE (A.) :

- *Le consommateur de soins*, Recueil Dalloz, 2000, n°26, p. 415.
- *Le code de déontologie médicale enfin modifié !*, Recueil Dalloz, 2012, n°26, p.1694.
- *Le patient entre responsabilité et responsabilisation*, Les Tribunes de la santé, 2013, n°41, p. 79.

LEPAGE (A.), *Droits de la personnalité*, Répertoire de droit civil, septembre 2009, actu. janvier 2021.

LEQUESNE ROTH (C.), *Covid-19 et applications de traçage : à la croisée des libertés et des technologies*, Recueil Dalloz, 2020, p.1096.

LEQUILLERIER (C.), *L'impact de l'intelligence artificielle sur la relation de soin*, Journal de Droit de la Santé et de l'Assurance Maladie, 2017, n° 17, p. 14 à p. 20.

LE REUN (R.), *Les métamorphoses numériques de l'hôpital. Le soignant et l'information sans papiers*, Ethique et santé, 2019, n°16, p. 44.

LESAULNIER (F.), *Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données*, Médecine & Droit, 2019, n°158, p. 103.

LEUZZI-LOUCHART (C.) :

- *Les devoirs du patient : l'échange réciproque d'information*, Revue générale de droit médical, 2013, n°49, p. 133.
- *Des dossiers médicaux au dossier hospitalier : la définition du dossier médical par la réglementation du contenu*, Revue générale de droit médical, 2014, n°53, p. 29.

LIBCHABER (R.), *Biens (Civ.)*, Répertoire de droit civil, mai 2016, actu. décembre 2019.

LOISEAU (G.) :

- *Typologie des choses hors du commerce*, Répertoire de droit civil, 2000, n°01, p. 47.
- *Pour un droit des choses*, Recueil Dalloz, 2006, n°44, p. 3015.
- *La crise existentielle du droit patrimonial à l'image*, Recueil Dalloz, 2010, n°08, p. 450.

LUCAS-SCHLOETTER (A.) :

- *Le « domaine commun informationnel »*, Dalloz IP/IT, 2018, n° 02, p. 90 à p. 93.
- *Synthèse - Objet du droit d'auteur. Titulaires du droit d'auteur*, JurisClasseur Propriété littéraire et artistique, 01 avril 2021.

MACREZ (F.), *Contrats de consultation et d'exploitation de bases de données*, JurisClasseur Communication, , Fasc. 700, 1^{er} octobre 2016

MALLET-POUJOL (N.) :

- *Appropriation de l'information : l'éternelle chimère*, Recueil Dalloz, 1997, n°38, p. 330.
- *Droit à et droit sur l'information de santé*, In *Le droit des données de santé*, Actes du colloque de l'Association française de droit de la santé organisé à Paris le 25 mars 2004, RGDM, 2004, n° 04, p. 77 à p. 95.

MAMZER BRUNEEL (M.-F.), HERVE (C.), *La requalification des données de soins en données de recherche : enjeux éthiques et blocages normatifs*, Ethics, Medicine and Public Health, 2017, n°3, p. 83.

MARTIAL-BRAZ (N.) :

- *Le renforcement des droits de la personne concernée*, Dalloz IP/IT, 2017, n°05, p. 253 à p. 259.
- *Le contrat entre responsable de traitement et sous-traitant*, Dalloz IP / IT, 2021, n° 04, p. 181 à p. 187.

MATTATIA (F.), YAÏCHE (M.), *Être propriétaire de ses données personnelles : peut-on recourir aux régimes traditionnels de propriété ? (partie I)*, Revue Lamy Droit de l'immatériel, 2015, n°114, p. 60.

MERCIER (V.), *USUFRUIT . – Prérogatives de l'usufruitier . – Droits de l'usufruitier (usage et jouissance)*, JurisClasseur Civil, Fasc. 10, juillet 2019.

MERLAND (G.), *L'intérêt général, instrument efficace de protection des droits fondamentaux ?*, Cahiers du Conseil constitutionnel, 2004, n° 16.

METALLINOS (N.), *Covid-19 : l'état d'urgence sanitaire à l'épreuve du droit de la protection des données à caractère personnel*, LexisNexis, Communication - Commerce Electronique, 2020, n° 5, étude n°9.

MINCKE (C.), *Effets, effectivité, efficience et efficacité du droit : le pôle réaliste de la validité*, Revue interdisciplinaire d'études juridiques, Vol. 40, 1998, n°01, p. 115.

MONTET (I.), *Le dossier médical en psychiatrie ambulatoire*, L'information psychiatrique, Vol. 84, 2008, n°4, p. 354.

MONZIOLS (G.), *Le dossier médical partagé face aux logiciels et applications mobiles du secteur privé*, Revue générale de droit médical, 2019, n°27, p. 149.

MORET-BAILLY (J.), *La déontologie médicale, de la résistance à la contre-offensive (à propos du décret du 7 mai 2012 portant modification du code de déontologie médicale)*, Revue de droit sanitaire et social, 2012, n°06, p. 1074.

MORLET-HAÏDARA (L.), :

- *Le nouveau cadre légal de l'équipe de soins et du partage des données du patient*, Revue de droit sanitaire et social, 2016, n°06, p. 1103.
- *Les usages du big data en santé et les exigences du respect des droits des patients*, Revue Pratique de la Prospective et de l'innovation , 2019, n°02, p. 37.

NICOLAS (G.), *L'accès au dossier hospitalier par le patient et sa famille : les cas particuliers (patient mineurs, majeurs protégés, patients décédés)*, Revue générale de droit médical, 2010, n°37, p. 185.

NONNOU (E. G.), *La patrimonialité des données personnelles*, La revue Lexbase Afrique-OHADA, 2020, n°38.

OCHOA (N.), *Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition*, Revue française de droit administratif, 2015, n°06, p. 1157.

PAMBOUKIS (H.), *Acte public étranger*, Répertoire de droit international, septembre 2019.

PASSA (J.), *La propriété de l'information : un malentendu ?*, Droit et Patrimoine, 2001, n° 91

PAWLOTSKY (A.), *L'utilisation des données personnelles dans le cadre de la lutte contre l'épidémie de Covid-19, un risque pour les droits et libertés ?*, La Revue des droits de l'homme, Actualités Droits-Libertés, avril 2020.

PECHILLON (E.), *L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ?*, L'information psychiatrique, Vol. 91, 2015, n°08, p. 645 à p. 649.

PELTIER (V.), *Révélation d'une information à caractère secret . – Conditions d'existence de l'infraction . – Pénalités*, JurisClasseur Pénal, Fasc. 20, mai 2015, actu. mai 2021.

PENIGAUD DE MOURGUES (T.), *Intérêt commun ou intérêt général ? De l'enjeu d'une décision terminologique chez Rousseau*, Astéris, 2017, n°17.

PERRAY (R.), *DONNÉES À CARACTÈRE PERSONNEL Principes fondamentaux relatifs aux traitements de données à caractère personnel. – Minimisation*, JurisClasseur Communication, Fasc. 932-30, 19 Juillet 2021.

PEUGEOT (V.), *Données personnelles : sortir des injonctions contradictoire*, 13 avril 2014. Article disponible en ligne sur le site [www.vecam.org]. Consulté le 4 février 2021.

PIEDELIEVRE (S.), *Fruits*, Répertoire de droit civil, octobre 2014.

PY (B.) :

- *Secret professionnel*, Répertoire de droit pénal et de procédure pénale, 2003, actu. 2017.
- *Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel*, Revue droit & santé, 2013, n°50 hors-série, p. 161 s.
- *Les épidémies et le secret professionnel*, Revue droit & santé, 2020, n° 96, p. 700.
- *Fallait-il sacrifier le secret professionnel sur l'autel de la santé publique ?*, Médecine & Droit, 2021, n° 166, p. 1 à p. 2.
- *Le secret professionnel est-il un droit du patient ?*, Revue de droit sanitaire et social, 2022, n°02, p. 225 à p. 234.

PY (B.), OLECH (V.), *La loi 24 juillet 2019 et le virage numérique, le DMP de troisième génération et l'espace numérique*, Revue Droit & Santé, 2019, n° 92, p. 930 à p. 935.

PY (B.), SEGURA (J.), *L'obligation d'information est le devoir incombant à la partie qui détient une information utile à l'autre partie de la lui délivrer, si cette information peut avoir une influence sur son consentement*, Revue droit & santé, 2005, n°8, p. 505.

REVET (T.), *Le corps humain est-il une chose appropriée ?*, RTD civ., 2017, n° 03, p. 587.

REY-SALMON (C.), *Secret médical et personnes vulnérables : le cas du mineur*, Recueil Dalloz, 2009, n°39, p. 2651.

RIVIERE (V.), *Refus par un mineur de la communication de son dossier médical*, Revue droit & santé, 2007, n°16, p. 245.

ROBIN (A.), *Le patrimoine scientifique de l'Etat, un patrimoine immatériel en quête de statut*, Revue Communication Commerce Électronique, 2014, n°10, étude 18.

ROMANO (V.), MACINTOSH (A.), SUEUR (C.), *Stemming the flow: information, infection and social evolution*, Trends in Ecology & Evolution, Vol. 35, 2020, n°10, p. 849.

ROUSSET (G.), *Le droit à l'information de l'utilisateur et du patient depuis les lois des 2 janvier et 4 mars 2002*, Revue de droit sanitaire et social, 2012, n°3, p. 431.

SAINT MARTIN (A.) :

- *Le secret médical et le patient (I) le patient (a priori) maître du secret professionnel médical*, Revue droit & santé, 2010, n°34, p. 108.
- *Le secret médical et le patient (II)*, Revue droit & santé, 2010, n° 36, p. 326.

SAINT-PAU (J.-C.), *L'article 9 du code civil : matrice des droits de la personnalité*, Recueil Dalloz, 1999, p. 541.

SAISON-DEMARS (J.), *Une nouvelle réforme en faveur de l'unité du système de santé*, Actualité juridique de droit administratif, 2019, n°42, p. 2488.

SAISON-DEMARS (J.), **BOUGHRIET (N.)**, *Les notes personnelles des médecins : un point d'incertitude dans la détermination du contenu transmissible du dossier*, Revue générale de droit médical, 2014, n°53, p. 43.

SAUVE (J.-M.), *Le principe de proportionnalité, protecteur des libertés*, Les Cahiers Portalis, Vol. 5, 2018, n°01, p. 09.

SCHÜTZ (R.-N.), *Inaliénabilité*, Répertoire de droit civil, juin 2014.

SÉRIAUX (A.), *Propriété*, Répertoire de droit civil, juin 2016.

SFERLAZZO-BOUBLI (K.), *Le respect du contradictoire l'emporte sur la protection du tiers demandeur d'une hospitalisation sans consentement*, Revue droit & santé, 2016, n° 73, p. 813.

SOREL (J.-M.), *Équité*, Répertoire de droit international, juillet 2017.

STEVENIN (P.), *La santé par l'éducation*, Les Sciences de l'éducation - Pour l'Ère nouvelle, Vol. 39, 2006, n°01, p. 75.

SUPIOT (E.), *Du secret médical à la mise à disposition des données de santé - le Health data hub*, Revue des contrats, 2020, n°117, p. 84.

TÜRK (P.), *L'autodétermination informationnelle : un droit fondamental émergent ?*, Dalloz IP / IT, 2020, n°11, p. 616 à p. 620.

VASSEUR-LAMBRY (F.), *Le secret professionnel/médical : une protection forte dans l'intérêt du patient*, Revue générale de droit médical, 2018, n°69, p. 97.

VAYR (J.), *Les données de santé : un enjeu pour le futur*, Les petites affiches, septembre 2016, n°120, p. 4.

VERON (P.), *Dissimulation par la patiente de son état de santé et exclusion de la responsabilité du praticien : vers un devoir de collaboration du patient ?*, Revue droit & santé, 2012, n°49, p. 603.

VIALLA (F.) :

- *La communication des informations personnelles au regard des dispositions de l'article L.1111-7 du code de la santé publique, Réflexions à propos de l'arrêt de la cour administrative d'appel de Paris du 30 septembre 2004*, Revue générale de droit médical, 2005, n°16, p. 195.
- *Les restrictions à l'accès au dossier médical*, Revue droit & santé, 2009, n°30, p. 341.
- *Le secret partagé*, Revue droit & santé, 2016, n°02, p. 52.

VIALLA (F.), FAURE (M.), MARTINEZ (E.), BOURRET (R.), VAUTHIER (J.-P.), *Mineur et secret médical – Le secret sur son état de santé demandé par le mineur à l'égard de ses parents : de la reconnaissance d'un droit à sa mise en œuvre concrète*, Médecine & Droit, 2015, n° 133, p. 79 à p. 104.

ZORN-MACREZ (C.) :

- *"Chronique martienne" des données de santé numérisées. Brèves observations sur une réglementation surréaliste*, Revue droit & santé, 2010, n° 36, p. 331.
- *Les « notes personnelles » du médecin ? : les conséquences d'un décret d'arrière-garde*, Revue droit & santé, 2012, n°49, p. 579.
- *État d'urgence pour les données de santé (II) : sidep et contact covid*, Dalloz actualité, 26 mai 2020.

V. Rapports, Etudes, Communications, Avis et Documents assimilés

AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPEENNE,
Application de la Charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale, Orientations, 2019.

AGENCE DES SYSTEMES D'INFORMATION PARTAGES EN SANTE:

- *Référentiel d'identification des acteurs sanitaires et médico-sociaux*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), V 1.0, décembre 2014.
- *Référentiel d'authentification des acteurs de santé*, Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), V 2.0, décembre 2014.
- *Guide Gestion des habilitations d'accès au SI*, Politique générale de sécurité des systèmes d'information de santé (PGSSI-S), V. 1.0, janvier 2017.

AGENCE NATIONALE D'ACCREDITATION ET D'EVALUATION EN SANTE,
Evaluation des pratiques professionnelles dans des établissements de santé, Dossier Du Patient : Réglementation et recommandations, juin 2003. Disponible sur le site [www.has-sante.fr]. Consulté le 1^{er} décembre 2021.

CAISSE NATIONALE DE SOLIDARITE POUR L'AUTONOMIE, AGENCE DES SYSTEMES D'INFORMATION PARTAGES EN SANTE, *Échange et partage des données de santé, Retour d'expérience des bonnes pratiques sur l'échange et le partage des données*, novembre 2018. Disponible en ligne sur le site [www.esante.gouv.fr]. Consulté le 03 décembre 2021.

CHAMBRE DISCIPLINAIRE NATIONALE DE L'ORDRE DES MEDECINS :

- 24 juin 2004, n°8856.
- 17 mars 2016, n°12639.

COMITE CONSULTATIF NATIONAL D'ETHIQUE :

- *Numérique & Santé Quels enjeux éthiques pour quelles régulations ?*, 19 novembre 2018.
- *Données massives et santé : Une nouvelle approche des enjeux éthiques*, Avis n°130, 29 mai 2019.
- *Éthique et santé publique*, Avis 137, 20 mai 2021, actu. 02 septembre 2021.

COMITE DE CONTROLE ET DE LIAISON COVID-19 :

- *Avis du 28 juillet 2021 portant sur le projet de loi n° 4386 relatif à la gestion de la crise sanitaire.*
- *Point de vigilance du 20 avril 2021 sur le Pass sanitaire Covid-19.*
- *Avis du 9 février 2021 sur les systèmes d'information et campagne de vaccination.*
- *Avis du 15 septembre 2020 pour un système d'information au service d'une politique cohérente de lutte contre l'épidémie.*
- *Avis du CCL du 19 octobre 2020 sur les évolutions nécessaires des outils numériques citoyens de lutte contre la Covid-19.*
- *Avis du 15 Décembre 2020 sur le projet de décret modifiant le décret n°2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid ».*

COMITE NATIONAL PILOTE D'ETHIQUE DU NUMERIQUE, *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, Bulletin de veille n°1, 7 avril 2020.

COMMISSION D'ACCES AUX DOCUMENTS ADMINISTRATIFS :

- **Avis**, 1^{er} avril 2004, n° **20041039**.
- **Avis**, 15 avril 2004, n° **20041645**.
- **Avis**, 25 août 2005, n° **20053225**.
- **Avis**, 11 mai 2006, n° **20062245**.
- **Avis**, 31 juillet 2008, n° **20082716**.
- **Conseil**, 18 juin 2009, n° **20091209**.
- **Conseil**, 24 janvier 2013, n° **20130176**.
- **Avis**, 21 février 2013, n° **20130447**.
- **Avis**, 18 septembre 2014, n° **20142924**.
- **Avis**, 5 mars 2015, n° **20150002**.
- **Conseil**, 21 mai 2015, n° **20151096**.
- **Conseil**, 29 juin 2016, n° **20162674**.
- **Avis**, 17 novembre 2016, n° **20164178**.
- **Avis**, 06 décembre 2018, n° **20183141**.
- **Avis**, 10 janvier 2019, n° **20183756**.

COMMISSION EUROPEENNE, *Avis n° 13 du 30 juillet 1999 : Aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*, Journal International de Bioéthique, Vol. 12, 2001, n°03, p. 113.

COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME, Avis du 22 mai 2018 sur la protection de la vie privée à l'ère du numérique, *JORF*, 3 juin 2018, texte 63.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES :

- **Délibération n° 2016-047** du 25 février 2016 suite à la demande d'autorisation n°1894953.
- **Délibération n° 2016-258** du 21 juillet 2016 portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'un traitement de données à caractère personnel dénommé « dossier médical partagé » (demande d'avis n° 16017107), *JORF* n°268, 18 novembre 2016, texte n° 37.
- **Délibération n° 2019-008** du 31 janvier 2019 portant avis sur un projet de loi relatif à l'organisation et à la transformation du système de santé.
- **Délibération n° 2020-046** du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid ».
- **Délibération n° 2020-051** du 8 mai 2020 portant avis sur un projet de décret relatif aux systèmes d'information mentionnés à l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire, *JOFR* n°117, 13 mai 2020, texte n°74.
- **Délibération n° 2020-056** du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », *JORF* n°131, 30 mai 2020, texte n°106.
- **Délibération n° 2020-081** du 18 juin 2020 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux, *JORF*, 28 juillet 2020, texte 94.
- **Délibération n° 2020-087** du 10 septembre 2020 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19.
- **Délibération de la formation restreinte n° SAN-2020-014** du 7 décembre 2020.
- **Délibération de la formation restreinte n° SAN-2020-015** du 7 décembre 2020.
- **Délibération n° 2021-004** du 14 janvier 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19.
- **Délibération n° 2021-054** du 12 mai 2021 portant avis sur le projet de mise en place d'un passe sanitaire conditionnant l'accès à certains lieux, évènements ou établissements impliquant de grands rassemblements de personnes.
- **Délibération n° 2021-062** du 27 mai 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19.

- **Délibération n° 2021-077** du 1er juillet 2021 portant avis sur un projet de décret modifiant le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions et le 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, *JORF* n°0162, 14 juillet 2021, texte n°103.
- **Délibération n° 2021-097** du 6 août 2021 portant avis sur un projet de décret modifiant le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire et le décret n° 2021-901 du 6 juillet 2021 relatif au traitement automatisé de données à caractère personnel dénommé « Convertisseur de certificats », *JORF* n°183, 8 août 2021, texte n° 93.
- **Délibération n° 2021-139** du 21 octobre 2021 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19.

CONSEIL D'ETAT :

- Avis n° 400104 du 1^{er} mai 2020 sur un projet de loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions.
- Avis n° 403629 du 19 juillet 2021 sur un projet de loi relatif à la gestion de la crise sanitaire.

CONSEIL D'ETAT, *Étude annuelle 2014 : le numérique et les droits fondamentaux*, Documentation française, 2014, 446 pp. Disponible en ligne sur le site [www.conseil-etat.fr]. Consulté le 03 décembre 2021.

CONSEIL D'ETAT, CONSEIL GENERAL DE L'ECONOMIE ET DE L'INSPECTION GENERALE DES FINANCES, *Rapport relatif aux données d'intérêt général*, septembre 2015.

CONSEIL NATIONAL DE L'ORDRE DES MEDECINS, *Échange et partage d'information au sein de l'équipe de soins prenant en charge une personne*, Recommandations, février 2017. Disponible en ligne sur le site [www.conseil-national.medecin.fr]. Consulté le 03 décembre 2021.

CONSEIL NATIONAL DE L'ORDRE DES MEDECINS, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES :

- *Guide pratique sur la protection des données personnelles*, juin 2018. Disponible sur le site [www.cnil.fr]. Consulté le 1^{er} décembre 2021.

CONSEIL SCIENTIFIQUE COVID-19 :

- *Avis du 20 avril 2020 relatif à la sortie progressive de confinement prérequis et mesures phares.*
- *Avis du 20 octobre 2020 relatif à un nouvel ensemble numérique pour lutter contre le SARS-CoV-2.*
- *Avis du 3 mai 2021 relatif à l'utilisation d'un pass sanitaire lors de grands rassemblements.*
- *Avis du 6 juillet 2021 Réagir maintenant pour limiter une nouvelle vague associée au variant Delta.*
- *Note d'alerte du 20 août 2021 relative à la fin de la période estivale et pass sanitaire rentrée de septembre 2021.*

CONTRÔLEUR EUROPEEN DE LA PROTECTION DES DONNEES :

- *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017.
- *Lignes directrices portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel*, décembre 2019.
- *Letter concerning the European Commission's draft Guidance on apps supporting the fight against the Covid-19 pandemic*, 14 avril 2020.
- *Lignes directrices 07/2020 sur les concepts de responsable du traitement et de sous-traitant dans le RGPD, V. 2.0*, 7 juillet 2021.

CUGGIA (M.), POLTON (D.), WAINRIB (G.), COMBES (S.), *Mission de préfiguration du Health Data Hub*, Rapport officiel du Ministère des solidarités et de la santé, 12 octobre 2018.

DEFENSEUR DES DROITS, 3 novembre 2017, n°2017-290.

DIRECTION GENERALE DE L'OFFRE DE SOINS, *Programme Hôpital numérique. Boîte à outils pour l'atteinte des pré-requis – Fiches pratiques*, octobre 2012. Disponible sur le site [solidarites-sante.gouv.fr]. Consulté le 1^{er} décembre 2021.

EVIN (C.), CHARLES (B.), DENIS (J.-J.), *Rapport n°3263 fait au nom de la commission des affaires culturelles, familiales et sociales sur le projet de loi relatif aux droits des malades et à la qualité du système de santé n°3258*, Assemblée Nationale, Vol. I, Titre 1^{er} Démocratie sanitaire, 26 septembre 2001.

FAUVEL (V.), THIEULIN (B.), PA (S.), HARTMANN (C.), BERTHET (C.), BONNET (Y.), *La santé, bien commun de la société numérique*, Rapport remis par le CNNum à la Ministre Affaires sociales, de la Santé et des Droits des femmes, octobre 2015. Disponible en ligne sur le site [www.cnnumerique.fr]. Consulté le 03 décembre 2021.

FERAL-SCHUHL (C.), PAUL (C.), *Numérique et libertés : un nouvel âge démocratique*, Rapport d'information déposé par la commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, Assemblée nationale, octobre 2015.

GAGNEUX (M.), *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé*, Recommandations à la ministre de la santé, de la jeunesse, des sports et de la vie associative, avril 2008.

GIRAUD (F.), DERIOT (G.), LORRAIN (J.-L.), *Rapport n°174 fait au nom de la commission des affaires sociales sur le projet de loi relatif aux droits des malades et à la qualité du système de santé*, Sénat, 16 janvier 2002.

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES :

- *Opinion 03/2013 on purpose limitation*, 02 avril 2013.
- *Avis 05/2014 sur les Techniques d'anonymisation*, 10 avril 2014.
- *Lignes directrices sur la transparence au sens du règlement (UE) 2016/679*, 29 novembre 2017, actu. 11 avril 2018.

GUEDON-MOREAU (L.), *Guide de bonnes pratiques de télésurveillance des dispositifs électroniques cardiaques implantables*, Société française de cardiologie, 5 novembre 2019. Disponible en ligne sur le site [www.sfcardio.fr]. Consulté le 20 août 2020.

HAUTE AUTORITE DE SANTE :

- *Annoncer une mauvaise nouvelle*, Service évaluation des pratiques, février 2008
- *Un guide pour faciliter la communication entre professionnels de santé*, octobre 2014. Disponible en ligne sur le site [www.has-sante.fr]. Consulté le 02 décembre 2021.
- *Identification du patient à toutes les étapes de sa prise en charge*, 26 juin 2017. Disponible en ligne sur le site [www.has-sante.fr]. Consulté le 04 mars 2020.

LEGLEYE (S.), ROLLAND (A.), Une personne sur six n'utilise pas Internet, plus d'un usager sur trois manque de compétences numériques de base, INSEE Première, n°1780, 30 octobre 2019.

MILON (A.), *Rapport n°524 fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé*, Sénat, 22 mai 2019.

PLANETE PUBLIQUE, *Pour un débat citoyen sur la santé plus actif*, Rapport d'étude commandé par le Ministère de la santé, de la jeunesse et des sports, 7 juillet 2011.

PON (D.), COURY (A.), *Accélérer le virage numérique*, Stratégie de transformation du système de santé, Rapport final fait au nom du Ministère des Solidarités et de la Santé, 18 septembre 2018.

RIST (S.), MESNIER (T.), *Rapport n°1767 fait au nom de la commission des affaires sociales sur le projet de loi relatif à l'organisation et à la transformation du système de santé*, Vol. I, Assemblée nationale, 14 mars 2019.

VÉRAN (O.), LACLAIS (B.), TOURAINE (J.-L.), GEOFFROY (H.), FERRAND (R.), *Rapport n°2673 fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé*, Assemblée nationale, 20 mars 2015.

VILLANI (C.), LONGUET (G.), *Rapport au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur l'intelligence artificielle et les données de santé*, Compte rendu de l'audition publique du 21 février 2019 et de la présentation des conclusions du 21 mars 2019.

VIRIOT-BARRIAL (D.), *Dignité de la personne humaine*, Répertoire de droit pénal et de procédure pénale, juin 2014, actu. septembre 2020.

WILLMANN (C.), *Conditions de travail et d'hébergement contraires à la dignité humaine*, Répertoire de droit pénal et de procédure pénale, octobre 2003, actu. mars 2014.

ZENATI (F.), *Pour une rénovation de la théorie de la propriété*, Revue trimestrielle de droit civil, Dalloz, 1993, n°02, p. 305.

VI. Décisions de jurisprudence

1. Cour de justice de l'Union européenne

CJCE, 15 juillet 1964, **aff. 6/64**, *Flaminio Costa contre E.N.E.L*, Rec. Lebon, p. 1141.

CJCE, 9 novembre 2004, **aff. C-203/02**, *The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd* : Propriété industrielle, 2005, n° 01, comm. 7, P. Kamina ; CCE, 2005, n° 01, comm. 2, C. Caron ; RTD com., 2005, n° 01, p. 90, obs. F. Pollaud-Dulian.

CJUE, 1er décembre 2011, **aff. C-145/10**, *Painer c/ Axel Springer AG* : CCE, 2012, comm. 26, C. Caron ; Prop. intell., 2012, n° 01, p. 30, obs. A. Lucas ; D., 2012, n° 07, p. 471, note N. Martial-Braz, *infra*, obs. J. Daleau ; RTD com., 2012, n° 01, p. 109, obs. F. Pollaud-Dulian.

CJUE, 21 juin 2012, **aff. C-84/11**, *Marja-Liisa Susisalo, Olli Tuomaala, Merja Ritala* : Europe, 2012, n° 8-9, comm. 321, note A. Rigaux ; RTD Eur., 2013, n° 03, p. 679, note F. Benoît-Rohmer.

CJUE, 6 septembre 2012, **aff. C-544/10**, *Deutsches Weintor eG c/ Land Rheinland-Pfalz* : Europe, 2012, comm. 430, obs. S. Roset ; RD rur, 2013, n° 412, comm. 61, F. Barthe ; RD rur. 2013, n° 413, comm. 88, N. Olszak.

CJUE, Gr. Ch., 13 mai 2014, **aff. C-131/12**, *Google Spain* : AJDA, 2014, n° 20, p. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D., 2014, n° 25, p. 1476, note V.-L. Benabou et J. Rochfeld et p. 1481, note N. Martial-Braz et J. Rochfeld ; D., 2014, n° 40, p. 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; AJCT, 2014, n° 10, p. 502, obs. O. Tambou ; JCP E, 2014, 1326, note M. Griguer et 1327, note G. Busseuil ; CCE, 2014, étude 13, A. Debet ; RLDI, 2014, n° 106, 3535 note C. Castets-Renard, 3536, note D. Forest et 3537, note A. Casanova.

CJUE, 24 septembre 2019, **aff. C-136/17** : Gaz. Pal., 2020, n° 06, p. 28, P. Piot ; JCP E, 2019, n° 40, act. 633 ; CCE, 2020, n° 02, étude 3, G. Desgens-Pasanau.

CJUE, 24 septembre 2019, **aff. C-507-17** : Gaz. Pal., 2020, n° 06, p. 31, P. Piot ; D., 2019, n° 36, p. 2022, note J.-L. Sauron ; D., 2020, n° 09, p. 515, note T. Douville ; Légipresse, 2019, n° 377, p. 687, note N. Mallet-Poujol.

CJUE, 16 juillet 2020, **aff. C-311/18**, *Data Protection Commissioner c/ Facebook Ireland Ltd, Maximillian Schrems* : JCP G, 2020, n° 41, 1116, note N. Martial-Braz ; Dalloz actu., 2020, obs. C. Crichton ; D., 2020, p. 2432, note C. Castets-Renard ; AJ contrat, 2020, p. 436, obs. T. Douville ; Dalloz IP/IT, 2020, p. 640, obs. B. Bertrand et J. Sirinelli ; RTD eur., 2021, p. 175, obs. B. Bertrand ; LPA, 2020, n° 243, p. 08, A. Rolin.

2. Cour européenne des droits de l'homme

CEDH, 25 février 1997, n° **22009/93**, *aff. Z. c. Finlande* : JCP G, 1998, I, 107, n° 35, chron. F. Sudre ; RSC, 1998, n° 02, p. 385, obs. R. Koering-Joulin.

CEDH, 27 août 1997, **74/1996/693/885**, *aff. M.S. c. Suède*, cons. 41 : AJDA, 1998, n° 01, p. 37, chron. J.-F. Flauss ; D., 2000, n° 24, p. 521, note I. Laurent-Merle.

CEDH, Gr. Ch., 16 février 2000, n° **27798/95**, *aff. Amman c. Suisse* : AJDA, 2000, n° 12, p. 1006, chron. J.-F. Flauss ; RFDA, 2001, n° 06, p. 1250, chron. H. Labayle et F. Sudre.

CEDH, Gr. Ch., 10 mai 2001, n° **25781/94** : AJDA, 2001, n° 12, p. 1060, chron. J.-F. Flauss.

3. Conseil constitutionnel

Décision n° 74-54 DC du 15 janvier 1975, *Loi relative à l'interruption volontaire de la grossesse* : D., 1975, p. 529, note Hamon.

Décision n° 79-107 DC du 12 juillet 1979, *Loi relative à certains ouvrages reliant les voies nationales ou départementales*, Rec. p. 31 ; RD publ., 1979, p. 1728.

Décision n° 90-283 DC du 8 janvier 1991, *Loi relative à la lutte contre le tabagisme et l'alcoolisme*, Rec. Lebon ; RDSS, 1991, n°02, p. 204, J.-S. Cayla ; AJDA, 1991, n° 05, p. 382, comm. P. Wachsmann.

Décision n° 91-296 DC du 29 juillet 1991, *Loi portant diverses mesures d'ordre social*, Rec. Lebon, p. 102.

Décision n° 93-325 DC du 13 août 1993, *Loi de la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France* : D., 1994, n° 13, p. 111, obs. D. Maillard Desgrées du Loû ; Dr. soc., 1994, n° 01, p. 69, étude J.-J. Dupeyroux et X. Prétot ; RFDA, 1993, n° 05, p. 871, note B. Genevois ; Rev. crit. DIP, 1994, n° 01, p. 01, ét. D. Turpin.

Décision n° 94-343/344 DC du 27 juillet 1994, *Loi relative au respect du corps humain et loi relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal*.

Décision n° 2000-434 DC du 20 juillet 2000, *Loi relative à la chasse* : LPA, 2000, n° 146, p. 18, note J.-E. Schoettl ; D., 2001, n° 23, p. 1839, note. D. Ribes.

Décision n° 2004-504 DC du 12 août 2004, *Loi relative à l'assurance maladie* : JCP A, 2004, n° 37, act. 1565.

Décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, Cons. 8 ; JCP A, 2012, act. 232 ; RLDI, 2012, n° 83, 2783, obs. L. Costes ; AJDA, 2012, p. 623, note R. Grand.

Décision n° 2012-248 QPC du 16 mai 2012 : JCP G, 2012, n° 22, 630 ; Dr. fam., 2012, n° 07, comm. 120, C. Neirinck ; AJDA, 2012, n° 19, p. 1036 ; S. Brondel ; D., 2013, n° 21, p. 1436, obs. F. Granet-Lambrechts ; AJ fam., 2012, n° 07-08, p. 406, obs. F. Chénéde ; RDSS 2012, n° 04, p. 750, note D. Roman ; RTD civ., 2012, n° 03, p. 520, obs. J. Hauser.

Décision n° 2013-675 DC du 9 octobre 2013, *Loi organique relative à la transparence de la vie publique*, cons. 26 : JCP A, 2014, 2018, etu. M. Verpeaux ; JCP G, 2013, n° 44-45, 1143 ; JCP A, 2013, n° 42, act. 800.

Décision n° 2013-681 DC du 5 décembre 2013, *Loi organique portant application de l'article 11 de la Constitution*, cons. 27 : JCP G, 2013, n° 52, 1365, obs. C. Tukov ; JCP A, 2013, n° 51, act. 951, obs. R. Bourrel ; JCP G, 2013, n° 05, doct. 152, étu. M. Verpeaux.

Décision n°2014-690 DC du 13 mars 2014, *Loi relative à la consommation*, cons. 51 : AJDA, 2014, p. 384.

Décision n° 2015-458 QPC du 20 mars 2015 : AJDA, 2015, n° 11, p. 611, note J.-M. Pastor ; JCP G, 2015, n° 22, p. 1055, note K. Foucher et V. Rachet-Darfeuille ; JCP G ; 2016, n° 36, p. 1607, chron. B. Mathieu et M. Verpeaux ; Dr. fam., 2015, n° 05, p. 03, note M. Lamarche ; RJPF, 2015, n° 05, p. 25, note A. Cheynet de Beaupré ; LPA, 2017, n° 21, p. 06, chron. M. Verpeaux.

Décision n° 2018-765 DC du 12 juin 2018, *Loi relative à la protection des données personnelles*, cons. 47 : JCP A, 2018, n° 24, act. 517 ; CCE, 2018, n° 09, comm. 65, A. Debet ; CCE, 2018, n° 10, comm. 76, A. Debet ; JCP S, 2018, n° 25, act. 202 ; JCP E, 2018, n° 25, act. 498.

Décision n° 2020-800 DC du 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions* : Gaz. Pal., 2016, n° 20, p. 16, note J. Gicquel ; AJDA, 2020, n° 22, p. 1242, note M. Verpeaux ; LDFP, 2020, n° 06, p. 01, obs. D. Larralde ; D., 2020, n° 22, p. 1262, obs. W. Maxwell et C. Zolynski.

Décision n° 2021-824 DC du 5 août 2021, *Loi relative à la gestion de la crise sanitaire* : D., 2021, n° 29, p. 1548 ; AJDA 2021, n° 44, p. 2610, note M. Verpeaux ; AJ fam., 2021, n° 09, p. 448, obs. A. Dionisi-Peyrusse.

4. Conseil d'Etat

CE, Section, 6 novembre 1936, *Arrighi et Dame Coudert*, Rec. Lebon, 1936, p. 966.

CE, 10 mai 1974, **n° 88032 et n° 88148**, *Denoyez et Chorques*, Rec. Lebon, 1974, p. 274 ; AJDA, 1974, p. 298, chron. M. Franc et M. Boyon.

CE, Ass., 19 mai 1983, **n° 40680**, *Bertin*, Rec. Lebon, 1983, p. 208 ; AJDA, 1983, p. 402, chron. Lasserre et Delarue.

CE, 12 octobre 1983, **n° 37768**, *Mme Rolland et autres*, Rec. Lebon, 1983, p. 855.

CE, 1^{er} mars 1989, **n° 67255**, *Époux Peyres*, Rec. Lebon, 1989, p. 65.

CE, 17 avril 1992, **n° 115688 et n° 116291**, Rec. Lebon T.

CE, 26 septembre 2005, **n° 270234** : AJDA, 2006, n° 06, p. 308, note J.-P. Markus.

CE, 10 avril 2009, **n° 289794**, *Rivoallan*, Rec. Lebon, 2009, p. 752 ; RDSS, 2009, n° 04, p. 688, note F. Dieu ; RDS, 2009, n° 30, p. 343, obs. F. Vialla.

CE, 2 septembre 2009, **n° 292783**, *M^{me} Peignien*, Rec. Lebon T. ; D., 2009, n° 34, p. 2283, C. De Gaudemont ; ADJA, 2009, n° 29, p. 1581, C. Biget ; RDSS, 2010, n° 01, p. 104, note F. Dieu.

CE, 24 août 2011, **n° 336382**, *HSBC Private Bank (Suisse) SA*, Rec. Lebon T., p. 939 ; RJEP, 2012, n° 699, comm. 40, note J. Boucher ; Dr. fisc., 2018, n° 45, comm. 443, note E. Crépey.

CE, Ass., 26 octobre 2011, **n° 317827**, *Association pour la promotion de l'image*, Rec. Lebon, 2011, p. 505, concl. J. Boucher ; AJDA, 2011, n° 36, p. 2036, note R. Grand ; LPA, 2011, no 248, p. 10, note F. Chaltiel ; AJDA, 2012, n° 01, p. 35, chron. M. Guyomar et X. Domino.

CE, 10 avril 2015, **n° 377207**, *Société Red Bull on Premise et autre*, Rec. Lebon T., p. 675 ; Dr. fisc., 2015, n° 26, comm. 434, note B. Bohnert.

CE, 10e et 9e ch., 08 février 2017, n° **389806**, *Société NotreFamille.com*, Lebon 2017 ; ADJA, 2017, n°06, p. 318, note D. Poupeau ; La Semaine Juridique Administrations et Collectivités territoriales, 2017, n° 41, comm. 2241, N. Gabayet ; AJ Collectivités Territoriales, 2017, n° 06, p. 350, note J.-D. Dreyfus.

CE, 10^e et 9^e ch., 07 juin 2017, n° **399446**, Rec. Lebon, T. ; ADJA, 2017, n° 30, p. 1697 ; JCP A, 2017, n° 41, comm. 2238, note A. Vinot-Landais ; JCP A, 2017, n° 24, act. 444, F. Tesson ; Revue Communication Commerce électronique, 2017, n° 10, comm. 84, N. Metallinos ; AJ fam., 2017, n° 09, p. 497, N. Levillain.

CE, 10^e et 9^e ch., 18 mars 2019, n° **406313**, Rec. Lebon, T. ; D., 2019, n° 30, p. 1673, obs. W. Maxwell et C. Zolynski ; Dalloz IP/IT, 2019, n° 07-08, p. 450, obs. D. Forest ; JCP A, 2019, n° 13, act. 209, C. Friedrich.

CE, 2^e et 7^e ch., 6 novembre 2019, n° **434376**, Rec. Lebon T. ; JCP A, 2019, n° 46, act. 710, M. Meyer ; Revue Communication Commerce électronique, 2020, n° 04, comm. 37, A. Debet.

CE, 6 décembre 2019, n° **405464**, Rec. Lebon T. ; Revue Communication Commerce électronique, 2020, n° 02, comm. 17, N. Metallinos.

CE, ord., 19 juin 2020, n° **440916**, Inédit Rec. Lebon ; AJDA, 2020, n° 23, p. 1262, note M.-C. De Montecler ; RLDI, 2020, n°172, 5904, obs. L. Costes.

CE, ord., 13 octobre 2020, n° **444937**, Inédit Rec. Lebon ; JCP A, 2021, n° 21, chron. 2163, J.-C. Videlin ; JCP A, 2021, n° 03, chron. 2019, L. Paravano et J.-L. Sauron ; Dalloz IP/IT, 2020, n° 11, p. 590, obs. N. Maximin ; AJDA, 2021, n° 13, p. 741, note L. Cluzel-Métayer ; RLDI, 2020, n° 176, comm. F. Zannotti et P. Navarro ; Dalloz IP/IT, 2021, n° 02, p. 103, obs. O. De Maison Rouge.

5. Cour de cassation

i. Chambre des requêtes

Cass. req., 28 janvier 1942, *Teyssier*, Gaz. Pal., 62, 1942, 1, p. 177 ; D. Recueil critique de jur., 1942, p. 63.

ii. Assemblée plénière et chambres réunies

Cass. Ass. Plén., 7 mars 1986, n°83-10.477, *Société Babolat c/ Pachot*, Bull. civ. ; D. 1986, p. 405, note B. Edelman ; RIDA, 1986, n° 03, p. 136, note A. Lucas.

iii. Chambres civiles

Civ. 1^{ère}, 18 octobre 1994, n° 92-17.770, Bull. civ., I, n° 298 ; RIDA, 1995, n° 04, p. 305, note A. Latreille.

Civ. 1^{ère}, 17 janvier 2008, n° 06-20.107, Bull. civ., I, n° 14 ; D., 2008, n° 18, p. 1256, note A. Dumery ; Revue Responsabilité civile et Assurances, 2008, n° 03, Mars 2008, comm. 110, C. Radé ; LPA, 2008, n°69, p. 10, note C. Youego.

Civ. 1^{ère}, 27 novembre 2008, n° 07-15.963, Bull. civ., I ; D., 2008, n° 44, p. 3085 ; Gaz. Pal., 2009, n° 71, p. 47, note V. Vuailat ; D., 2009, n° 19, p. 1302, obs. J. Penneau ; LPA, 2009, n° 178, p. 7, note F. Dekeuwer-Defossez.

Civ. 1^{ère}, 11 décembre 2008, n° 07-19.494, Bull. civ., I, n° 282 ; JCP G, 2009, n° 07, jur. II. 10025, note G. Loiseau ; Légipresse 2009, III, p. 109, note Th. Roussineau ; CCC, 2009, n° 03, comm. 68, obs. L. Leveneur ; RTD civ., 2009, n° 02, p. 342, obs. T. Revet, *supra* p. 295, obs. J. Hauser.

Civ. 1^{ère}, 3 juin 2010, n° **09-13.591**, Bull. civ. I n° 128 ; RGDM, 2010, n° 36, p. 233, note S. Prieur ; Recueil Dalloz, 2010, p. 1522, note P. Sargos, p. 2092, chron. N. Auroy et C. Creton ; RDSS, 2010, n° 05 p. 898, note F. Arhab-Girardin ; RTD civ. 2010, n° 03, p. 571, obs. P. Jourdain ; JCP 2010, p. 788, note S. Porchy-Simon, et Chron. resp. civ. 1015, spéc. n° 3 et 6 ; C. Corgas-Bernard, RLDC, oct. 2010, p. 21 ; LPA 17-18 août 2010, note R. Milawsk.

Civ. 1^{ère}, 20 janvier 2011, n° **09-68.042**, JurisData n° 2011-000527.

Civ. 1^{ère}, 20 octobre 2011, n° **10-21.251** : LEPI, 2012, n° 03, obs. F. Herpe.

Civ. 1^{ère}, 1^{er} décembre 2011, n° **09-15.819**, Bull. civ., I, n° 208 ; D., 2011, n° 44, p. 2995 ; RTD civ., 2012, n° 01, p. 131, obs. T. Revet ; RTD com., 2012, n° 01, p. 110, obs. F. Pollaud-Dulian.

Civ. 1^{ère}, 5 mars 2015, n° **14-13.292**, Bull. civ., I, n° 52 ; D., 2015, n° 11, p. 623 ; JCP G, 2015, n° 19, p. 927, note Bacache ; Gaz. Pal., 2015, n° 183, p. 18, comm. M. Mekki ; Gaz. Pal., 2015, n° 78, p. 26, note C. Berlaud.

Civ. 1^{ère}, 30 septembre 2015, n° **14-16.273**, Bull. civ., I, n° 228 ; LEFP, 2015, n° 10, p. 2, note T. Douville ; Gaz. Pal., 2015, n° 288, p. 24, note C. Berlaud ; JCP G, 2015, n° 51, comm. 1385, P. Ducoulombier ; CCE, 2015, n° 11, comm. 92, obs. A. Lepage ; D., 2016, n° 05, p. 277, obs. E. Dreyer ; RTD civ., 2016, n° 02, p. 449, obs. N. Cayrol.

Civ. 1^{ère}, 26 septembre 2018, n° **17-20.143**, Bull. civ., ; D., 2018, n° 39 p. 2153, obs. M. Bacache, A. Guégan et S. Porchy-Simon ; RTD civ. 2019, n° 01, p. 119, obs. P. Jourdain ; Revue Responsabilité civile et assurances, 2018, n° 12, comm. 306, note L. Bloch ; Gaz. Pal., 2018, n° 35, p. 29, note C. Berlaud.

iv. Chambre criminelle

Crim., 19 décembre 1885, Watelet, Bull. crim., 1885, n° 363 ; D., 1885, p. 345 ; S., 1886, p. 86 ; DP, 1886, p. 347.

Crim., 22 décembre 1966, n° **66-92.897**, Bull. crim, n° 305 ; D., 1967, p. 122 ; JCP, 1967, jur. II. 15126, note R. Savatier ; RSC, 1967, 453, obs. Levasseur.

Crim., 18 novembre 1986, n° **85-93.308**, Bull. crim., n ° 345 ; Gaz. Pal., 1987, 167, note J.-P. Doucet et Le Fauc.

Crim., 8 avril 1998, n° **97-83.656**, Bull. crim., n° 138 ; D., 1999, n° 43, p. 381, obs. J. Penneau ; Dr. pén., 1998, comm. 113, M. Véron ; LPA, 1999, n° 142, p. 24, note D. Krajeski.

v. Chambre sociale

Cass. soc., 13 novembre 2008, n° **06-45.991** : Semaine sociale Lamy 2009, n° 1383, p. 6, obs. M. Blatman ; Propr. intell., 2009, n° 31, p. 158, obs. A. Lucas.

6. Juridictions administratives du fond

i. Tribunaux administratifs

Bordeaux, 14 novembre 1990, n° **9000617**, Rec. Lebon T., p. 974.

Amiens, 24 octobre 2013, n° **1200264**.

Melun, 16 octobre 2015, n° **1504175**.

ii. Cours administratives d'appel

Nantes, 1^{ère} ch., 21 décembre 1995, n° **94NT00321**, JurisData n° 1995-049980.

Paris, 24 mars 1998, n° **96PA02373**, *Assistance publique -Hôpitaux de Paris, M. B...*, Inédit Rec. Lebon ; Dr. adm. 1998, p. 292.

Nantes, 3^e ch., 07 octobre 1999, n° **96NT01287**, Rec. Lebon T., Gaz. Pal., 2001, n° 44, p. 33, note P. Graveleau.

Paris, 30 septembre 2004, n° **03PA01769** : RDS, 2015, n° 05, p. 201, obs. F. Vialla.

Marseille, 25 juin 2009, n° **07MA02024**, Inédit Rec. Lebon ; JCP A, 2010, 2009, n° 02, obs. S. Renard ; JCP A, 2010, n° 38, comm. 2280, C. Lantero.

Marseille, 2^e ch., 12 avril 2018, n° **15MA03742**, Inédit Rec. Lebon.

7. Juridictions judiciaires du fond

i. Juridictions judiciaires du premier degré

TGI, Paris, 4 juin 2010 : Légipresse, 2010, n° 274, p. 129 ; LPA, 2010, n° 196, p. 10, note E. Derieux.

TGI, Paris, 8 oct. 2010 : Légipresse, 2010, n° 277, p. 333 ; Propr. intell., 2011, n° 38, p. 83, obs. A. Lucas.

ii. Cours d'appel

CA, Paris, 27 mai 1997, *aff. du Docteur Gubler*, JurisData n° 1997-990005 : JCP G, 1997, jur. II 22894, note E. Derieux ; LPA, 1997, n° 82, p. 26, note E. Derieux et F. Gras

CA, Paris, 24 juin 2005, 4^e ch., sect. B, n° **03/11140**, JurisData n° 2005-279386 : CCE, 2005, comm. 131, note C. Caron.

CA, Paris, 4^e ch., sect. A, 5 décembre 2007, n° **06/15937**, JurisData n°2007-350003 : D., 2008, n° 07, p. 461, J.-M. Bruguière ; CCE, 2008, comm. 17, Ch. Caron ; Légipresse 2008, n° 251, III, p. 83, A. Maffre-Baugé.

CA, Aix-en-Provence, 9 mars 2011, n° **2011/111**, JurisData n° 2011-009638 : RLDI, 2011, n° 70, p. 27, obs. M. Trézéguet.

CA, Paris, Pôle 5, 2^e ch. 2, 1^{er} avril 2011, n° **10/03052**, JurisData n° 2011-012983.

CA, Paris, Pôle 5, 2^e ch., 23 mars 2012, n° **10/11168**, JurisData n° 2012-011871 : D., 2015, n° 15, p. 908, note T. Lancrenon ; RTD com., 2015, n° 02, p. 294, note F. Pollaud-Dulian ; CCE, 2012, n° 7-8, , comm. 76, A. Debet.

CA, Paris, Pôle 5, 1^{ère} ch., 6 juin 2012, n° **10/21371**, JurisData n° 2012-016964 : LEPI, 2012, n° 09, p. 02, note C. Bernault ; CCE, 2013, n° 06, chron. 6, B. Montels ; RLDI, 2012, n° 84, 2817.

CA, Toulouse, ch. sociale, 15 juin 2012, n° **11/03433**, JurisData n° 2012-018228.

CA, Riom, ch. sociale, 6 mars 2018, n° **15/03035**.

Table des matières

Sommaire.....	5
Principales abréviations.....	7
INTRODUCTION GENERALE.....	13
Paragraphe 1 : L'absence de protection juridique spécifique à la donnée médicale	20
A) Les caractéristiques de la donnée médicale personnelle.....	20
B) L'application d'un régime de droit commun à une donnée médicale particulière	24
1. L'application du droit à la protection des données personnelles.....	25
2. L'application du droit à la confidentialité de la vie privée du patient	30
Paragraphe 2 : La réduction de l'autodétermination informationnelle du patient	35
A) Le caractère obligatoire du traitement de la donnée médicale.....	35
B) La restriction des prérogatives du patient à l'égard de sa donnée médicale.....	37
Paragraphe 3 : La réglementation spécifique à la donnée médicale du patient.....	41
PREMIERE PARTIE : LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AU PROFIT DE SA PRISE EN CHARGE SANITAIRE	47
TITRE 1 : LA FORMALISATION DES DONNEES MEDICALES AU SEIN DES DOSSIERS MEDICAUX DU PATIENT	49
Chapitre 1 : Les contours des données personnelles colligées dans les dossiers médicaux du patient	53
Section 1 : Les dossiers de soins constitués à l'initiative des professionnels et des établissements de santé.....	54
Paragraphe 1 : Les données médicales générées lors de la prise en charge médicale du patient	54
A) Les données médicales recueillies auprès du patient.....	55

B)	Les données médicales produites par les professionnels de santé.....	57
	Paragraphe 2 : L'intégration des données médicales du patient au sein d'une pluralité de dossiers de soins.....	60
A)	Le dossier médical hospitalier	61
B)	Les fiches d'observation personnelles	65
C)	La formalisation des données médicales générées à l'occasion de la télésanté	66
D)	Les notes personnelles prises par le professionnel de santé	72
	Section 2 : Le Dossier Médical Partagé intégré dans l'Espace numérique de santé	74
	Paragraphe 1 : Le périmètre du contenu du Dossier Médical Partagé.....	75
A)	Les données médicales renseignées par les professionnels intervenant à la prise en charge sanitaire du patient.....	76
B)	Les données renseignées par le titulaire du Dossier Médical Partagé.....	80
	Paragraphe 2 : La nécessaire centralisation des données relatives à la prise en charge médicale du patient en un dossier national et exclusif.....	84
A)	La disparité des dossiers numériques partagés	84
B)	L'essentiel affermissement du rôle central du DMP	89
	Conclusion du chapitre	95
	 Chapitre 2 : La limitation des droits du patient sur les données personnelles colligées dans ses dossiers médicaux.....	 97
	Section 1 : L'ineffectivité du droit d'opposition au traitement des données médicales aux fins de constitution et d'alimentation des dossiers médicaux	98
	Paragraphe 1 : L'obligation de constitution des dossiers de soins	98
A)	L'inopposition à l'obligation de constitution du dossier médical hospitalier.....	98
B)	L'inopposition à l'obligation de constitution des fiches d'observation personnelles	102
C)	L'opposition à la prise de notes personnelles par le médecin	105
	Paragraphe 2 : La constitution du Dossier Médical Partagé.....	109
A)	L'opposition à la création du Dossier Médical Partagé.....	110

B)	L'inopposition à l'obligation d'alimentation du Dossier Médical Partagé	113
	Section 2 : La réduction des droits du patient à la modification de ses dossiers médicaux	119
	Paragraphe 1 : La modification des dossiers de soins	119
A)	La rectification des données colligées dans les dossiers de soins	119
1.	Les conditions d'exercice du droit de rectification.....	120
2.	La rectification des données administratives contenues dans les dossiers de soins ..	123
3.	La rectification des données médicales contenues dans les dossiers de soins.....	125
B)	L'effacement des données colligées dans les dossiers de soins	128
1.	L'obligation d'effacement des données non minimisées.....	130
2.	L'obligation d'effacement des données périmées	132
	Paragraphe 2 : La modification du Dossier Médical Partagé	139
A)	La modification des données consignées par les professionnels de santé	139
1.	Le droit de rectification des données médicales colligées par les professionnels de santé	139
2.	Le droit à l'effacement des données médicales colligées par les professionnels de santé	143
B)	La modification des données documentées par le titulaire du Dossier Médical Partagé.....	147
	Conclusion du chapitre	151
	Conclusion du titre.....	153

**TITRE 2 : LA COMMUNICATION DES DONNEES MEDICALES FORMALISEES
DANS LES DOSSIERS MEDICAUX DU PATIENT 155**

Chapitre 1 : L'accès du patient aux données médicales générées lors de sa prise en charge sanitaire	157
---	------------

Section 1 : Le principe de l'accès direct aux données médicales consignées dans les dossiers médicaux	158
Paragraphe 1 : L'exercice du droit d'accès direct par la personne concernée.....	158
A) La reconnaissance du droit d'accès direct à l'information médicale.....	158
B) Les modalités d'accès aux données médicales consignées dans les dossiers médicaux	166
Paragraphe 2 : L'exercice du droit d'accès de la personne juridiquement incapable....	172
A) L'accès indirect aux données médicales du mineur	172
B) L'accès direct aux données médicales du majeur protégé.....	178
Section 2 : Les limitations de l'accès direct aux données médicales consignées dans les dossiers médicaux	183
Paragraphe 1 : Le principe d'accès aux seules informations formalisées	183
A) L'accès aux informations formalisées en considération de leur fonction.....	184
B) L'abandon du critère de fonctionnalité de l'information formalisée.....	185
Paragraphe 2 : L'accès indirect aux informations requérant un accompagnement	190
A) Les dangers de l'accès direct à des données médicales ésotériques	191
B) La nécessaire préservation du patient à l'égard de ses données médicales	192
Paragraphe 3 : Le secret des données personnelles concernant les tiers	196
A) La protection des données médicales relatives aux tiers à la relation sanitaire ...	197
B) L'atteinte au droit d'accéder à ses informations personnelles recueillies auprès d'un tiers	200
Conclusion du chapitre	205
 Chapitre 2 : L'accès des professionnels aux données médicales du patient	207
Section 1 : L'échange et le partage des données médicales du patient	209
Paragraphe 1 : Les conditions d'échange et de partage des données médicales entre les professionnels concourant à la prise en charge du patient	209
A) La participation du professionnel à la prise en charge du patient.....	209

B)	La minimisation des données médicales échangées ou partagées	215
	Paragraphe 2 : Les droits du patient sur ses données médicales à l'aune du secret médical	220
A)	La maîtrise de la communication des données médicales par le patient	221
1.	La maîtrise de l'échange des données médicales par le patient.....	221
2.	La maîtrise du partage des données médicales par le patient	225
B)	Les restrictions de la maîtrise de la communication des données médicales par le patient	235
	Section 2 : L'inéluctable responsabilisation de la personne concernée par le traitement de ses données médicales	242
	Paragraphe 1 : Le devoir du patient de renseigner ses données médicales	243
A)	L'instauration prétorienne d'un devoir légal d'information à la charge du patient... ..	243
B)	L'instauration d'un devoir moral de documentation du DMP par son titulaire ..	249
	Paragraphe 2 : La renonciation du patient concerné à la plénitude de ses droits	256
A)	Le devoir de non-opposition à la communication des données médicales entre professionnels.....	256
B)	La remise en cause de l'autodétermination du patient concerné par le traitement de ses données médicales	263
1.	La collision entre le droit fondamental à la santé et le droit fondamental à la protection des données personnelles	264
2.	L'instauration de devoirs en contrepartie des droits fondamentaux	271
	Conclusion du chapitre	277
	Conclusion du titre.....	279
	Conclusion de la première partie	281

DEUXIEME PARTIE : LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AU BENEFICE DE LA COLLECTIVITE	283
--	------------

TITRE 1 : LA DETERMINATION DU STATUT JURIDIQUE ET DU REGIME APPLICABLES A LA DONNEE MEDICALE	285
---	------------

Chapitre 1 : L'extrapatrimonialité de la donnée médicale	287
Section 1 : Tentative de qualification de la donnée médicale	288
Paragraphe 1 : Le statut de la donnée médicale à caractère personnel.....	288
A) L'émergence d'une chose anthropomorphique personnelle.....	288
1. La personnification de la donnée personnelle	289
2. La réification de la condition physiologique du patient	292
B) La création d'un régime hybride d'ordre public.....	294
Paragraphe 2 : Le statut de la donnée médicale anonymisée	302
A) L'apparition d'une chose commune désaffectée	302
B) L'application d'un régime protecteur contre les dérives mercantiles.....	310
Section 2 : L'inappropriabilité de la donnée médicale	315
Paragraphe 1 : Le rejet du régime de la propriété mobilière	315
A) L'impossible appropriation de la donnée médicale	316
B) L'altération des attributs de la propriété.....	320
Paragraphe 2 : Le rejet du régime du droit de la propriété intellectuelle	327
A) L'absence de création originale protégeable	328
B) La titularité des droits d'auteur.....	333
Conclusion du chapitre	341

Chapitre 2 : La valorisation économique du traitement de la donnée médicale extrapatrimoniale.....	343
Section 1 : La valorisation économique de l’exploitation de la donnée médicale au profit du responsable de traitement.....	344
Paragraphe 1 : Les droits de l’exploitant sur les résultats du traitement de la donnée médicale	344
A) La valorisation du contenu de la base de données médicales à caractère personnel	345
1. La valorisation des bases de données médicales produites par des organismes chargés d’une mission de service public	347
2. La valorisation des bases de données médicales produites par le secteur privé ..	361
B) La valorisation des créations et inventions consécutives à la réutilisation des données médicales.....	364
Paragraphe 2 : L’existence d’un droit d’user de la donnée médicale personnelle	369
Section 2: La valorisation économique de la participation du patient au traitement de ses données médicales.....	374
Paragraphe 1 : L’absence d’usufruit sur les données médicales personnelles	375
A) Le défaut d’usus.....	375
B) Le défaut de fructus	379
Paragraphe 2 : Le patient créancier à l’égard de la collectivité.....	384
A) La participation ignorée à un processus créatif	384
B) La récompense nationale pour la participation à un acte civique d’intérêt général...	390
Conclusion du chapitre	397
Conclusion du titre.....	399

TITRE 2 : LE TRAITEMENT DES DONNEES MEDICALES DU PATIENT AUX FINS D'INTERET PUBLIC DANS LE DOMAINE DE LA SANTE : LA RECHERCHE, L'INNOVATION ET LA SANTE PUBLIQUE	403
Chapitre 1 : La requalification des données médicales en données de recherche	405
Section préliminaire : Le changement de la finalité du traitement des données médicales produites à l'occasion du soin	406
Section 1 : Les prérogatives du patient à l'égard de ses données de recherche utilisées pour un motif d'intérêt public dans le domaine de la santé.....	415
Paragraphe 1 : Le droit à l'information relative à l'utilisation des données de recherche	415
A) Le principe de l'information individuelle et spécifique complémentaire à l'information générale	416
B) La dissipation de l'information individuelle relative à l'utilisation des données de recherche	426
Paragraphe 2 : L'atténuation des droits du patient sur ses données de recherche	433
A) Les droits du patient sur ses données médicales intégrées dans une base de données massives pour la recherche.....	434
B) Les droits du patient sur ses données de recherche utilisées pour un projet déterminé	443
Section 2 : La réduction de l'autodétermination informationnelle du patient au profit de l'indispensable exploitation des données de recherche	449
Paragraphe 1 : L'opposabilité du droit d'opposition au patient concerné par l'utilisation de ses données de recherche	450
A) Le principe d'un supposé droit d'opposition à l'utilisation des données de recherche	450
B) Les limites normatives à l'exercice du droit d'opposition à l'utilisation des données de recherche.....	454
Paragraphe 2 : L'instauration d'un devoir de concours à la recherche et à l'innovation au bénéfice de la santé publique.....	461

A) Le patient débiteur de la mise en œuvre de la protection de la santé publique ...	462
B) Le contrôle de la finalité des usages des données de recherche par la société civile	466
Conclusion du chapitre	473
Chapitre 2 : La lutte contre les menaces sanitaires par la datasurveillance : l'exemple des traitements déployés pour faire face à la pandémie de la Covid-19.....	477
Section 1 : L'exceptionnalité du fichage massif de données sensibles	481
Paragraphe 1 : L'exception de la communication des données médicales confidentielles	481
A) La divulgation des données médicales de la personne fichée.....	482
B) La préservation de la confidentialité des données médicales divulguées.....	493
Paragraphe 2 : L'exception aux droits et libertés fondamentaux de la personne fichée	503
A) Le traitement obligatoire des données médicales des citoyens au bénéfice de la lutte contre la crise sanitaire	504
B) Le traitement facultatif des données médicales des citoyens en appui de la gestion de la crise sanitaire	515
Section 2 : La légitimation des fichages d'exception par la préservation de la santé publique.....	523
Paragraphe 1 : La prévalence de la protection de la santé publique.....	524
A) La poursuite d'un motif d'intérêt général nécessaire et proportionné.....	525
1. La nécessité du fichage des citoyens	525
2. La proportionnalité et la pertinence du fichage des citoyens	537
B) La temporalité des atteintes portées aux droits fondamentaux de la personne fichée 549	
Paragraphe 2 : L'affermissement de la démocratie sanitaire en faveur de la santé publique.....	554
A) La coopération citoyenne pour la prévention des menaces sanitaires	555

B) La coconstruction citoyenne des dispositifs numériques de lutte contre les menaces sanitaires.....	562
Conclusion du chapitre	569
Conclusion du titre.....	571
Conclusion de la deuxième partie.....	575
CONCLUSION GENERALE	577
Index Alfabétique	581
Bibliographie	597
Table des matières	645
Résumé	655

Résumé

Appartenant à la catégorie des données de santé, la donnée médicale constitue un élément immatériel du corps humain généré à l'occasion de la prise en charge sanitaire du patient. En effet, la donnée médicale tend à réifier un état physiologique intrinsèque à la personne humaine en une information tangible et accessible. Il en advient que cette information authentique, attachée à la personne de laquelle elle émane, touche profondément à l'intimité de son hôte. En conséquence, la donnée médicale mérite une protection juridique accrue, indépendamment de son utilisation, à l'instant de sa génération. De surcroît, son usage nécessite d'être strictement encadré pendant que l'autodétermination informationnelle du patient concerné exige d'être précisément déterminée. Néanmoins, ni la protection de la donnée médicale, ni les droits que le patient détient à son égard ne doivent contrevenir à son traitement dans le domaine de la santé. Si la donnée médicale représente un élément immatériel du corps humain du patient, elle est également observée comme un matériau indispensable à la protection de la santé individuelle comme à la protection de la santé collective. D'une part, les services de soins de santé délivrés au patient reposent indispensablement sur la collecte, la circulation et l'analyse de cet outil médical. A l'évidence, toute décision sanitaire ne peut être prise, par les professionnels de santé, qu'à l'appui de ces informations particulières. D'autre part, la donnée médicale constitue le matériau de recherche des acteurs participant à l'innovation sanitaire ainsi qu'aux activités connexes à la santé publique. Assurément, le développement, l'amélioration et la protection de la santé collective reposent inextricablement sur le traitement des données médicales des membres de la société. Force est d'observer que la donnée médicale est devenue un instrument sanitaire globalisé dont l'exploitation est impérieusement nécessaire pour la prise en charge individuelle du patient comme pour l'exercice de la santé publique. Le traitement de la donnée médicale apparaît donc comme un impératif sanitaire entraînant une diminution des droits qui lui sont effectivement reconnus à l'égard des éléments immatériels de son corps humain. Au surplus, le patient aurait même le devoir de collaborer à sa prise en charge sanitaire en favorisant le traitement de ses informations capitales ; ainsi que le devoir de placer ses données médicales à la disposition de tout projet concourant à la santé publique au profit de l'intérêt général. Néanmoins, la restriction de l'autodétermination informationnelle du patient sur sa donnée médicale ne constitue-t-elle pas une atteinte à son droit fondamental à la protection des données personnelles ? Il en résulte des points de tension entre

l'autodétermination informationnelle du patient envers sa donnée médicale, l'incontournable utilité de cet instrument sanitaire par-delà le colloque singulier, et le nécessaire renforcement de la protection de cet élément immatériel et confidentiel issu du corps humain. Seulement, la donnée médicale ne bénéficie d'aucun encadrement juridique permettant de considérer ses spécificités, ses enjeux, et les risques inhérents à sa création comme à son usage. Les présents travaux ont alors pour objet de démontrer l'inadaptation du droit positif aux particularités de la donnée médicale et prétendent à concevoir un cadre juridique qui lui serait dédié. Pendant que la sacralisation de la donnée médicale affirmerait sa sauvegarde, son exploitation serait favorisée par la redéfinition des prérogatives et des obligations que le patient disposerait à son égard : d'abord lorsqu'elle est traitée aux fins de sa prise en charge sanitaire, mais également lorsqu'elle fait l'objet d'une réutilisation à des fins de recherche, d'innovation et de santé publique.

Mots-clés : Donnée médicale - Protection des données personnelles - Prise en charge sanitaire - Santé publique - Choses communes - Mise à disposition.

Abstract

Belonging to the health data category, medical data is an intangible element of the human body generated during the health care of the patient. Indeed, medical data tends to reify a physiological state intrinsic to the human person into tangible and accessible information. It happens that this authentic information, attached to the person from whom it emanates, deeply touches the intimacy of its host. As a result, medical data deserves increased legal protection, regardless of its use, at the moment of its generation. Moreover, its use needs to be strictly regulated while the empowerment of the patient concerned needs to be precisely determined. Nevertheless, neither the protection of medical data nor the rights held by the patient towards himself must contravene his processing in the field of health. If medical data represents an immaterial element of the patient's human body, it is also observed as an indispensable material for the protection of individual health as well as for the protection of collective health. On one hand, the health care services provided to the patient are essentially based on the collection, circulation and analysis of this medical tool. Clearly, any health decision can only be taken by health professionals in support of this

particular information. On the other hand, medical data is the research material of actors involved in health innovation as well as activities related to public health. Certainly, the development, improvement and protection of collective health depend inextricably on the processing of medical data of members of the society. It must be observed that medical data has become a globalised health instrument whose exploitation is imperatively necessary for the individual management of the patient as well as for the exercise of public health. The processing of medical data therefore appears to be a health imperative leading to a reduction a decrease in the agreed rights actually in regard to immaterial elements of its human body. In addition, the patient would even have the duty to collaborate in his health care by promoting the processing of this crucial and vital information ; along with the duty to place his medical data at the disposal of any project contributing to public health for the benefit of the public interest. Nevertheless, does not the restriction of the patient's empowerment over his medical data constitute an infringement of his fundamental right to the protection of personal data ? This results in tension points between the patient's empowerment towards his medical data, the unavoidable worth of this health instrument beyond the singular colloquium, and the necessary strengthening of this immaterial and confidential element from the human body. Thus, medical data does not benefit from any legal framework to consider its specificities, its stakes, and the risks inherent in its creation and use. The purpose of this work is then to demonstrate the inadequacy of positive law to the particularities of medical data and to design a legal framework dedicated to it. While the sacralization of medical data would affirm its preservation, its exploitation would be favoured by the redefinition of the prerogatives and obligations that the patient would have towards it : first when it is used for health care management but also when it is reused for research and innovation and public health purposes.

Keywords : *Medical data - Protection of personal data - Health care of the patient - Public health – Commons - Availability.*

