Ecole doctorale des Sciences Juridiques, Politiques, Economiques et Gestion SJPEG

Institut François Gény (IFG) – EA 7301
Institut de Sciences criminelles et de Droit médical (ISCREMED)

UNIVERSITE DE LORRAINE

FACULTE DE DROIT, SCIENCES ECONOMIQUES ET GESTION

THESE

Pour l'obtention du grade de
Docteur en Droit
Discipline : Droit privé et Sciences criminelles

Présentée et soutenue publiquement
Le 12 décembre 2022
Par
Elaine BUCKI

Titre :

LA DEMATERIALISATION EN ETABLISSEMENT DE SANTE

Analyses juridiques

Composition du Jury :

Directeur de recherches :

Monsieur Bruno PY, Professeur de Droit privé et sciences criminelles à l'Université de Lorraine, Directeur de thèse.

Suffragants :

Madame Marion GIRER, Maîtresse de conférences HDR de Droit privé et sciences criminelles à l'Université Jean Moulin Lyon 3, Rapporteur.
Monsieur Patrick MISTRETTA, Professeur de Droit privé et sciences criminelles à l'Université Jean Moulin Lyon 3, Rapporteur.
Monsieur François VIALLA, Professeur de Droit privé et sciences criminelles à l'Université de Montpellier, Président du jury.
Maître Caroline ZORN, Docteure en droit, Avocate au barreau de Strasbourg.

« *La Faculté n'entend donner ni approbation ni improbation aux opinions émises dans cette thèse, celles-ci devant être considérées comme propres à leur auteur* ».

A ma famille,

A mon conjoint Lorris,

A ma fille Charline.

REMERCIEMENTS

Viens le moment pour moi de clôturer ma thèse par ces remerciements, marquant l'aboutissement de mon travail de recherches qui m'aura tenu en haleine ces dernières années.

Je tiens tout d'abord à remercier Monsieur le Professeur Bruno PY, qui, dès la lecture de mon mémoire m'a proposé et m'a poussée à poursuivre mon chemin universitaire par cette thèse. Ce travail est, sans aucun doute, un accomplissement personnel que je n'avais pas envisagé à l'époque. Grâce à son implication envers ses étudiants, Monsieur le Professeur Bruno PY nous pousse à aller au-delà de ce que l'on pourrait envisager et même imaginer.

Je remercie également Madame Marion GIRER, Messieurs les Professeurs Patrick MISTRETTA et François VIALLA ainsi que Maître Caroline ZORN, d'avoir accepté de composer mon jury de thèse.

Mes remerciements vont aussi à la Direction du GIP Pulsy (et anciennement, du GCS Télésanté Lorraine), pour m'avoir soutenue dans mes projets universitaires et professionnels en me donnant la possibilité d'effectuer ma Cifre à leurs côtés. Je n'aurais pu espérer trouver meilleur Groupement pour commencer ma carrière professionnelle, tant au regard du travail que nous accomplissons au quotidien, que des extraordinaires personnes qui le composent. Mes collègues ont été sans nul doute, un facteur de réussite de ce travail, et pour cela je les en remercie.

Je ne peux que clôturer en remerciant ma famille et ma belle-famille, qui ont cru en mes capacités et m'ont poussée à mener à bien ce projet, et tout particulièrement ma maman pour ses relectures plus qu'intensives et ses conseils avisés, ainsi que ma sœur, qui a été mon soutien le plus tenace. Bien évidemment, mes remerciements vont également à mes amis du P3, qui ne sont, ni plus, ni moins que ma famille de cœur.

Pour terminer, je tiens à remercier mon conjoint Lorris, pour m'avoir accompagnée et appuyée tout au long de cette sacrée aventure, et ma fille, Charline, qui m'a donné l'envie et l'énergie nécessaire pour terminer de rédiger ces pages.

LISTE DES PRINCIPALES ABREVIATIONS

al.	Alinéa
ANAP	Agence Nationale de la Performance Sanitaire et Médico-Sociale
ANS	Agence du Numérique en Santé
ANSSI	Agence nationale de la sécurité des systèmes d'information
ApCV	Application Carte Vitale
ARS	Agence régionale de santé
art.	Article(s)
ASIP	Agence des systèmes d'information partagés de santé
C. civ.	Code civil
C. coll. ter.	Code des collectivités territoriales
C. patr.	Code du patrimoine
C. pén.	Code pénal
C. proc. pén.	Code de procédure pénale
C. santé publ.	Code de la santé publique
C. sécurité soc.	Code de la sécurité sociale
Cass.	Cour de cassation
CGU	Conditions Générales d'Utilisation
ch.	Chambre
CNIL	Commission nationale de l'informatique et des libertés
Cnam	Caisse nationale de l'assurance maladie
CNOM	Conseil National de l'Ordre des Médecins
CNRS	Centre National de la Recherche Scientifique
Cofrac	Comité français d'accréditation
CPS	Carte de professionnel de santé
CPTS	Communauté Professionnelles Territoriales de Santé
DC	Dénomination Commune
DGOS	Direction générale de l'Offre de soins
DP	Dossier Pharmaceutique
DPI	Dossier Patient Informatisé

DMP	Dossier Médical Partagé
EHPAD	Établissement d'hébergement pour personnes âgées dépendantes
eIDAS	electronic IDentification, Authentication and trust Services
ENS	Espace Numérique de Santé
FDI	Forum des droits sur l'internet
FEVAD	Fédération e-commerce et vente à distance
GED	Gestion Electronique de Documents
GHT	Groupement Hospitalier de Territoire
GRADeS	Groupement Régional d'Appui au Développement de la e-Santé
HAS	Haute Autorité de Santé
HDS	Hébergeur de Données de Santé
IA	Intelligence Artificielle
INS	Identité Nationale de Santé
INSEE	Institut National de la Statistique et des études économiques
INSi	Identifiant National de Santé intégré
Jurispr.	Jurisprudence
NTI	Nouvelles technologies de l'information
OTP	One-Time Password
p.	Page
pp.	Pages
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information en Santé
PSDC	Prestataire de Service de Dématérialisation et de Conservation
PSDC-D	Prestataire de Service de Dématérialisation et de Conservation – Dématérialisation
PV	Procès-verbal (verbaux)
RDS	Revue Droit & Santé
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RH	Ressources Humaines
RJSP	La revue des juristes de sciences po
ROR	Répertoire Opérationnel des Ressources
RTDCiv	Revue trimestrielle de Droit civil
s.	Suivant

SAE	Système d'archivage électronique
SI	Système d'information
SIAF	Service Interministériel des Archives de France
SIH	Système d'Information Hospitalier
SMS	Short Message Service
SMSI	Système de Management de la Sécurité de l'Information
Trib.	Tribunal
UNESCO	Nations Unies pour l'éducation, la science et la culture
VSM	Volet de Synthèse Médicale

SOMMAIRE

INTRODUCTION GENERALE

« En 2030, la première porte d'entrée dans le système de santé sera dématérialisée »[1]

1. **L'informatisation de la société**. L'informatisation est un des événements majeurs qui a marqué l'évolution de notre société. Elle a connu plusieurs grandes phases en France : dès 1947, le CNRS[2] et la société Logabox ont conclu un contrat « *pour la construction de la machine de Couffignal, la première calculatrice numérique électronique conçue en France* »[3], marquant le premier pas de l'informatisation sur le territoire national. Une petite dizaine d'années plus tard, les premières formes d'ordinateurs voient le jour. Elles sont utilisées tout d'abord par la Défense puis par quelques entreprises commerciales, avant que l'informatique soit finalement enseignée dans certaines Universités, dès 1957[4]. A partir des années 60, le développement de l'informatique en France connaît un réel essor jusqu'à aboutir dans les années 80 à l'équipement d'ordinateurs au sein des foyers. 20 ans plus tard, le monde connaît une évolution exponentielle de l'informatique avec le développement croissant de l'Internet, de la dématérialisation des données et de l'utilisation de l'informatique dans la vie quotidienne. *« La société de l'information* [que l'on connaît aujourd'hui] *est née du progrès technique qui nous permet désormais de traiter, de stocker, de trouver et de communiquer des informations, sous quelque forme que ce soit, sans être limité par des contraintes d'espace, de temps ou de volume* ».[5] En l'espace de 70 ans, l'informatisation de la société a subi une évolution remarquable, elle est à l'origine de la troisième et de la quatrième révolution industrielle.

2. **La quatrième révolution industrielle.** « *Par « révolution », on entend un changement brusque et radical. L'histoire est ponctuée de révolutions ; à chaque fois, une*

[1] Olivier BABINET, Corinne ISNARD BAGNIS, *La e-santé en question(s)*, Hygée éditions, 2020, p. 17.
[2] Le Centre National de la Recherche Scientifique.
[3] Musée informatique, *comment s'est développé l'informatique en France ?- évolution de l'informatique,* 2022.
[4] *Ibid.*
[5] Nicolas VALLUET, « Présentation générale des nouvelles technologies de communication et d'information », *LPA* 06 nov. 1996, n° 134, p. 7.

innovation technologique ou une idéologie nouvelle déclenche une transformation en profondeur des structures économiques et sociales »[6]. Une des premières que le monde a vécue est le changement radical du mode de vie de la personne par la révolution de l'agriculture ; l'apparition de l'agriculture et de la domestication des animaux a permis une production accrue de l'alimentation ainsi qu'une croissance démographique, entraînant « *la concentration des populations, d'où le processus d'urbanisation et l'essor des villes* »[7].

Les différentes révolutions qui se sont succédé ont laissé la place à des révolutions dites industrielles. « *Plus qu'une époque, on désigne par « révolution industrielle » un ensemble de phénomènes qui ont accompagné, à partir de XVIIIe siècle, la transformation du monde moderne par le développement du capitalisme, de la technique, de la production et des communications* »[8]. On décompte aujourd'hui quatre révolutions industrielles :

La première révolution industrielle a débuté en 1760 avec la transformation du mode de fabrication passant de la production artisanale à la production mécanisée. Cela est notamment possible grâce à l'exploitation du charbon, ainsi que par la création de la machine à vapeur et son utilisation pour faire fonctionner les machines servant à la fabrication des produits. La construction des chemins de fer a également contribué à cette première révolution industrielle.

La deuxième révolution industrielle a débuté dans les années 1840 avec la création de l'électricité et du pétrole. Ces deux nouveaux modes d'énergie profitent à l'industrie afin de faire fonctionner les machines. « *Cette période correspond à l'essor du Taylorisme*[9]*, du travail à la chaîne et de la production en masse »*[10].

La troisième révolution industrielle débute au milieu du XXème siècle dans les années 60, qui est également appelée révolution informatique ou révolution numérique. Elle est apparue à la suite du développement de l'informatisation dans notre société et des innovations technologiques, changeant considérablement la manière de fonctionner des entreprises, avec l'utilisation de robots. La production est plus rapide, plus optimale, et peut ainsi remplacer en

[6] Klaus SCHWAB, *La quatrième révolution industrielle*, Dunod, 2017.
[7] *Ibid.*
[8] Larousse encyclopédie, *Révolution industrielle.* Disponible à l'adresse : https://www.larousse.fr/encyclopedie/ (consulté le 10/08/2022).
[9] Vie publique, « Qu'est-ce que le taylorisme ? », *Fiche thématique*, 2019. : « *Le taylorisme est une méthode d'organisation du travail industriel dont les caractéristiques principales sont la division horizontale et verticale du travail ainsi que le salaire au rendement* ».
[10] Sesa systems, « qu'est-ce que l'industrie 4.0, la quatrième révolution industrielle », *Industrie 4.0.* Disponible à l'adresse : https://www.sesa-systems-digital.com/ (consulté le 10/07/2022).

partie l'Homme ; la troisième révolution industrielle marque le début de l'automatisation de la chaîne de production[11].

Actuellement, nous nous trouvons au sein de la quatrième révolution industrielle qui a débuté en 2011 : l'industrie 4.0. Ce terme a vu le jour lors de la Foire de Hanovre[12] en Allemagne montrant le début des « usines intelligentes ». Les entreprises utilisent les nouvelles technologies ainsi que le numérique pour optimiser leur production. Toute la chaîne de production est transformée grâce aux innovations que permettent les nouvelles technologies notamment l'intelligence artificielle, le big data, ou encore les interconnexions. Cette quatrième révolution industrielle se distingue de la précédente par la capacité des usines, non plus seulement à produire grâce aux technologies informatiques, mais à être « intelligentes » grâce à l'interconnexion permettant une production quasiment autonome.

3. **L'évolution de la dématérialisation : les correspondances.** Même si l'informatisation en France n'est apparue que dans les années 50, engendrant la troisième révolution industrielle, et plus généralement le développement de notre société dans son ensemble, on constate que la technologie est apparue bien avant. Prenons l'exemple de l'évolution des correspondances comme objet de communication : depuis toujours, les Hommes ont besoin de communiquer les uns avec les autres par quelque moyen que ce soit. La première forme de correspondance à laquelle on pense est la communication verbale face à face. Mais comment communiquer lorsque les deux personnes se trouvent éloignées ?

Les plus anciennes formes de communication étaient réalisées : par un messager délivrant le message soit de manière orale ou en main propre par écrit, par signaux visuels et sonores, ou encore par le *biais* de pigeons voyageurs, spécialement dressés pour délivrer des messages. Ces derniers ont été utilisés depuis l'Antiquité dans de nombreux domaines : les marins prévenaient de leur arrivée au port, ou de leur retard dû à une tempête ; ils servaient à délivrer des informations stratégiques en temps de guerre mais permettaient également de créer des réseaux d'informations commerciaux entre les différentes villes. « *En 1832, l'installation du télégraphe aurait pu mettre un frein à l'engouement pour le pigeon voyageur. Mais le développement des lignes de chemin de fer allait au contraire entraîner le plein essor de cette activité redevenue très populaire. Autrefois, les oiseaux étaient transportés dans des paniers chargés sur des charrettes. Les convoyeurs marchaient jusqu'à 40 km par jour avec un*

[11] *Ibid.*
[12] La Foire de Hanovre en Allemagne est un des plus grands salons de la technologie ayant lieu chaque année depuis 1947.

chargement de 40 à 50 volatiles. Désormais, le train ou le camion en acheminaient des milliers à la fois. Le nombre de colombophiles[13] *augmentait au même rythme que les concours de lâchers de pigeons. Cette activité s'enracina plus particulièrement en Belgique, en Allemagne et dans le nord de la France* »[14]. Les pigeons voyageurs ont perduré de nombreuses années et ont même connu un succès lors de la première et de la seconde Guerre Mondiale. *« Un […] oiseau anglais baptisé GI Joe participa à la libération de l'Italie en 1943. Grâce à lui, un village fut épargné par les bombardements. Décoré, cité par le Congrès américain, GI Joe termina sa vie de héros au zoo de Detroit ; il vécut jusqu'à 19 ans »*[15].

Pour autant, même si le pigeon voyageur a été une forme de communication utilisée et éprouvée jusqu'à un certain point, l'invention de l'électricité a permis la création du télégraphe électrique par P. Shilling puis, cinq ans plus tard, un nouveau code télégraphique par S. Morse permettant la réalisation de communication dématérialisée. Grâce à cette technologie, le premier télécopieur (fax) a pu être inventé, bien que son utilisation ne soit devenue populaire que dans les années 80[16].

A suivi ensuite l'invention du téléphone favorisant les échanges d'un bout à l'autre du monde de manière orale, mais également écrite, par l'envoi de SMS avec la création des smartphones. La correspondance dématérialisée par excellence est bien évidemment le courrier électronique (ou mail) apparu dès 1965, qui est utilisé tant dans le domaine personnel que professionnel.

En parallèle de ces formes de communication, il reste bien évidemment les lettres et courriers envoyés par voie postale, qui sont encore aujourd'hui, un moyen de communication très répandu et populaire. Pour autant, même l'envoi de courriers par voie postale, peut se faire de manière dématérialisée par Maileva ; « *confiez nous vos envois : nous les imprimons, les mettons sous plis, les affranchissons et les remettons à la Poste* »[17].

[13] Un colombophile est une personne qui élève et dresse des pigeons voyageurs.
[14] Florence CALVET, Jean-Paul DEMONCHAUX, Régis LAMAND et Gilles BORNERT, « La brève histoire de la colombophilie », *Revue historique des armées*, 2007, pp. 93-105.
[15] *Ibid.*
[16] Jean-Paul BRETHES, « La télécopie : 150 ans d'histoire (1843-1993) », *Réseaux, communication – technologie - société*, volume 11, n°59, 1993. Droit et communication. pp. 119-131.
[17] Maileva, « Plate-forme d'envoi de courriers en ligne ». Disponible à l'adresse : https://www.maileva.com/ (consulté le 15/08/2022).

La dématérialisation n'est donc pas liée à l'informatisation, mais existe depuis bien longtemps, elle est possible grâce à la technologie. En revanche, l'informatisation permet de développer sa pratique.

4. **La dématérialisation : définition**. Mais qu'est-ce que l'on entend par dématérialisation ? Elle peut être entendu de deux manières différentes :

i. Le dictionnaire Le Robert donne un premier sens : « *action de rendre immatériel, fait de devenir immatériel »*[18]. Cette définition reste encore trop floue pour comprendre pleinement son premier sens. Le dictionnaire Larousse est plus précis ; la dématérialisation est l'« *action ou [le] fait de rendre immatériel, d'ôter la matière concrète »*[19]. Une chose immatérielle est donc quelque chose d'intouchable, d'impalpable. L'utilisation du préfixe « dé » suppose que la chose immatérielle a été autrefois matérielle, c'est-à-dire tangible, palpable et touchable. La dématérialisation est donc l'action de transformer quelque chose de matériel, en quelque chose d'immatériel par un procédé technologique. Il s'agit par exemple de numériser un document afin que son support ne soit plus qu'informatique, sans support matériel.

ii. La seconde définition est la suppression du support matériel, ou l' « *action de transformer des supports d'information matériels en supports numériques »*[20]. Dans ce contexte, la transformation d'un support matériel en un support immatériel n'est pas à prendre au pied de la lettre. Cette transformation se fait nativement, au moment de la création de la « chose » dématérialisée. Si l'on prend toujours l'exemple des correspondances, le courrier papier est quelque chose de tangible et de matériel. Sa dématérialisation est le fait de créer nativement ce courrier ; typiquement, il s'agit des courriers électroniques. *« La « dématérialisation » ainsi décrite fait naître une opposition entre l'écrit représenté sur support tel qu'il a été envisagé jusqu'à présent – caractérisé par sa matérialiste – et l'écrit d'écran, caractérisé par son opposition au monde analogique. Appréhendé de la sorte, la « dématérialisation » concernerait aussi bien les supports de la mémoire que ceux de la communication »*[21].

A l'heure actuelle, dès lors que l'on parle de dématérialisation, les profanes l'associent simplement à la dématérialisation des documents afin d'aboutir à un résultat « sans papier » ou « zéro papier ». Cependant dans la réalité, elle n'est pas simplement limitée aux documents : il peut s'agir de la dématérialisation d'un échange, d'un processus, d'une

[18] Le Robert, *V° « dématérialisation »*, nom fém.
[19] TLFi, *V° « dématérialisation »*, subst. fém.
[20] Larousse, *V° « dématérialisation »*, nom fém.
[21] Valérie OLECH, *Le secret médical et les technologies de l'information et de la communication*, Thèse dactylographiée, 2019, p. 97.

administration ou encore d'une pratique. *« La dématérialisation recouvrirait donc plusieurs procédés techniques : la numérisation des supports papier de l'information, l'absence de matérialisation et enfin la dématérialisation des moyens de communiquer »*[22].

L'intérêt d'envisager la dématérialisation dans son sens le plus large et dans tous les domaines confondus, est d'aboutir à une société 100% dématérialisée, à l'instar de l'Estonie.

5. **De l'incitation à la dématérialisation**. Aujourd'hui, notre société est hyper-informatisée, *« nulle contrée n'échappe totalement à l'entreprise de ces nouvelles technologies de l'information et de la communication devenues les instruments d'une civilisation nouvelle. On parle alors de la société de l'information, devenue l'horizon incontournable du développement. […] L'impact réel de cette transformation se mesure aux possibilités de partage et de diffusion du savoir sur le comportement socio-économique, les pratiques du monde des affaires et de la politique, des professionnels de l'éducation et de la santé, des créateurs, des loisirs et des divertissements. La particularité de ce nouvel environnement est la vitesse à laquelle les informations sont rassemblées et transmises à travers le monde. Ainsi, on définit la société de l'information comme une société qui fait un usage intensif des réseaux d'information et de la technologie de l'information, produit de grandes qualités de biens et de services d'information et de communication et possède une industrie de contenus diversifiée ». (Eskanen-Sundström, 2001) »*[23]. Si bien qu'aujourd'hui, la dématérialisation concerne absolument tous les domaines, que ce soit dans la vie professionnelle que personnelle ; *« la réalité quotidienne évolue au même rythme que ces technologies. La dématérialisation a pris le pas sur les échanges physiques. D'un lieu à un autre, les informations circulent, et non les hommes. On peut acheter, apprendre, troquer, jouer, voire séduire par le biais de la Toile »*[24]. Les actions ou activités qui autrefois, étaient réalisées face à face, grâce à des objets matériels sont maintenant devenues des actions et activités dématérialisées.

Dans la vie quotidienne et personnelle, qui n'a jamais fait de e-commerce ? Le e-commerce est la pratique du commerce en ligne, *via* le réseau internet, remplaçant ou complétant le commerce traditionnel que l'on connaît, soit se déplacer dans un magasin pour acheter. Grâce au e-commerce, des plateformes 100% dématérialisées ont vu le jour, si bien qu'aucune

[22] *Ibid.*
[23] Serge Théophile BALIMA, « Une ou des « sociétés de l'informatique » ? », *Hermès, La Revue*, 2004/3, n°40, pp-205-209.
[24] Stéphanie LANGARD, Approche juridique de la télémédecine. Entre Droit commun et règles spécifiques, Thèse dactylographiée, Nancy, 2012, p. 24.

boutique physique n'existe (Zalando[25], Amazon[26], ou encore eBay[27]). Pour faire face à cette nouvelle concurrence permettant aux personnes de faire leurs emplettes de leur canapé, les boutiques physiques ont également proposé un service de e-commerce permettant de proposer deux alternatives d'achat, de manière physique en boutique, ou de manière dématérialisée. Outre le e-shopping, la dématérialisation du commerce concerne tous les secteurs d'activités, y compris l'alimentaire avec les drives, ou la livraison à domicile, la souscription d'un abonnement téléphonique, de gaz ou d'électricité.

Le commerce n'est pas le seul secteur d'activité possible de manière dématérialisée ; aujourd'hui, il est possible de faire des rencontres par le biais de sites dédiés, de faire du relationnel, non plus en sortant voir des personnes, mais en flânant sur les réseaux sociaux, de lire des livres sur tablette ou les écouter en audio ou même encore, de faire du e-sport, désignant « *l'ensemble des pratiques permettant à des joueurs de se confronter par l'intermédiaire d'un support électronique, et notamment le jeu vidéo, et cela quels que soient le type de jeu et la plateforme (ordinateur, console ou tablette) »*[28].

Toutes ces pratiques sont rendues possibles par la dématérialisation mais ne sont que facultatives, si bien que toute personne n'est pas dans l'obligation de faire ces activités de manière dématérialisée, bien que la société actuelle pousse fortement en ce sens.

6. **A l'obligation de dématérialiser**. En revanche, d'autres pratiques sont aujourd'hui obligatoirement dématérialisées ; l'exemple le plus marquant est le développement de la e-administration. « *Sommairement, l'administration électronique comprend trois degrés : la possibilité d'échanger avec l'administration par courrier électronique, la possibilité d'obtenir des documents provenant de l'administration par voie électronique (téléchargement), la possibilité de traiter l'ensemble d'une démarche administrative par voie électronique (téléservice)*[29]. Or l'e-administration n'est plus aujourd'hui une faculté mais une obligation ; la plupart des liens entre un usager et une administration sont dématérialisés, c'est notamment l'objectif du programme « Action publique 2022 » lancé par Edouard Philippe en 2017, la dématérialisation de tous les services publics d'ici la fin de l'année. A titre d'exemple, tous les citoyens français ont eu l'obligation cette année, de réaliser leur déclaration de revenus en ligne *via* le téléservice du service des

[25] Entreprise de commerce électronique spécialisée dans le commerce de chaussures et vêtements, créée en 2008.
[26] Entreprise de commerce en ligne créée en 1994.
[27] Site internet de commerce en ligne créé en 1995.
[28] Association France eSports, « La Charte de l'eSport », disponible à l'adresse : https://www.france-esports.org/, (consulté le 26/08/2022).
[29] Olivier VIBOUD, « e-administration », *Dictionnaire d'administration publique,* 2014, pp. 177-178.

impôts dédié à cet effet, sauf si le domicile principal de l'usager n'était pas connecté à un réseau internet[30]. Même si le recours à l'e-administration devient une obligation, des exceptions persistent afin de faire face aux quelques particularités (absence de connexion internet, accompagnement du public le plus fragile).

Le monde universitaire n'est, lui non plus, pas épargné par cette obligation de dématérialisation ; aujourd'hui tout étudiant voulant s'inscrire ou se réinscrire à la faculté doit réaliser son inscription de manière dématérialisée, soit *via* parcoursup[31] (lors d'une première inscription après le lycée), soit *via* le portail dématérialisé de son Université. A titre d'exemple, les doctorants à l'Université de Lorraine doivent se rendre chaque année sur la plateforme ADUM pour faire une demande de réinscription pour l'année suivante ou encore déposer leur dossier complet de demande de soutenance en cas de soutenance avant le 31 décembre de l'année en cours.

Dans le milieu plus professionnel, l'obligation de dématérialisation gagne de plus en plus de terrain : depuis le 1er janvier 2020, toutes les entreprises ont l'obligation d'envoyer leurs factures à destination du secteur public, par voie dématérialisée *via* le service Chorus Pro[32]. Cette obligation de facturation électronique a été étendue au secteur privé, pour les entreprises assujetties à la TVA, par la Loi de finances pour 2020[33]. Ainsi, d'ici 2026, toute la facturation interentreprise sera dématérialisée[34] à l'instar de la facturation avec le secteur public. La dématérialisation dans le milieu professionnel est devenue le principe, tandis que l'absence de dématérialisation est devenue l'exception ! Cette réalité est d'autant plus vraie dans le secteur public. En effet, le Droit de la commande publique impose aux pouvoirs adjudicateurs[35] et

[30] C. gén. impôts, art. 1649 quater B quinquies. *« La déclaration prévue à l'article 170 et ses annexes sont souscrites par voie électronique par les contribuables dont la résidence principale est équipée d'un accès internet ».*

[31] Parcoursup est une plateforme permettant aux lycéens de d'exposer leurs vœux d'études supérieures. Par cette plateforme, les écoles, organismes de formations ou encore les universités pourront accepter la demande du futur étudiant ou la refuser, entraînant immédiatement une demande d'inscription au second vœu du lycéen, et ainsi de suite.

[32] Chorus Pro est le service permettant aux administrations publiques de recevoir leurs factures en ligne.

[33] Loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020 (1), JORF n°0302, 29 décembre 2019, texte n°1.

[34] Ordonnance n° 2021-1190 du 15 septembre 2021 relative à la généralisation de la facturation électronique dans les transactions entre assujettis à la taxe sur la valeur ajoutée et à la transmission des données de transaction : Cette ordonnance fixe un calendrier d'exécution de cette obligation : « *Les obligations de facturation électronique seront imposées : à compter du 1er juillet 2024, en réception, à l'ensemble des assujettis, à compter du 1er juillet 2024, en transmission, aux grandes entreprises, à compter du 1er janvier 2025 aux entreprises de taille intermédiaire, à compter du 1er janvier 2026 aux petites et moyennes entreprises et microentreprises* ».

[35] C. com. publ., art. L. 1211-1. *« Les pouvoirs adjudicateurs sont : 1° Les personnes morales de droit public ; 2° Les personnes morales de droit privé qui ont été créées pour satisfaire spécifiquement des besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial, dont : a) Soit l'activité est financée*

aux entités adjudicatrices[36] de dématérialiser les marchés publics à compter du 1er octobre 2018. Ainsi, une offre reçue en format papier, en réponse à un marché public lancé, doit être qualifiée d'irrégulière et se voit donc écartée au seul motif que son format n'est pas dématérialisé.

La dématérialisation n'est donc pas qu'une simple possibilité mais peut se révéler être une véritable obligation, touchant notre sphère personnelle et professionnelle, si bien que toute personne est amenée à utiliser la dématérialisation, un jour ou l'autre, y compris pour les données les plus importantes et les plus sensibles.

7. **La dématérialisation de données les plus importantes et sensibles.** Trois secteurs d'activités ont marqué les esprits grâce à la dématérialisation de leurs services, de leurs activités et de leurs documents, alors même que les données traitées sont sensibles : les secteurs bancaires, notariaux et judiciaires.

Le secteur bancaire en France est l'un des précurseurs dans le domaine de la dématérialisation ; dès le 5 novembre 1984, les titres financiers ont été dématérialisés. Cela « *a consisté à remplacer les titres (tels que les actions ou les obligations) papier détenus physiquement par les investisseurs par des inscriptions dans les comptes titres au sein des banques. Elle a entraîné la gestion informatisée des comptes de titres (compte titres ordinaire ou PEA) et des opérations d'échange sur le marché boursier* »[37]. En 2022, nous pouvons considérer que presque la totalité des activités bancaires peuvent être dématérialisées, si bien que certaines banques ne bénéficient même pas d'agences physiques, mais ne sont accessibles que sur la Toile[38]. En quelques clics, il est aujourd'hui possible de consulter ses comptes, de faire un virement bancaire, de faire opposition, ou bien encore de souscrire à un prêt bancaire.

---

majoritairement par un pouvoir adjudicateur ; b) Soit la gestion est soumise à un contrôle par un pouvoir adjudicateur ; c) Soit l'organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par un pouvoir adjudicateur ; 3° Les organismes de droit privé dotés de la personnalité juridique constitués par des pouvoirs adjudicateurs en vue de réaliser certaines activités en commun ».

[36] C. com. publ. art. L. 1212-1. *« Les entités adjudicatrices sont : 1° Les pouvoirs adjudicateurs qui exercent une des activités d'opérateur de réseaux définies aux articles L. 1212-3 et L. 1212-4 ; 2° Lorsqu'elles ne sont pas des pouvoirs adjudicateurs, les entreprises publiques qui exercent une des activités d'opérateur de réseaux définies aux articles L. 1212-3 et L. 1212-4 ; 3° Lorsqu'ils ne sont pas des pouvoirs adjudicateurs ou des entreprises publiques, les organismes de droit privé qui bénéficient, en vertu d'une disposition légalement prise, de droits spéciaux ou exclusifs ayant pour effet de leur réserver l'exercice de ces activités et d'affecter substantiellement la capacité des autres opérateurs économiques à exercer celle-ci. Ne sont pas considérés comme des droits spéciaux ou exclusifs les droits d'exclusivité accordés à l'issue d'une procédure permettant de garantir la prise en compte de critères objectifs, proportionnels et non discriminatoires ».*

[37] Ministère de l'économie des finances et de la souveraineté industrielle et numérique, « La gestion des transactions financières », *faciléco,* 2013. Disponible à l'adresse : https://www.economie.gouv.fr/ (consulté le 12/09/2022).

[38] Le terme « Toile » signifie « Internet ».

Pour autant, tout n'est pas encore dématérialisé ; les citoyens sont encore attachés à l'argent liquide, bien que son utilisation soit en baisse. *« Technologiquement, on peut très bien envisager la disparition du liquide et la création de nouvelles infrastructures de paiement privées, du type diem, la monnaie que voulait lancer Facebook (ex-libra). Mais la monnaie est une construction sociale. Oui, l'argent liquide disparaîtra un jour mais cette disparition n'arrivera pas tout de suite et pas en même temps dans tous les pays »*[39]. A titre d'exemple, en Suède, *« les billets ne représentent plus que 1% de la masse monétaire de la couronne suédoise, ce qui permet de donner un aperçu de l'avenir. […] l'utilisation de l'argent liquide est passée de 40% des paiements en 2010 à moins de 10% en 2020 »*[40], annonçant progressivement la fin du paiement en liquide en Suède. Cependant la Suède n'est pas révélatrice des habitudes des pays de la zone euro. Selon une étude réalisée par la Banque centrale européenne en 2020[41], 79% des transactions ont été réalisées en espèce en 2016 (54% en valeur), contre 73% en 2019 (48% en valeur), montrant que l'espèce reste toujours le moyen de paiement privilégié. En France, l'espèce reste également *« le moyen de paiement le plus utilisé […] dans l'Eurosystème, en magasin et entre particuliers : leur part s'établit à 59 % en France (73 % en zone euro) alors que les paiements par carte ne représentent que 35 % des transactions (24 % en zone euro) »*[42]. Pour autant, la pandémie du Covid-19 est venue contrebalancer les pratiques ; l'utilisation de la carte bancaire et notamment du « sans contact », ou encore l'utilisation du mobile comme moyen de paiement, s'utilise de plus en plus, même si les espèces restent le moyen de paiement le plus utilisé, pour les achats du quotidien. On tend tout de même vers une utilisation toujours plus croissante des moyens de paiement dématérialisés, notamment avec le développement des plateformes d'achats en ligne. Le secteur bancaire en France est l'un des secteurs les plus avancés dans la dématérialisation, pour autant la dématérialisation totale des moyens de paiement n'est pas pour tout de suite.

« *A la pointe de la dématérialisation des échanges depuis les années 90, le notariat a permis la signature du premier acte authentique électronique en 2008. En 2015, 1 102 061 actes en particulier ont ainsi été signés par leur clients sur une tablette graphique et sont dotés d'une*

[39] Eric ALBERT et Olena HAVRYLCHYK, « L'argent liquide disparaîtra un jour, mais pas tout de suite », *Le monde*, 2022.
[40] *Ibid.*
[41] Banque Centrale Européenne, *« Study on the payment attitudes of consumers in the euro area (SPACE)* », Etude, 2020.
[42] Banque de France, « Utilisation des espèces dans les transactions ». Disponible à l'adresse : https://www.banque-france.fr/ (consulté le 12/09/2022).

sécurité identique à celle du support papier ».[43] L'acte authentique en tant que tel est un document revêtu d'une forte valeur légale et d'importantes garanties, rédigé par un officier public, et concerne les actes les plus importants de la vie : un contrat de mariage, un testament, ou encore un achat immobilier. Ces actes d'une extrême importance pour la personne ont la possibilité depuis 2000 d'être dématérialisés, grâce à la reconnaissance de la valeur probante équivalente entre l'écrit dématérialisé et l'écrit papier. Pour autant, il a fallu attendre huit ans, avant que le premier acte notarial soit dématérialisé. Depuis, la dématérialisation ne fait que se développer dans le monde notarial, par exemple avec l'obligation depuis 2018[44] pour les notaires, d'effectuer les dépôts de documents auprès des services chargés de la publicité foncière de manière dématérialisée. Il s'agit notamment des actes de vente ou des actes portant constitution d'une servitude[45].

« *Le monde juridique est indiscutablement en train de basculer dans l'ère du numérique. Le ministère de la justice s'est engagé dans un plan sans précédent de transformation numérique, qui aura pour conséquence un changement profond de ses modes de fonctionnement. Ce plan de transformation a pour ambition de rendre la justice plus accessible, plus rapide, plus efficace et plus transparente. Il offrira la possibilité d'une dématérialisation totale des procédures civiles et pénales. Il fera évoluer en profondeur les systèmes d'information de l'administration pénitentiaire et de la protection judiciaire de la jeunesse* »[46]. Si bien que depuis le 4 janvier 2021, toute personne peut saisir la justice en ligne, et depuis le 15 novembre de la même année, toute personne peut consulter l'état d'avancement d'une procédure pénale qui la concerne en ligne. Cette transformation numérique de la justice permet aux justiciables un meilleur accès aux informations les informant de leurs droits, un meilleur suivi des démarches qu'ils ont entrepris, mais également un accès à certaines de leurs données à l'instar du bulletin n°3 de leur casier judiciaire qui est disponible en ligne. Les justiciables ne sont pas les seuls concernés ; les greffes et les magistrats peuvent également suivre les différentes affaires en ligne, se servir d'outils d'aide à la rédaction de documents facilitant considérablement leur travail. Aussi, on se rend compte que la justice elle-même se dématérialise alors même que les données traitées sont sensibles, à

[43] Conseil supérieur du notariat, « Les notaires avancent avec vous », *Rapport annuel,* 2015, p.10.
[44] Décret n° 2017-770 du 4 mai 2017, portant obligation pour les notaires d'effectuer par voie électronique leurs dépôts de documents auprès des services chargés de la publicité foncière, JORF n°0107, 6 mai 2017, texte n°23.
[45] Arrêté du 2 juin 2017 définissant le champ d'application de l'obligation faite aux notaires d'effectuer par voie électronique leurs dépôts de documents auprès des services chargés de la publicité foncière, JORF n°0137, 13 juin 2017, texte n°14.
[46] Justice.fr, « La transformation numérique du Ministère de la Justice », disponible sur le site : https://www.cours-appel.justice.fr/ (consulté le 24/02/2022).

l'instar du casier judiciaire qui, au regard des données traitées, revêt des conditions d'accès très strictes. En effet, même le justiciable n'a pas accès à l'intégralité de son casier judiciaire, mais seulement au bulletin n°3 alors même que les données contenues dans l'ensemble du casier juridique le concernent.

Aussi, on constate que la dématérialisation concerne absolument tous les domaines, des plus anodins aux plus sensibles et devient véritablement une pratique ordinaire et est entrée dans les mœurs. Elle fait partie de notre quotidien et présente des avantages incontestables, mais également des inconvénients.

8. **Les avantages et les inconvénients**. Le premier avantage que l'on peut citer au regard des développements précédents, est l'accès facilité aux données, aux documents mais également aux services et activités. Pour autant, cet accès optimisé n'est pas le seul avantage de la dématérialisation : le gain de temps en est un autre, car les données et les services étant accessibles à distance et instantanément, toute personne ne perd plus de temps à se déplacer pour aller chercher un document ou bénéficier d'un service. Un troisième avantage : une traçabilité plus accrue grâce aux métadonnées[47] permettant à toute personne de contrôler qui a eu accès à la donnée ou au service, de savoir ce qui a été réalisé sur la donnée (création, modification, suppression), garantissant ainsi sa fiabilité.

En revanche, malgré ces avantages évidents, certains inconvénients persistent, faisant parfois préférer, la méthode « traditionnelle » à la dématérialisation. La première chose venant à l'esprit est la difficulté d'utilisation des outils liés à la dématérialisation. Bon nombre de personnes ne sont pas acculturées à l'utilisation des nouvelles technologies telles que l'ordinateur ou la tablette, outils nécessaires dans le cadre de l'informatisation de notre société. Cette dématérialisation met à l'écart toute personne en incapacité d'utiliser ces outils, ou tout simplement ne voulant pas les utiliser. Les raisons pour lesquelles une personne ne souhaite pas dématérialiser ses données sont multiples : ne pas vouloir changer ses habitudes, une plus grande confiance envers un document papier, plutôt qu'en un document dématérialisé, mais également la conscience du risque de piratage et de vol de données[48], qui est un des inconvénients majeurs de la dématérialisation. En effet, dès lors que les données sont dématérialisées, elles risquent d'être dérobées afin d'être utilisées à d'autres fins que celles initialement prévues ou encore d'être chiffrées pour obtenir une compensation

[47] Larousse, *V° « métadonnée »*, nom fém. La métadonnée est définie comme étant une « donnée servant à caractériser une autre donnée, physique ou numérique ».
[48] ANSSI, *Une année 2021 marquée par la professionnalisation des acteurs malveillants*, 2021. Disponible à l'adresse : https://www.ssi.gouv.fr/ (consulté le 06/05/2022).

financière contre la clé de déchiffrement. « *Dans son "Panorama de la menace informatique", l'Agence nationale de la sécurité des systèmes d'information (ANSSI) revient sur les grandes tendances ayant marqué le paysage cyber en 2021 et souligne des risques d'évolution à court terme. Alors que la généralisation des usages numériques - souvent mal maitrisés – continue de représenter un défi pour les entreprises et les administrations, l'agence observe une amélioration constante des capacités des acteurs malveillants. Ainsi, le nombre d'intrusions avérées dans des systèmes d'information signalées à l'ANSSI a augmenté de 37% entre 2020 et 2021 (786 en 2020 contre 1082 en 2021, soit désormais près de 3 intrusions avérées par jour) »*[49].

Or le piratage des données n'est pas la seule raison pouvant mener à l'inaccessibilité des données, la panne informatique l'est également : « *Une nuit, j'ai fait un cauchemar incroyable… Je commençais ma journée à l'étude et, consternation, la connexion « intranet/internet » était « hors service »… Je téléphonais au prestataire qui prenait acte de la panne… malheureusement, aucune intervention ne se programmait, faute de réactivité des sous-traitants dudit prestataire.*

Absence de mails ; impossibilité de téléacter, de se connecter aux divers sites partenaires, d'effectuer les formalités, de gérer la comptabilité (CDC-Net, notamment), d'acter les signatures électroniques ; les transformations en « support papier » étaient apportées (en catastrophe) lors des rendez-vous, sous les sourires dubitatifs des clients…

Je réalisais soudain l'état de totale dépendance « extérieure » de l'office notarial, liée à la dématérialisation des activités, et de l'absence possible de réponse lorsque les outils, initiant cette dématérialisation, ne fonctionnaient plus.

Et si, le même jour, le serveur de l'étude avait été lui aussi hors service… ?

Le réveil se mit alors à sonner ; je me réveillais et m'empressais de constater que, pour l'instant, tout fonctionnait merveilleusement bien… »[50]. Qui n'a jamais craint la panne informatique, surtout dans le milieu professionnel ? Quoi faire dans ce cas, lorsque toutes les données, tous les outils de travail sont dématérialisés ? L'entreprise (la société ou encore l'office) est bloquée et ne peut plus fonctionner engendrant une perte de temps et d'argent. Cependant, l'absence d'accès peut avoir différentes conséquences, allant d'une simple perte d'un client à la mise en danger d'une vie.

[49] ANSSI, *Une année 2021 marquée par la professionnalisation des acteurs malveillants*, 2021. Disponible à l'adresse : https://www.ssi.gouv.fr/ (consulté le 06/05/2022).
[50] Rémy GENTILHOMME, « Dématérialisation, oui, mais…», *Defrénois,* 2012, n°19, p. 937.

La dématérialisation nécessite la mise en place de garde-fous juridiques et techniques afin d'endiguer les risques liés à la dématérialisation. Malgré ces risques avérés, la dématérialisation ne fait que s'accroitre, y compris la dématérialisation des données sensibles ou d'une extrême importance, montrant que les avantages sont plus nombreux que les risques d'autant que ces risques sont connus, contrôlés et maîtrisés selon le type de données traitées et l'activité concernée.

9. **Un moyen de faire face à la pandémie du Covid-19.** Cela est d'autant plus vrai que la dématérialisation s'est considérablement développée lors de la pandémie du Covid-19 qui nous a tous touché[51]. Le risque de contamination, les confinements et les couvre-feux ont conduit les personnes à devoir rester chez elles pour des questions de sécurité sanitaire, les obligeant à s'adapter à ces nouvelles mesures. Plus question d'aller voir ses proches, de flâner dans les magasins, ou encore d'aller sur son lieu de travail. Pour autant, il était nécessaire de continuer à faire toutes ces choses, mais autrement. La dématérialisation était la réponse parfaite à cette problématique ! Le lien avec les proches étaient maintenus grâce aux réseaux sociaux ou au visio, les courses pouvaient se faire par drive, limitant les contacts avec les autres, ou *via* les plateformes de e-commerce, les patients pouvaient voir leur médecin par le biais d'une téléconsultation limitant la propagation du virus en cas de cas positif au Covid-19, et le travail pouvait se faire depuis son domicile. Le télétravail a permis pour bon nombre de personnes et d'entreprises de continuer leur activité professionnelle, malgré les restrictions sanitaires. Pour autant, il a été nécessaire de mettre en place des outils de visioconférence, permettant les échanges plus fluides entre les salariés (en appui aux mails) ainsi qu'un lien social, mais également des outils de partage de documents, le cas échéant. Le Droit s'est également vu bousculé à la suite de cette pandémie, accélérant parfois la parution de certains textes. Prenons l'exemple de la signature électronique à distance des actes notariés : depuis le 4 avril 2020, les actes notariés ont la possibilité d'être signés électroniquement à distance[52]. Pour autant, ce Décret ne devait voir le jour que l'année suivante, mais son entrée en vigueur a été avancée pour faire face au premier confinement.

La dématérialisation a véritablement été un moyen efficace et indispensable pour faire face aux problématiques posées par la pandémie. Aujourd'hui encore, certaines habitudes

[51] Laura LETOURNEAU, « Transformations numériques et entrepreneuriales – l'improbable transformation numérique de la santé », *Le journal de l'école de Paris du management,* 2022, n°155, pp.23-30.
[52] Décret n° 2020-395 du 3 avril 2020 autorisant l'acte notarié à distance pendant la période d'urgence sanitaire, JORF n°0082, 4 avril 2020, texte n°1.

dématérialisées prises perdurent à l'instar du télétravail qui est entré véritablement dans les mœurs comme la consultation de professionnels de santé par téléconsultation.

10. **La dématérialisation en santé.** La dématérialisation en santé n'a pas été impulsée par cette pandémie, elle était déjà présente depuis plusieurs années ; « *le champ de l'informatisation s'est élargi. Visant d'abord la gestion des Caisses*[53] *pour simplifier et accélérer le traitement des dossiers de remboursement, et pour permettre le contrôle médicalisé des dépenses, il s'est étendu à l'ensemble du système de santé en se donnant des objectifs strictement médicaux, concernant l'information des praticiens, le suivi des patients, et l'assistance au diagnostic. Il s'ouvre donc sur une exploitation et une circulation des données médicales* »[54]. En effet, se sont développés très tôt des échanges dématérialisés entre professionnels de santé par mail ou par téléphone afin d'avoir un avis sur un patient, ce qui est un pas vers la discipline appelée télémédecine, mais également les créations de premiers dossiers patients informatisés à la fin des années 90. Les données de santé se dématérialisent dans un but précis : une prise en charge du patient optimisée.

On se rend compte que dès le début, la dématérialisation dans le domaine de la santé ne concerne pas que la dématérialisation des documents contenant des données de santé, elle concerne également la dématérialisation de la prise en charge du patient, de manière générale. En effet, des outils tels que le téléphone ou le mail servent à apporter une expertise, un avis ou à se coordonner, et cela dans le but d'une meilleure prise en charge patient. « *Ce sont les modalités d'exercice de la médecine qui sont influencées par le recours aux TIC*[55]*, en participant à l'évolution même de la relation de soins […]. Si le citoyen peut être virtuel, le patient ou le médecin l'est tout autant. Le e-patient peut donc rencontrer un e-médecin au cœur d'une relation médicale alors dématérialisée. Le colloque singulier désormais dématérialisé se réunit autour de la réalisation d'un acte médical dématérialisé* »[56].

Avant même les années 2000, il était déjà fait état que « *les technologies de l'information et de la communication sont au cœur de la mise en œuvre de nouvelles pratiques médicales* »[57].

[53] Les Caisses d'assurance maladie.
[54] Jean-Claude CHOCQUE, « Impacts et enjeux de l'informatisation dans le système de santé », *Gazette du Palais*, 2000, n°293, p15.
[55]Technologie de l'information et de la communication.
[56] Claire DEBOST, *Les technologies de l'information et de la communication et la relation de soins : invariances et inconstances*, Thèse dactylographiée, Montpelier, 2014, p. 8.
[57] Gérard THERY, « Les autoroutes de l'information : rapport au Premier Ministre », *Collection des rapports officiels*, 1994, p. 56.

11. **Une modification de notre système de santé.** *« Les nouvelles technologies de l'information (NTI) transforment les sociétés. Peu d'époques ont connu une mutation d'une telle ampleur ; aucune au rythme impose par les NTI. Dans ce maelström historique, le secteur de la santé est soumis à des pressions extrêmes. Parce que l'information est au cœur de la relation médecin-malade, les bouleversements en cours retentissent directement sur les équilibres traditionnels du système de santé »*[58]. L'informatisation et la dématérialisation ont entraîné une modification de notre système de santé tout entier notamment au regard du caractère sensible des données de santé. En effet, la mise en place de la dématérialisation a nécessité l'utilisation des nouvelles technologies qui ont impliqué d'une part, l'ouverture de nombreuses possibilités en santé grâce à ces nouvelles technologies et d'autre part, une sécurité particulière à accorder aux données de santé, au regard de leurs sensibilité. En effet, il serait préjudiciable pour le patient, le professionnel de santé mais aussi pour l'établissement de santé, de voir les données de santé du patient erronées, ou encore volées.

Ces quinze dernières années marquent une évolution exponentielle de l'utilisation du numérique en santé et de la dématérialisation des données. Les évolutions les plus marquantes en la matière sont : la création en 2009 de l'Asip Santé (aujourd'hui l'Agence Numérique de Santé (ANS)) chargée de contribuer « *à l'amélioration du système de santé aux côtés de tous les acteurs, privés comme publics, professionnels ou usagers, grâce à la transformation numérique »*, l'encadrement juridique de la télémédecine[59] dès 2010, le lancement du programme « hôpital numérique » en 2011 piloté par la Direction Générale de l'Offre de Soins (DGOS) permettant de définir un plan de développement de modernisation des systèmes d'information hospitaliers sur six ans, l'inclusion dans le Code de la santé publique de la valeur probante des documents contenant des données de santé en 2017 puis récemment, la mise en place de la stratégie de transformation du système de santé « Ma santé 2022 ».

Toutes ces évolutions marquantes montrent la transformation de notre système de santé, afin de prendre en compte l'utilisation des technologies et le développement du numérique en santé. Elles permettent notamment d'optimiser au mieux la prise en charge du patient grâce au développement de certains procédés, la création de nouveaux outils à l'instar du dossier médical partagé ou des logiciels favorisant la coordination entre les professionnels de santé ou

[58] Didier TABUTEAU, « e-santé et nouvelles technologies », *Les tribunes de la santé*, 2010, n°29, pp. 3-5.
[59] C. santé publ., art. L. 6316-1. *« La télémédecine est une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport un professionnel médical avec un ou plusieurs professionnels de santé, entre eux ou avec le patient et, le cas échéant, d'autres professionnels apportant leurs soins au patient ».*

encore la prise en charge du patient à distance. Notre système de santé est encore aujourd'hui en pleine mutation.

12. **L'informatisation en santé en progression.** L'outil phare le plus emblématique associé à la dématérialisation en santé est le dossier patient informatisé. En effet, chaque établissement de santé a l'obligation de tenir pour chaque patient, un dossier patient. Avec le développement de la dématérialisation et des technologies, ce dossier initialement papier est devenu un dossier informatisé. Ce dossier patient informatisé[60] par rapport au dossier papier traditionnel[61], permet notamment une meilleure prise en charge du patient, une meilleure coordination des soins et un gain de temps considérable[62] pour les professionnels[63].

Bien que ce dossier patient informatisé soit de plus en plus l'outil indispensable pour les établissements de santé, on constate tout de même que tous n'en sont pas équipés ou pas totalement. Depuis 2013, la DGOS publie annuellement un Atlas des systèmes d'informations hospitaliers (SIH) « *afin de mettre à disposition de l'ensemble des acteurs de la santé les données principales et tendances de l'évolution des systèmes d'information hospitaliers sur le territoire* »[64]. Le dernier Atlas des SIH en date est celui de 2020 ; seul 84% des établissements ont fourni leurs données. *« Sur 1 575 établissements répondants, 76% ont achevé*

---

[60] ANAP, « Comprendre les problématiques d'un projet de Dossier Patient Informatisé et Interopérable », 2015. Disponible à l'adresse : https://ressources.anap.fr/ (consulté le 06/07/2021).

[61] Mathias BEJEAN, Frédéric KLETZ et Jean-Claude MOISDON, « Création de valeur organisationnelle et technologies de l'information à l'hôpital : le cas du dossier patient informatisé », *Gestion et Management Public*, 2018/2, vol. 6/n°4, pp. 9-24. D'autres avantages sont à envisager : *« rappelons que le DPI est censé éviter les inconvénients bien connus d'un dossier patient manuscrit parfois illisible, et que l'on recherche de bureau en bureau ; il permet de transmettre ou de recevoir en un clic les données médicales d'un patient, parfois anciennes ; il facilite, en outre, par copier/coller la constitution du compte rendu de sortie. En bref, il s'agit d'un outil qui se présente davantage comme une aide à la pratique. […] L'information médicale doit contribuer à l'amélioration de la qualité, de la sécurité et de l'efficience de la prise en charge en se centrant sur les données du patient. En apportant à tout moment et à tout professionnel hospitalier habilité un ensemble d'informations riche et structuré sur le patient, le DPI offre de fortes promesses. Par sa traçabilité, sa lisibilité et la cohérence des informations, il est présenté comme un outil pouvant permettre la réduction des examens redondants, des décisions plus rapides, ou encore une meilleure coordination entre professionnels ».*

[62] *Ibid.* D'après une étude menée en 2018, il apparaît que le gain de temps n'est pas ressenti de la même manière par tous les professionnels de santé ; *« sur la perception des gains de temps, si les médecins ne perçoivent pas de gain induit par le DPI (d'où, d'ailleurs, un phénomène de contournement de certains, qui continuent à utiliser des dossiers papier), ils apprécient la plus grande traçabilité et l'accessibilité des données dans leur grande majorité. Et le personnel infirmier, malgré des difficultés lors de la mise en œuvre, ne pourrait plus s'en passer, estimant majoritairement gagner du temps (consultations fréquentes du dossier et alimentation du DPI pour tout ce qui concerne le dossier de soins) ; le secrétariat estime en gagner davantage encore (pré-rédaction du Compte rendu de sortie par des médecins, recherche d'informations etc.) ».*

[63] Marc DUPONT, « Dossier médical – Dossier en établissement de santé. Dossier dématérialisé », *Droit médical et hospitalier*, Litec, fasc. 10-20, 2022. On peut même aller plus loin en affirmant que le DPI *« présente un intérêt évident au plan médical (disponibilité, partage et circulation de l'information), épidémiologique, économique ou encore archiviste (conservation des documents) ».*

[64] Atlas des SIH 2020, « Etat des lieux des systèmes d'information hospitaliers », 2021.

l'informatisation du dossier médical du patient et 21% sont en cours d'informatisation »[65], ce qui est en nette progression par rapport à 2018. Pour autant, même si l'informatisation du dossier patient est en cours depuis de nombreuses années, on constate que le chantier n'est pour autant pas terminé, y compris pour de grands centres hospitaliers ; 32% d'entre eux n'ont pas encore terminé le déploiement d'un dossier patient informatisé.

13. **Un des derniers projets en date.** L'enjeu de la dématérialisation ne se limite pas au dossier patient informatisé, mais va bien au-delà. Comme cela a été évoqué, la dernière grande évolution du numérique en santé est la Loi relative à l'organisation et à la transformation du système de santé[66] dite loi « Ma Santé 2022 ». Cette Loi « *propose une vision d'ensemble et des réponses globales aux défis auxquels est confronté le système de santé français. Tout d'abord, des inégalités dans l'accès aux soins, avec de plus en plus de Français qui connaissent des difficultés à accéder à un médecin dans la journée et sont parfois contraints de se rendre aux urgences par défaut. Ensuite, des aspirations chez les professionnels à mieux coopérer entre eux, à disposer de davantage de temps pour soigner leurs patients et à être formés autrement* ». Pour parvenir aux objectifs liés à la transformation de notre système de santé, le numérique joue une place primordiale. « *La transformation de notre système de santé ne pourra avoir lieu sans un développement massif et cohérent du numérique en santé en France* »[67] impliquant la mise en place de la feuille de route « accélérer le virage du numérique en santé ». Cette feuille de route est divisée en cinq grandes orientations : *« renforcer la gouvernance du numérique en santé, intensifier la sécurité et l'interopérabilité des systèmes d'information en santé, accélérer le déploiement des services numériques socles, déployer au niveau national des plateformes numériques de santé, soutenir l'innovation et favoriser l'engagement des acteurs* »[68]. Cela a notamment abouti à la création de l'espace numérique de santé (ENS), aussi appelé « mon espace santé » disponible depuis janvier 2022 pour toute personne. Il permet d'offrir a tout usager un espace numérique regroupant des services numériques socles[69] pour sa prise en charge tels qu'une messagerie sécurisée ou encore l'accès à son dossier médical partagé.

---

[65] *Ibid.*

[66] Loi n°2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1), JORF n°0172, 26 juillet 2019, texte n°3.

[67] Ministère des Solidarités, de l'autonomie et des personnes handicapées, « Feuille de route « accélérer le virage numérique » », 2019. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 10/06/2022).

[68] ANS, « Feuille de route « accélérer le virage numérique en santé » ». Disponible à l'adresse : https://esante.gouv.fr/ (consulté le 06 :06/2022).

[69] Et plus généralement tout service numérique. *« On comprend que la liste est finalement ouverte et que l'espace numérique de santé est pensé comme un outil évolutif amené à évoluer au gré du développement des nouvelles technologies en santé ».* (Lydia MORLET-HAIDARA, « L'espace numérique de santé : une création

Par la mise en place de la feuille de route « accélérer le virage du numérique en santé », on constate que le numérique en santé est véritablement un chantier moteur de la transformation de notre système de santé et est primordial. Le numérique en santé et la dématérialisation des données sont l'avenir de la santé, sont l'avenir de la prise en charge du patient.

14. **Des modifications en perspective.** Cette informatisation du monde de la santé implique inévitablement un changement des pratiques impulsées par l'usage des nouvelles technologies. Ces dernières contribuent à faire évoluer notre système de santé à tous les niveaux, y compris le rapport qu'entretient le professionnel de santé avec son métier. Chaque professionnel de santé possède des compétences médicales spécifiques à sa profession. Or, les compétences médicales ne suffisent pas pour prendre en charge le patient ; en effet depuis toujours, le professionnel de santé doit aussi avoir des notions de Droit et aujourd'hui, des notions d'informatique.

La relation de soin qu'entretient le professionnel avec son patient repose sur des principes remontant au serment d'Hippocrate, qui sont devenus des principes juridiques. *« Admis(e) dans l'intimité des personnes, je tairai les secrets qui me seront confiés. Reçu(e) à l'intérieur des maisons, je respecterai les secrets des foyers et ma conduite ne servira pas à corrompre les mœurs »*[70]. Cet extrait du serment d'Hippocrate renvoie à la notion de secret professionnel que tout professionnel doit respecter. Certes, ce serment ne possède aucune valeur juridique en tant que tel, mais il est tout de même un des textes fondateurs de la déontologie médicale dont certains principes font échos à des textes de lois. En l'espèce, depuis toujours, le médecin a le devoir de respecter le secret des informations concernant chacun de ses patients. Ce secret est le fondement même de la relation de confiance[71] entre le médecin et son patient, et est aujourd'hui un principe juridique[72]. Au fil du temps, d'autres principes juridiques se sont développés créant des droits pour les patients et donc des obligations pour les professionnels de santé, les obligeant à avoir des compétences juridiques, dans le cadre de la prise en charge du patient.

Outre les compétences juridiques, le développement du numérique en santé oblige les professionnels de santé à développer également des compétences informatiques. Bien que la nouvelle génération ait grandi avec les nouvelles technologies dont l'utilisation devient

---

de la loi relative à l'organisation et à la transformation du système de santé », *Journal du Droit de la Santé et de l'Assurance-Maladie,* 2019/3, n°24, pp. 17-21).

[70] CNOM, « Le serment d'Hippocrate », 2019.

[71] Portes L. « Du secret médical », Communication à l'Académie des Sciences Morales et Politiques, 5 juin 1950, publiée dans son ouvrage posthume : *À la recherche d'une éthique médicale,* Masson, 1964, p. 153.

[72] C. santé publ., art. L. 1110-4.

presque innée, les professionnels en exercice voient leur rapport avec leur métier évoluer ; ce n'est plus le professionnel avec le patient, mais le professionnel avec le patient et l'outil informatique. Si bien que les professionnels de santé doivent s'adapter aux nouvelles pratiques notamment lorsque le Droit oblige à la dématérialisation comme cela peut être le cas pour la déclaration de certaines maladies[73]. Or il ne faut pas penser que les compétences informatiques une fois acquise le sont *ad vitam aeternam*. A l'instar du domaine médical ou du Droit, l'informatique évolue d'année en année mais de manière exponentielle, obligeant, y compris la nouvelle génération, à s'adapter aux nouvelles technologies.

Les compétences médicales et juridiques acquises par les professionnels de santé doivent donc aujourd'hui s'étendre aux compétences informatiques.

15. **Les enjeux de la dématérialisation en santé.** On constate donc que le numérique en santé et la dématérialisation des données ont beaucoup d'impact sur le système de santé en général. Or, cet impact et ces changements sont-ils suffisamment bénéfiques au regard du bouleversement que cela entraîne ? La réponse à cette question est oui, tout simplement au regard des évolutions bénéfiques pour la prise en charge du patient qu'ils peuvent apporter. De plus, tous les domaines d'activités sont confrontés à la dématérialisation ; le domaine de la santé ne peut faire exception.

Les nouvelles technologies permettent des opportunités qui à l'heure actuelle peuvent relever de la science-fiction mais qui demain seront réalité. Prenons l'exemple de l'hologramme qui est l'image en trois dimensions ; autrefois relevant de la fiction, l'hologramme est aujourd'hui une réalité. « *Je peux tout en étant à Paris, donner une conférence en temps réel à Singapour par la voix de mon hologramme. On me filme à Paris et l'image immatérielle de mon être est « télé portée » en trois dimensions, à plusieurs milliers de kilomètres. Et je peux répondre en temps réel, par la voix de mon hologramme, aux questions posées par les lointains spectateurs dont l'image m'est aussi retransmise en trois dimensions et qui du coup paraissent réellement être en face de moi. Un authentique dialogue s'établit dans la « salle immersive ». Il s'agit donc de beaucoup plus qu'une simple « vidéo-conférence » sur écran, mais bien d'une présence virtuelle et désincarnée, véritablement « télé portée »* »[74]. La dématérialisation de la personne par l'hologramme n'est que la retranscription de l'image de quelqu'un ou de quelque chose en trois dimensions, mais l'interaction possible reste assez limitée. Mais qui

[73] Instruction N°DGS/SP2/DGOS/PF5/2016/112 du 4 juillet 2016 relative au déploiement de l'application e-DO pour la télé-déclaration de l'infection par le VIH/Sida.
[74] Xavier LABBÉE, « L'hologramme, la téléprésence et l'être immatériel », *LPA* 20 sept. 2012, n° 264, p. 11.

sait, avec le développement des technologies, il pourra peut-être être possible de pousser la téléprésence permettant à l'hologramme d'interagir physiquement, permettant la réalisation d'acte à distance, en l'absence de la robotique. Avec les nouvelles technologies, le champ des possibilités reste infini et présente un intérêt primordial pour la santé.

16. **La dématérialisation au sein des établissements santé**. En l'état actuel des choses, le numérique en santé et la dématérialisation des données de santé font leur chemin au sein des établissements de santé afin de faire partie intégrante de la prise en charge du patient. Or cette intégration nécessite un encadrement juridique, mais également technique à la hauteur des données traitées.

On constate que la dématérialisation n'est absolument pas une pratique nouvelle, et est d'ores et déjà utilisée dans de nombreux domaines, y compris en santé. Elle bénéficie également d'un encadrement juridique déjà très riche dans de nombreux domaines tels que les marchés publics, la facturation, les actes authentiques notariés, l'écrit électronique de manière générale et tend même à devenir la norme, avec l'obligation de dématérialiser dans certains cas comme la e-déclaration d'impôt ou bientôt la e-prescription médicale.

Pour autant, la dématérialisation est un sujet très vaste impliquant l'utilisation des nouvelles technologies qui ne cessent de se développer au fil du temps de manière exponentielle créant toujours plus de nouvelles opportunités, mais également de nouveaux risques. Si bien que l'encadrement juridique et technique de la dématérialisation est d'une extrême complexité, en particulier pour les données de santé au regard de leur sensibilité.

L'intérêt de l'étude « la dématérialisation en établissement de santé » consiste à établir si les données de santé dématérialisées bénéficient d'une sécurité et d'une valeur juridique équivalentes aux données de santé matérialisées sur un support tangible et si oui, de déterminer les modalités à mettre en place pour arriver à ce résultat. Le second intérêt de l'étude est de déterminer les conséquences qu'entraînent la dématérialisation des données de santé au sein d'un établissement de santé pour le patient.

L'étude porte exclusivement sur la dématérialisation des données de santé ; est donc exclue la dématérialisation des actes administratifs tels que les documents RH, la facturation mais également les documents envoyés et les échanges effectués avec les Caisses d'Assurance Maladie.

Notre analyse portera donc d'une part sur la dématérialisation matérielle de la donnée de santé (partie 1) ; est envisagée dans cette partie de déterminer les mesures devant être mises en

place afin de garantir la valeur juridique d'un document contenant des données de santé à l'instar d'un document papier. Et d'autre part, nous nous interrogerons sur les conséquences qu'entraînent la dématérialisation des données pour le patient au sein d'un établissement de santé (partie 2).

PREMIERE PARTIE : LA DEMATERIALISATION PHYSIQUE DE LA DONNEE DE SANTE

17. **La dématérialisation d'un support physique.** Au sein d'un établissement de santé, l'enjeu premier de la dématérialisation est de rendre immatériel le maximum de documents, en les créant directement en format numérique et/ou en transformant les documents papier en format numérique. Les documents concernés sont ceux relatifs aux ressources humaines, les factures aux fournisseurs[75], mais tout particulièrement ceux contenant des données de santé. Ces derniers représentent une part très importante des documents produits par un établissement de santé et leur dématérialisation représente des intérêts qui ne sont plus à démontrer : une meilleure prise en charge du patient, une optimisation des coûts pour l'établissement[76].

18. **La dématérialisation : un projet à part entière[77]**. Le souhait pour un établissement, de procéder à la dématérialisation de ses documents est un projet à part entière et de grande envergure, notamment au regard du temps et des coûts à consacrer. Il est donc impératif pour la direction d'un établissement de réaliser une étude complète de ce projet afin d'identifier : les documents à dématérialiser (que ce soit les nouveaux directement en format numérique et/ou les documents papier à copier en format numérique), le personnel impliqué, les coûts inhérents aux projets, les risques envisagés, les solutions à mettre en place pour minimiser les risques encourus par l'établissement, et notamment la prise en compte du cadre éthique et juridique.

19. **Le cadre juridique de la dématérialisation.** Le Droit français admet depuis longtemps, notamment dès la création du Code civil en 1804, la valeur juridique de l'écrit sous sa forme papier, afin que celui-ci puisse être utilisé en tant que preuve devant un tribunal. La preuve est un « *fait, témoignage, raisonnement susceptible d'établir de manière irréfutable la vérité ou la réalité de (quelque chose) »*[78] et notamment *« tout moyen tendant à établir la réalité d'un acte ou d'un fait juridique »*[79]. L'émergence des technologies a conduit le Droit français à évoluer en 2000[80] afin d'adapter le droit de la preuve aux nouvelles technologies et reconnaitre l'écrit numérique comme mode de preuve valable qu'il soit créé nativement de manière numérique ou qu'il résulte de la dématérialisation d'un écrit papier.

---

[75] Christophe DE LA MARDIERE, « Dématérialisation de la preuve : la facture électronique », *Gestion & Finances Publiques*, 2017/6, n°6, pp. 99-91.
[76] ANAP, « Zéro papier pour soigner : pourquoi ? Comment ? », 2017. Disponible à l'adresse : https://ressources.anap.fr/ (consulté le 05/08/2021).
[77] *Ibid.*
[78] TLFi, *V° « preuve »*, subst. fém.
[79] *Ibid.*
[80] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62, 14 mars 2000, texte n°1.

Pour qu'un document numérique puisse être utilisé comme preuve devant un tribunal, des conditions inhérentes à ce format numérique sont à prendre en compte et à respecter par l'établissement de santé, lors de la mise en place de son projet de dématérialisation des documents. Le respect de ces conditions permettra de rendre admissible un document en tant que preuve permettant à l'établissement de santé de s'en prévaloir en cas de contentieux.

20. **L'admissibilité de la preuve**. En Droit français, le principe est la liberté du mode de preuve sauf dispositions contraires. En effet, le code de procédure pénale précise qu' « *hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui* »[81]. Il en est de même en droit commercial[82], « *la preuve de l'existence et du contenu d'un engagement commercial peut être rapportée par tous moyens, quel que soit le montant de celui-ci, s'il a pour objet une somme d'argent. Ce peut être, bien entendu en produisant un écrit, acte sous seing privé (même en matière commerciale, les parties en ont généralement rédigé un) ou acte authentique (ce qui est rare)* »[83] ainsi qu'en droit civil : « *hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen* »[84]. En revanche l'admissibilité du mode de preuve ne signifie pas que la preuve aura forcément une valeur juridique.

21. **Les modes de preuves**. Cinq modes de preuves[85] sont prévues en droit civil : l'écrit, le témoignage, les présomptions, l'aveu et le serment. Chaque mode de preuve définit des conditions à remplir afin de le rendre admissible devant un juge. À titre d'exemple, « *les présomptions qui ne sont pas établies par la loi, sont laissées à l'appréciation du juge, qui ne doit les admettre que si elles sont graves, précises et concordantes, et dans les cas seulement où la loi admet la preuve par tout moyen* »[86]. Ainsi, la preuve par présomptions est admise sous certaines conditions : celles-ci doivent être « *graves, précises et concordantes* »[87]. Dans le cas contraire, ce mode de preuve ne pourra pas être utilisé, peu importe la position du juge.

[81] C. proc. pén., art. 427.
[82] Cass. Civ. 1re, 23 sept. 2020, n° 19-11.441, publié au bulletin. Dans cet arrêt, la Cour de cassation rappelle que « *la preuve à l'égard d'une société commerciale peut être rapportée par tout moyen* ».
[83] Inconnu, Preuve commerciale, fiches d'orientation, *Dalloz*, septembre 2021.
[84] C. civ., art. 1358.
[85] Inconnu, Preuve (Droit civil), fiches d'orientation, *Dalloz*, juin 2022.
[86] C. civ., art. 1382.
[87] *Ibid.*

22. **Le poids de la preuve**. Ces modes de preuves n'ont pas tous la même force devant un juge. En effet, on distingue les preuves parfaites et les preuves imparfaites[88] : les preuves parfaites qui lient le juge et les preuves imparfaites qui permettent au juge d'apprécier la valeur probante de la preuve[89]. *« La valeur probante d'une preuve est son aptitude à emporter la conviction du juge. C'est son caractère convainquant, la crédibilité, la confiance, le crédit que le juge peut lui accorder en conscience »*[90].

23. **Les preuves parfaites**. Les preuves parfaites sont l'écrit, l'aveu et le serment dit décisoire. A titre d'exemple, *« l'aveu est la déclaration par laquelle une personne reconnaît pour vrai un fait de nature à produire contre elle des conséquences juridiques. Il peut être judiciaire ou extrajudiciaire »*[91]. Lorsque l'aveu est extrajudiciaire, soit réalisé en dehors d'une instance judiciaire, il perd sa qualification de preuve parfaite, *« sa valeur probante* [sera] *laissée à l'appréciation du juge »*[92]. En revanche, lorsqu'il est judiciaire, celui-ci *« est irrévocable, sauf en cas d'erreur de fait »*[93]. La preuve est parfaite si celle-ci respecte les conditions, le cas échéant, énoncées par le Code civil. Si une des conditions n'est pas remplie, la preuve n'est plus parfaite et le juge appréciera si cette preuve est convaincante.

24. **Les preuves imparfaites**. Les preuves imparfaites sont le témoignage, les présomptions et le serment dit supplétoire. Ces modes de preuves ne liant pas le juge, il est nécessaire d'emporter la conviction du juge[94]. Il est recommandé, lors de l'utilisation d'une de ces preuves, de la compléter par une autre preuve corroborant la première, à l'instar du commencement de preuve par écrit.

25. **Le commencement de preuve par écrit**. En principe, l'écrit est une preuve parfaite qui est valable devant un juge dès lors qu'il répond aux conditions exigées par la Loi. Dès lors qu'une des conditions n'est pas réunie, l'écrit perd de sa valeur et n'est plus qu'un commencement de preuve par écrit. « *Constitue un commencement de preuve par écrit tout écrit qui, émanant de celui qui conteste un acte ou de celui qu'il représente, rend vraisemblable ce qui est allégué »*[95]. À titre d'exemple, une blockchain est considérée comme commencement de preuve par écrit, notamment car « *les utilisateurs d'une blockchain étant*

[88] Gwendoline LARDEUX, « Preuve : modes de preuves », *Répertoire de droit civil - Dalloz*, 2019.
[89] Isabelle GAVANON, « Blockchain, PI et mode : enjeux de la blockchain au regard des règles relatives à la preuve électronique », *Dalloz 2019*, p. 91.
[90] Dominique MOUGENOT, *« Droit des obligations – La preuve »*, Larcier, 2002.
[91] C. civ., art. 1383.
[92] *Ibid.*
[93] *Ibid.*
[94] Frédérique FERRAND, « Preuve », *Répertoire de procédure civile – Dalloz*, 2013 (actualisation 2022).
[95] C. civ., art. 1362.

sous pseudonymes, ils ne sont a priori pas identifiables »[96]. Or, une des conditions à remplir afin qu'un écrit se suffise à lui-même est l'identification de la personne dont émane cet écrit[97]. Ainsi, cet écrit devra être complété par une autre preuve dont l'appréciation de la valeur probante sera laissée à l'appréciation du juge[98].

De plus, à la lecture de cet article, il apparaît que deux conditions sont nécessaires pour qu'un commencement de preuve par écrit soit valable : *« i. une condition de forme : l'écrit, dont la spécificité doit être de provenir de celui à qui on veut l'opposer ou de son mandant ou représenté […]. ii. une condition qualitative : l'écrit doit rendre vraisemblable le fait allégué »*[99].

26. **La valeur juridique d'un écrit en tant que preuve**. Afin qu'un écrit, notamment numérique puisse être utilisé en tant que preuve, certaines conditions sont à respecter, tant à un moment précis (titre 1) c'est-à-dire au moment de sa création ou de sa transformation, qu'à long terme (titre 2), soit tout au long de son cycle de vie, sous peine de voir sa valeur diminuée pour n'être plus qu'un commencement de preuve par écrit.

[96] Isabelle GAVANON, « Blockchain, PI et mode : enjeux de la blockchain au regard des règles relatives à la preuve électronique », *op. cit*.
[97] C. civ., art 1366.
[98] Cass. Civ 1ère, 12 juillet 1972, 71-12.249, Publié au Bulletin.
[99] Frédérique FERRAND, « Preuve », *op. cit.*

TITRE 1 : La valeur juridique d'un écrit à un instant précis

27. **La valeur juridique d'un document : un double intérêt**. La valeur juridique d'un document ou d'un acte correspond aux conditions requises afin que ce document ou cet acte soit reconnu et puisse être utilisé en tant que preuve devant un tribunal en cas de contentieux. L'établissement de santé ne respectant pas ces conditions prend le risque de perdre les différents procès entraînant un impact financier important et une atteinte à sa réputation. Au-delà de l'intérêt probatoire, le respect de ces conditions permet à celui qui compte utiliser le document, d'avoir confiance en son contenu. En effet, si les conditions permettent de donner une valeur juridique au contenu du document, cela signifie qu'il est possible de l'utiliser sans remettre en doute son origine ou sa consistance. Cependant, cela ne signifie pas nécessairement que le contenu soit juste, mais seulement qu'il est conforme à ce que son auteur aura mis à l'intérieur. Cela est d'autant plus important dans le domaine de la santé. Dès lors qu'un médecin utilise un document pour prendre en charge le patient, il ne doit pas avoir de doute quant à la fiabilité de son contenu.

28. **Deux temporalités[100].** Pour que l'écrit sous format électronique puisse être utilisé comme preuve au même titre que l'écrit sur support papier, le Code civil prévoit plusieurs conditions à respecter :

i. La personne dont émane le document doit être identifiée,

ii. L'écrit doit être établi de manière à garantir son intégrité,

iii. Il doit être conservé de manière à garantir son intégrité[101]. On peut remarquer que ces conditions vont devoir être respectées sur deux temporalités : à un instant *t* et pendant tout sa durée de conservation (qui sera traité au sein du titre 2). Il en va de même pour la copie numérique. Il est prévu par le Code civil que « *la copie fiable a la même force probante que l'original »*[102]. La fiabilité est à prendre en compte tant au moment de sa reproduction en format numérique, que pendant sa durée de conservation.

---

[100] Albert Ndiack DIONE, *Les aspects juridiques de la dématérialisation des documents du commerce maritime,* Thèse dactylographiée, Paris, 2018. Dans cette thèse, l'intégrité des documents du commerce maritime est envisagée sur deux temporalités, d'une part au moment de la création du document et d'autre part, au moment de son archivage.
[101] C. civ., art. 1366.
[102] C. civ., art. 1379.

29. **L’instant *t* ou l’instant précis.** La valeur juridique à un instant *t* ou à un instant précis correspond au moment de la création d’un document dématérialisé qu’il soit créé nativement numérique, c’est-à-dire créé directement sous format numérique ou lors de sa transformation en format numérique, dès lors qu’il existait déjà en version papier.

30. **Les conditions à respecter.** Dès lors qu’un établissement de santé souhaite mettre en place un projet de dématérialisation, des conditions particulières devront être appliquées et respectées au moment de la création des documents natifs numériques (chapitre 1), ou au moment de la reproduction des documents papiers en format numérique (chapitre 2).

Chapitre 1 : L'écrit original électronique

31. **La définition de l'écrit**. *« L'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support »*[103]. Un écrit peut donc être constitué de lettres, peu importe la langue employée, de chiffres et de nombres tels qu'un bilan financier ou encore un schéma comportant des symboles explicites ou associés à une légende. La qualification d'écrit ne dépend pas du support sur lequel il se trouve, il apparaît qu'un format électronique tel qu'un document Word ou encore PDF puisse être envisageable. Cet écrit électronique peut être soit une copie, soit un original c'est-à-dire créé directement grâce aux technologies de l'information et de la communication.

32. **L'écrit contenant des données de santé**. Dans le cadre de la prise en charge d'un patient, de nombreux documents contenant des données de santé[104] sont produits. Les établissements de santé publics et privés, ont même l'obligation de créer un dossier médical pour tout patient hospitalisé[105]. Ce dossier comprend notamment « *les motifs d'hospitalisation ; […] le compte rendu opératoire ou d'accouchement ; […] la prescription*

---

[103] C. civ., art. 1365.

[104] Valérie OLECH, *Le secret médical et les technologies de l'information et de la communication*, *op. cit*. « *Pendant longtemps le législateur national n'avait pas prévu de définition des données de santé. Aussi la recherche du contenu de la notion conduisait-elle à se référer à d'autres sources. C'est finalement le RGPD qui pose une définition désormais comme à tous les Etats de l'Union européenne* ».
Sont des données de santé, « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui relèvent des informations sur l'état de santé de cette personne » :* Règl. (UE). PE et Cons. UE 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à liberté de circulation de ces données, art. 4 15ème. JOUE n° L 119, 4 mai 2016.
Cette définition fait écho à celle établie par la Cour de justice de l'Union européenne en 2003 : CJCE, 6 nov. 2003, aff. C*101/01, procédure pénale contre *Bodil Lindqist*.
Pour mieux appréhender cette définition, il est nécessaire de la lire au regard du considérant 35 du RGPD : « *Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro* ».

[105] C. santé publ., art. R. 1112-2.

de sortie et les doubles d'ordonnance de sortie »[106] qui sont des écrits au sens du Code civil. Ce dossier patient dans les établissements de santé, notamment les centres hospitaliers est de plus en plus informatisé. Ainsi, les documents qu'il contient sont des écrits électroniques.

33. **La force probante de l'écrit natif électronique**. Depuis l'année 2000, le Droit français a reconnu la valeur probante de l'écrit produit sous forme électronique en affirmant qu'il était « *admis en preuve au même titre que l'écrit sur support papier »*[107]. Cette position a notamment été réaffirmée au niveau européen en 2014 au sein du Règlement eIDAS : « *L'effet juridique et la recevabilité d'un document électronique comme preuve en justice ne peuvent être refusés au seul motif que ce document se présente sous une forme électronique »*[108]. L'Ordonnance du 10 février 2016[109] portant notamment réforme sur la preuve des obligations, vient donner davantage de valeur à l'écrit électronique en reconnaissant explicitement la même force probante à l'écrit qu'il soit créé sous format papier ou sous format électronique[110]. La force probante[111] est à ne pas confondre avec la valeur probante. « *C'est la foi due à cet acte en tant qu'il est retenu comme preuve par la loi* »[112] alors que « *la valeur probante d'une preuve est son aptitude à emporter la conviction du juge. C'est son caractère convainquant, la crédibilité, la confiance, le crédit que le juge peut lui accorder en conscience »*[113]. Ainsi, la loi confère à l'écrit électronique la même valeur qu'à l'écrit papier. Le juge n'aura pas la possibilité d'accorder moins d'importance à cet écrit, sous prétexte qu'il est au format électronique sauf dans le cas où une des conditions imposées par le code civil n'est pas respectée.

34. **Les conditions à respecter**. Pour que l'écrit électronique ait la même force probante que l'écrit sur support papier, le Code civil prévoit des conditions à respecter. Ces conditions doivent être tout d'abord définies (section 1) afin de pouvoir les mettre en œuvre

---

[106] *Ibid.*
[107] Ancien article 1316-1 du Code civil abrogé par l'ordonnance n°216-131 du 10 février 2016.
[108] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 46.
[109] Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035, 11 février 2016, texte n°26.
[110] C. civ., art. 1366.
[111] Gwendoline LARDEUX, « Preuve : modes de preuves », *op. cit.* La *« force probante est prédéterminée par la loi qui prévoit qu'à condition qu'un certain nombre de règles de forme soient respectées, elles s'imposent au juge qui ne peut donc pas souverainement apprécier leur crédibilité. En d'autres termes, si les conditions légales sont respectées, et parce que celles-ci sont censées assurer une grande fiabilité au mode de preuve présenté, le juge doit admettre que la preuve du fait allégué est rapportée sur le seul fondement de ce mode de preuve et ce, quelle que soit son intime conviction ».*
[112] Dominique MOUGENOT, Droit des obligations – La preuve, op. cit.
[113] *Ibid.*

(section 2) permettant de garantir à l'écrit électronique, une valeur juridique équivalente à celle de l'écrit papier.

Section 1 : La valeur probante d'un écrit numérique

35. ***Specialia generalibus derogant*[114].** Le Code civil reconnaît la même force probante à l'écrit papier ou électronique, cependant, se pose la question de l'application de ces dispositions. En effet, le principe en Droit français est que les lois spéciales dérogent aux lois générales, cela signifie qu'en cas de contradiction entre deux cadres juridiques, le cadre spécifique l'emportera. Comme la dématérialisation des supports envisagés contient des données de santé, le droit applicable en priorité est celui du Code de la santé publique par rapport au Code civil. Le Code de la santé publique prévoit notamment qu' « *un document mentionné à l'article L. 1111-25*[115] *du présent code créé sous forme numérique a la même force probante qu'un document sur support papier lorsqu'il a été établi et conservé dans les conditions prévues à l'article 1366 du code civil* ».[116] En espèce, le présent article prévoit, à l'instar du Code civil, la même force probante entre l'écrit sur support papier et sur support électronique ainsi que l'obligation d'être établi et conservé dans les mêmes conditions que celles prévues par le Code civil. Si l'on s'attarde sur l'article 1366, on peut ressortir deux conditions de validité de l'écrit électronique : d'une part l'identification de la personne et d'autre part l'obligation de respecter l'intégrité du document à sa création et pendant toute sa durée de conservation. Au regard de la rédaction des deux articles, il semblerait que l'article L. 1111-27 ait prévu l'application de la condition d'intégrité du document, mais que la condition concernant l'« *identification de la personne dont émane le document* »[117] ne soit pas envisagée. En effet, l'utilisation des mots « établi et conservé » dans l'article L. 1111-27 du code de la santé publique font échos aux mêmes mots utilisés dans l'article 1366 du Code civil qui ne sont applicables qu'à la notion d'intégrité du document.

---

[114] François DE FONTETTE, *Vocabulaire juridique*, Que sais-je coll., Presses Universitaires de France, 1994. *« Les lois spéciales dérogent aux lois générales. » Un texte qui vise un cas particulier doit être considéré comme une dérogation à une règle générale ».*

[115] C. santé. publ., art L. 1111-25. « *La présente section s'applique aux documents comportant des données de santé à caractère personnel produits, reçus ou conservés, à l'occasion d'activités de prévention, de diagnostic, de soins, de compensation du handicap, de prévention de perte d'autonomie, ou de suivi social et médico-social réalisées dans les conditions de l'article L. 1110-4, par :*
1° Un professionnel de santé, un établissement ou service de santé ;
2° Un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code ;
3° Le service de santé des armées ;
4° Un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ».

[116] C. santé publ., art. L. 1111-27.

[117] C. civ., art. 1366.

36. **Les objectifs de l'Ordonnance créant l'article L. 1111-27**. Le projet de loi ratifiant notamment l'ordonnance n°2017-29 du 12 janvier 2017[118], établit que celle-ci « *précise les conditions dans lesquelles les documents médicaux doivent être produits, signés et conservés pour avoir force probante* »[119]. La notion de signature renvoie inévitablement à la notion d'identification de la personne dont émane le document. Il apparaît donc que cette condition du Code civil soit également à prendre en compte pour les documents contenant des données de santé. De plus, le mot « établir » peut être interprété en son sens premier, c'est-à-dire les conditions à respecter dès le moment où le document est créé. Dans ce cas et au regard de l'article 1366 du Code civil, il faut bien prendre en compte d'une part l'identification de la personne et d'autre part l'intégrité du document à sa création. Cette position est confirmée à la lecture des documents préparatoires qui précisent qu'il « *est fait le choix de ne pas créer de règles spécifiques pour ces documents et d'appliquer expressément les seules dispositions du code civil relatives, d'une part, à la copie numérique et, d'autre part, à l'écrit électronique et la signature électronique* »[120], impliquant que toutes les dispositions du Code civil concernant la copie numérique, l'écrit électronique et la signature électronique sont applicables, notamment l'« *identification de la personne dont émane le document* »[121].

37. **Les conditions à respecter**. Afin qu'un document original électronique puisse avoir la même force probante qu'un écrit sur support papier, deux conditions sont à respecter : d'une part, la personne à l'initiative du document doit être identifiée (§1), d'autre part, le document doit être intègre tant au moment de sa création que pendant sa conservation (§2).

§1 L'identification de la personne dont émane le document

38. **La première condition**. La première condition à respecter pour qu'un écrit électronique puisse avoir la même valeur qu'un écrit papier, est que la personne dont émane le document doit être identifiée. On entend par cela la personne qui est à l'initiative du

[118] Projet de loi ratifiant les ordonnances n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel et n° 2017-29 du 12 janvier 2017 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique (AFSZ1703539L).
[119] *Ibid.*
[120] Rapport au Président de la République relatif à l'ordonnance n° 2017-29 du 12 janvier 2017 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique.
[121] C. civ., art 1366.

document, ce qui laisse à penser qu'il s'agit de son auteur, de la personne qui est à l'origine, celle qui le rédige. Cependant dans les faits, l'identité du rédacteur d'un document (A) peut être différent de celui qui est identifié comme étant son auteur ou qui en prend la responsabilité (B).

A) L'identification du rédacteur

39. **Le rédacteur.** Le terme « rédacteur » est défini de plusieurs manières : « *auteur de la rédaction d'un texte »*[122] ou encore *« personne qui rédige, qui a rédigé, qui est chargée de rédiger un texte, un document »*[123]. Ces définitions bien que semblables possèdent une différence importante. Pour l'une, il est précisé que le rédacteur est la personne à l'origine de la rédaction du texte, tandis que pour l'autre, le rédacteur est simplement la personne qui le rédige ; en d'autres termes, l'un est le cerveau, l'autre la plume. Aussi, pour la seconde définition, il est fait une distinction entre la personne qui rédige le texte (la plume), et la personne qui en est l'auteur (le cerveau). Cette dernière semble être la définition la plus complète et la plus juste permettant de prendre en compte les deux facettes du terme rédacteur et les conséquences qui en découlent.

40. **Le rédacteur différent de la personne identifiée comme auteur**[124]. Lors de la création d'un document, une ou plusieurs personnes peuvent construire et rédiger l'écrit. Ce sera le cas lorsqu'un écrivain va écrire son nouveau roman, ou bien lorsque plusieurs personnes vont collaborer pour produire et rédiger des guides explicatifs ou encore lors de la rédaction d'articles par plusieurs auteurs identifiés. Dans ce cas, les rédacteurs des textes en sont également les auteurs, ceux à l'origine du contenu, et seront identifiés comme tels sur le document. En revanche il arrive très fréquemment que le rédacteur d'un document n'est pas celui qui en est à l'origine ou qui en a produit le contenu.

41. **En santé : la fonction de secrétaire médicale**. Cela est d'autant plus vrai dans le domaine de la santé, notamment pour la secrétaire médicale. Une de ses fonctions est la réalisation ainsi que la mise en forme de documents, « *par exemple, elle devra saisir des courriers médicaux, des comptes-rendus de consultation et examens médicaux, ou encore des*

[122] Larousse, V° « rédacteur », nom.
[123] TLFi, V° « rédacteur », subst.
[124] Cass. crim., 1 avril 2020, n°19.80.375. Dans le cas d'espèce, les juges ont fait une distinction entre la fonction de rédacteur du document et d'auteur intellectuel, montrant bien la différence entre les deux fonctions. L'auteur est celui qui réalise un cheminement intellectuel contrairement au rédacteur.

certificats médicaux »[125]. La secrétaire médicale aura donc la charge de rédiger des documents contenant des données de santé à caractère personnel, en revanche le contenu de ces documents ne proviendra pas de la secrétaire médicale, mais sera produit et dicté par le médecin. Peut-on donc considérer qu'elle soit la véritable auteure ? Lorsque la secrétaire médicale réalisera une retranscription écrite d'un courrier au préalable enregistré sur dictaphone par un médecin par exemple, on ne peut pas considérer qu'elle en soit l'auteure, en revanche elle en est la rédactrice ou la transcriptrice. Cela signifie qu'elle a la charge de transcrire un contenu qu'elle n'aura pas produit.

42. **La responsabilité du rédacteur.** Dès lors que le rédacteur d'un document n'est pas son auteur mais plutôt un transcripteur, se pose la question de sa responsabilité quant au contenu qu'il rédige. Par principe, le rédacteur n'est pas responsable de la consistance du contenu qu'il rédige, c'est-à-dire la qualité et/ou la véracité du contenu, en revanche il est responsable de la retranscription en tant que telle. En effet, le rédacteur pourrait voir sa responsabilité engagée si la retranscription ne correspond pas à ce qui aurait pu être relaté ou encore dicté.

43. **La personne dont émane le document.** La question qui se pose est de savoir qui est véritablement visé derrière la condition « *identification de la personne dont émane le document* »[126] et notamment si la personne dont émane le document peut être le rédacteur d'un document qui n'est pas son auteur. L'objectif de l'article 1366 du Code civil est de déterminer les conditions à respecter afin qu'un écrit électronique puisse avoir la même force probante qu'un écrit papier et ainsi pouvoir produire des effets juridiques. Nous venons de démontrer que le rédacteur d'un document dont il n'a pas produit le contenu, ne peut voir sa responsabilité engagée concernant la teneur du contenu. Est-il donc pertinent d'identifier la personne dont il émane dès lors que le rédacteur n'en est pas l'auteur ? Cela pourrait-être le cas en utilisant le document produit comme un moyen de preuve sans pour autant être suffisant à lui seul. En effet, le document pourra relater des faits, ou des décisions prises, mais sans validation de son contenu par celui ou ceux qui en sont l'auteur, la portée du document est limitée, elle ne pourra venir qu'à l'appui d'autres preuves.

44. **La personne non-visée par l'article.** Il apparaît donc que le rédacteur d'un acte qui n'est pour autant pas son auteur n'est pas la personne visée par l'article 1366 du Code

[125] Amandine, « Quel est le rôle de la secrétaire médicale au sein d'un cabinet médical ? », *Le blog du Centre Européen de Formation*, mai 2018. (Consulté le 23 janvier 2021).
[126] C. civ., art 1366.

civil puisque l'identification de ce seul rédacteur ne permet d'avoir des effets juridiques que très limités.

B) L'identification de la personne qui en assume le contenu du document

45. **L'auteur du document**. L'auteur est défini comme « *celui ou celle qui est la cause première ou principale d'une chose* »[127] ou encore la « *personne qui est à l'origine de quelque chose de nouveau, qui en est le créateur, qui l'a conçu, réalisé ; initiateur, inventeur : l'auteur d'une découverte* »[128], il est donc la personne qui est à l'origine d'un contenu, c'est lui qui l'a créé. Cela signifie donc, à la suite de la démonstration réalisée ci-dessus, que c'est lui qui supporte les effets juridiques relatifs au contenu d'un document et qu'il est la personne à identifier pour remplir la condition prévue à l'article 1366 du Code civil. Cela est notamment le cas d'un compte-rendu médical, qu'il soit rédigé par la secrétaire médicale ou par le médecin. On considère que le médecin est à l'origine du contenu du compte-rendu, qu'il en est l'auteur et sera celui qui supportera les conséquences de son contenu, notamment en cas d'erreur. Cependant, l'auteur d'un document n'est pas toujours celui qui supportera les effets juridiques.

46. **L'auteur n'est pas toujours celui qui supporte les effets juridiques**. Le juriste au sein d'une entreprise est la personne chargée de rédiger des documents juridiques tels que des marchés publics, des contrats de travail, ou encore des règlements intérieurs. En tant que juriste, c'est lui qui possède la connaissance du droit et doit rédiger ces documents conformément à la règlementation en vigueur et doit veiller à y inclure toutes clauses permettant de protéger son entreprise. En revanche, bien que le juriste soit l'auteur du document produit ce n'est pas lui qui en porte les effets, mais la personne qui validera le document. Pour un contrat par exemple, celui qui valide son contenu par l'apposition de sa signature est la personne habilitée à engager l'entreprise, comme le directeur. Aussi, en cas d'erreur au sein du contrat, celui qui en assumera les effets vis-à-vis des autres parties ou des tiers, sera le signataire. En cas d'utilisation d'un contrat en tant que preuve, il faudra identifier son signataire afin de démontrer qu'il a bien validé le contenu du contrat, et son auteur qui est le juriste.

47. **Le parallèle avec les établissements de santé : le cas particulier de l'interne en médecine**. L'interne est un *« praticien en formation spécialisée, il consacre la totalité de*

[127] TLFi, *V° « auteur »*, subst. masc.
[128] Larousse, *V° « auteur », nom.*

son temps à sa formation médicale, odontologique ou pharmaceutique en stage et hors stage »[129] et *« exerce des fonctions de prévention, de diagnostic et de soins, par délégation et sous la responsabilité du praticien dont il relève »*[130]. Ainsi grâce à une délégation, l'interne en médecine pourra rédiger et signer des documents tels que des ordonnances ou prescrire des traitements. Cependant, l'interne en médecine ne pourra pas avoir de délégation pour tous les types de documents ; l'interne n'a pas, par exemple, la possibilité de signer des certificats et documents dont la production est prescrite par les textes législatifs et réglementaires[131] et qui peuvent comporter des effets juridiques. Jusqu'en juillet 2019[132], un interne n'avait pas l'autorisation de signer les certificats de décès. Cette position avait été appuyée par une réponse délivrée en 2000 par le Ministère de la santé : *« S'agissant de la rédaction des certificats médicaux, certains d'entre eux, compte tenu de l'importance ou la gravité de leurs effets, ne peuvent faire l'objet d'une délégation de signature. Il s'agit des certificats de décès, des certificats d'hospitalisation sous contrainte et des certificats d'expertise au sens de l'article 89 du code de déontologie des médecins »*[133]. Cependant, au sein d'un hôpital, la rédaction du certificat de décès était très régulièrement réalisée par l'interne, en revanche la signature de celui-ci est réalisée par son médecin responsable. C'était donc ce dernier qui validait le contenu de l'acte créé par l'interne en apposant sa signature. En cas de contestation ou d'erreur, c'était le médecin responsable qui était responsable de l'acte fait et de son contenu. Depuis 2019, l'article L. 2223-42 du Code général des collectivités territoriales a été modifié permettant aux étudiants[134] « *en cours de troisième cycle des études de médecine en France* »[135] d'établir un certificat de décès « *par délégation et sous la responsabilité du praticien maître de stage ou responsable de stage dont ils relèvent* »[136]. Cette autorisation donnée notamment aux étudiants, permet de pallier le *« manque de médecins pour établir des*

[129] C. santé publ., art R. 6153-2.
[130] C. santé publ., art R. 6153-3.
[131] C. santé publ., art. R. 4127-76.
[132] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1), JORF n°0172, 26 juillet 2019, texte n°3.
[133] Question écrite n°23923 de M. Dominique LECLERC sur la capacité des internes faisant fonction d'internes ou résidents dans les services hospitaliers à signer des certificats, publiée dans le JO Sénat du 30/03/2000, p-1123. Réponse du ministère de la Santé, publiée dans le JO Sénat du 05/10/2000, p-3405.
[134] Les étudiants de troisième cycle ne sont pas les seuls à pouvoir réaliser des certificats de décès. Depuis décret n°2020-446 du 18 avril 2020 (JORF n°0096, 19 avril 2020, texte n°2), les médecins retraités sans activité ainsi que les praticiens à diplôme étranger hors de l'UE, sont également autorisés à établir un certificat de décès.
[135] C. gén. coll. ter., art. L. 2223-42.
[136] C. gén. coll. ter., art. D. 2213-1-1-2. *« Les étudiants de troisième cycle des études de médecine ayant validé deux semestres au titre de la spécialité qu'ils poursuivent sont autorisés à établir des certificats de décès dans le cadre de leurs stages de troisième cycle, par délégation et sous la responsabilité du praticien maître de stage ou responsable de stage dont ils relèvent ».*

certificats de décès »[137] surtout dans les zones rurales, alors même que *« la présence d'un praticien* [est] *indispensable pour s'assurer des causes naturelles de la mort »*[138]. Ce décret est une des solutions trouvées pour faire face à la désertification médicale.

48. **La personne visée par l'article 1366 du Code civil.** La notion de *« personne dont il émane »* est imprécise et peut porter à confusion dans son application. Il a été démontré que la personne à prendre en compte n'est pas toujours le rédacteur, pour autant c'est bien la personne dont émane le document. Ce n'est pas non plus systématiquement l'auteur du document, puisque certains documents sont effectivement produits par une personne, mais ne sera pas celle qui en assumera les effets juridiques. *« Il aurait été préférable de considérer que doit être identifiée la personne qui est l'auteur de la volonté qu'il relate »*[139]. Il apparaît donc que la condition « *identification de la personne dont émane le document* »[140] au regard de l'objectif attendu de cet article, soit plutôt l'identité de la personne qui prend à sa charge la responsabilité du contenu[141].

§2 L'intégrité du document à sa création : une condition primordiale

49. **La seconde condition.** Afin de reconnaître la même force probante à l'écrit électronique qu'à l'écrit papier, le Code civil, en plus de l'identification de la personne dont émane le document, exige que le document soit « *établi et conservé dans des conditions de nature à en garantir l'intégrité »*[142]. A la lecture de cet article, on peut constater que l'intégrité est envisagée sur deux temporalités différentes : à la création du document électronique et pendant sa conservation.

50. **Une distinction essentielle ?** Cependant y a-t-il une réelle pertinence à envisager de scinder l'intégrité à la création du document, et l'intégrité pendant sa conservation afin d'en faire deux conditions distinctes ? Cette distinction de temporalité n'est pas prise en compte par la doctrine en estimant que l'article 1366 du Code civil « *pose deux conditions de validité de l'écrit électronique […]. D'abord, l'auteur de cet écrit doit être identifié. Ensuite, il doit être établi et conservé dans des conditions de nature à en garantir*

[137] Question écrite n°26533 de M. Olivier PACCAUD sur le manque de médecins pour établir des certificats de décès, publiée dans le JO Sénat du 03/02/2022, p-542. Réponse du ministère des solidarités et de la santé, publiée dans le JO Sénat du 28/04/2022, p-2397.
[138] *Ibid.*
[139] Marc MIGNOT, « Commentaire article par article de l'ordonnance du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations (XIII) », *actu-juridique*, mai 2016. (Consulté le 2 janvier 2021). Disponible à l'adresse : https://www.actu-juridique.fr/
[140] C. civ., art 1366.
[141] Alexandre RODRIGUES, « La valeur probante de l'écrit numérique », *avocats Picovschi*, 2014.
[142] C. civ., art 1366.

l'intégrité »[143] ou que « *la preuve littérale sous forme électronique est admise à une double condition : l'identification de l'auteur à qui l'acte est imputé et la garantie de son intégrité dans le temps »*[144]. Cela reviendrait à envisager que l'intégrité au moment de la création du document et celle pendant toute sa conservation, c'est-à-dire pendant tout son cycle de vie seraient complètement liées et qu'elles sont à envisager toujours en binôme impliquant que la réalisation de cette condition dans les deux temporalités soit réalisée de la même manière et que l'une n'ait pas d'influence sur l'autre.

51. **L'appropriation de la notion.** Afin de déterminer s'il est pertinent d'appréhender l'intégrité sur les deux temporalités et ainsi pouvoir déterminer les moyens à mettre en œuvre pour respecter cette condition, il est nécessaire de déterminer le périmètre de la notion (A) et de la définir par rapport à l'écrit électronique (B).

A) Les contours de l'intégrité

52. **La définition générale de l'intégrité.** Dans tous les domaines, l'intégrité est définie comme l' « *état d'une chose, d'un tout, qui est entier, qui a toutes ses parties* »[145] ou encore « *l'intégrité d'un objet est le fait qu'il n'ait subi aucune altération, qu'elle soit accidentelle ou intentionnelle* »[146]. Le point commun de ces deux définitions, et ce qui caractérise le mieux la notion d'intégrité est la non-altération de quelque chose, que ce soit un document, un objet, ou encore une donnée. La non-altération implique que ce « quelque chose », objet de l'intégrité, n'ait subi aucune modification quant à son état et sa qualité. La définition même de l'intégrité ne pose pas de difficulté dans son sens général, qui est assez claire, et approuvée par tous. C'est une notion large pouvant convenir dans tous les domaines et à tous les supports. Cependant, cette définition est tellement générale, qu'il est très difficile de l'appréhender par rapport à l'écrit numérique et notamment d'en déterminer l'objet.

53. **L'objet de l'intégrité.** L'intégrité est caractérisée par la non-altération de quelque chose, qui n'est pas défini et qui peut prendre plusieurs formes. Cette absence permet de déterminer pour chaque domaine, quel sujet doit faire l'objet de l'intégrité. Cependant,

---

[143] Marc MIGNOT, « Commentaire article par article de l'ordonnance du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations (XIII) », *op. cit.*
[144] Jean-Luc SABOURIN, « L'établissement, la transmission et la conservation des informations juridiques », *UNJF*. (Consulté le 14/05/2021).
[145] TLFi, *V° « intégrité »*, subst. fém.
[146] Françoise BANAT-BERGER, Anne CANTEAUT, « Intégrité, signature et processus d'archivage », *INRIA*, p-1.

l'article 1366 du Code civil, ne le précise pas. L'intégrité se rapporte-t-elle au support de l'écrit, à son contenu ou aux deux ?

L'objectif d'avoir un écrit est de pouvoir prendre connaissance du contenu et de pouvoir l'utiliser. Cette utilisation peut avoir plusieurs finalités, prenons l'exemple de l'ordonnance pour la prescription de médicaments établie par un médecin. Cette ordonnance a deux finalités principales outre la prise en charge du patient : la première est de permettre au pharmacien, grâce au contenu de l'ordonnance (posologie, durée du traitement[147] etc.), de fournir les médicaments prescrits par le médecin, au patient[148]. La seconde est la prise en charge des frais[149] liés aux médicaments par l'Assurance maladie, à la suite de la transmission par le pharmacien de l'ordonnance[150]. Une troisième finalité de l'ordonnance, mais qui ne sera pas toujours utilisée est de s'en servir comme moyen de preuve. En effet, en cas d'erreur de médicaments, ou de posologie, il sera nécessaire de déterminer le responsable. Le contenu de l'ordonnance permettra de déterminer si l'erreur provient du médecin ou du pharmacien. Il apparaît que la non-altération du contenu d'un écrit est primordiale, notamment en tant que preuve ; son intégrité est donc particulièrement attendue.

L'intégrité du support de l'écrit, est-elle tout autant attendue ? Prenons toujours l'exemple de l'ordonnance pour la prescription de médicaments et intéressons-nous à son support. Dans une grande majorité des cas, l'ordonnance rédigée par un médecin sera réalisée de manière informatique. Elle sera ensuite imprimée puis, signée de manière manuscrite par le médecin qui la confie au patient. Le patient donnera cette ordonnance au pharmacien, qui la transmettra par voie dématérialisée à l'Assurance Maladie. L'ordonnance aura donc bénéficié de plusieurs supports : tout d'abord du format numérique, puis du format papier, pour être à nouveau dématérialisée. Ces changements n'entraînent pas nécessairement une perte de valeur du document, puisque le Code civil prévoit que *« la copie fiable a la même force probante que l'original »*[151], y compris en cas de copie numérique d'un document papier et vice versa. Pour autant le support aura été modifié.

---

[147] C. santé publ., art R. 5123-1.

[148] Vidal, « Prescription et délivrance des médicaments : l'intervention du pharmacien d'officine sur les prescriptions », *Infos pratiques,* 2021. Disponible à l'adresse : https://www.vidal.fr/ (consulté le 21/09/2022).

[149] Pierre-Jean LANCRY, « Le médicament - Médicament et régulation en France », *Revue Française des Affaires Sociales,* 2007/3-4, pp. 25-51. On peut notamment constater que *« les médicaments remboursables représentent l'essentiel du marché des médicaments ».*

[150] Ameli, « Remboursement des médicaments et tiers payant », *Assurance maladie,* 2021. Disponible à l'adresse : https://www.ameli.fr/ (consulté le 13/09/2022).

[151] C. civ., art 1379 al. 1.

54. **Le support : un enjeu pour le maintien de l'intégrité.** Ce n'est donc pas tant l'intégrité du support de l'écrit qui est attendue, mais bien l'intégrité de son contenu. Pour autant, le support doit tout de même être pris en compte car c'est un des moyens utilisés pour le maintien de l'intégrité du contenu de l'écrit. A titre d'exemple, pour que le contenu d'un document électronique ne soit pas altéré, il est nécessaire qu'il ne puisse pas être modifié. Pour cela, le support utilisé, notamment le format d'enregistrement du document ne doit pas permettre de modifications du contenu. Il apparaît déjà clairement que le choix du support au moment de la création d'un document et de son enregistrement aura un impact sur l'intégrité de son contenu.

55. **L'altération accidentelle ou volontaire.** Les différentes définitions de l'intégrité sont presque toutes identiques quant à leur contenu. Cependant la définition introduite par Françoise Banat-Berger et Anne Canteaut vient préciser que l'intégrité est une non-altération, « *qu'elle soit accidentelle ou intentionnelle* »[152]. Cette précision vient appuyer le fait que l'intégrité d'un document est garantie par l'absence totale de modification de son contenu peu importe l'origine éventuelle de la modification, y compris par son auteur. Par définition, toute modification, qu'elle soit volontaire ou accidentelle, est une altération du contenu d'un document, lui faisant perdre son intégrité.

56. **En conclusion.** L'intégrité d'un écrit doit s'entendre comme la non-altération du contenu de l'écrit, que cette altération ait été volontaire ou involontaire. Pour garantir l'intégrité du contenu, le support utilisé joue un rôle majeur qui n'est pas à négliger.

B) Une définition plus fine

57. **La nécessité d'une définition plus fine.** La définition générale de l'intégrité ne suffit pas à elle seule, à déterminer ce que l'on entend et ce que l'on attend de l'intégrité d'un écrit électronique. La définition du périmètre de la notion a permis de mettre en avant ce qui doit faire l'objet de l'intégrité mais ne suffit pas encore à déterminer concrètement, ce qu'implique l'intégrité du contenu d'un écrit électronique. Le Code civil ne nous donne pas davantage d'éléments contrairement à la législation étrangère (1). Pour autant le Droit français ainsi que la doctrine, sont venus affiner la définition de l'intégrité (2).

[152] Françoise BANAT-BERGER, Anne CANTEAUT, « Intégrité, signature et processus d'archivage », *op. cit.* p-1.

1) La définition de l'intégrité au Québec introduite dans le Code civil du Québec

58. **Les similitudes de la reconnaissance de la valeur juridique d'un document électronique**. A l'instar de la France et dans la même temporalité, le Québec a promulgué une Loi « *concernant le cadre juridique des technologies de l'information »*[153] traitant notamment de la preuve par écrit électronique. A la lecture de cette Loi, on peut noter des similitudes entre droit québécois et droit français[154], notamment la même volonté de reconnaître une valeur équivalente à l'écrit papier qu'à l'écrit électronique[155]. En effet, la Loi dispose que « *le document dont l'intégrité est assurée a la même valeur juridique, qu'il soit sur support papier ou sur un autre support, dans la mesure où, s'il s'agit d'un document technologique, il respecte par ailleurs les mêmes règles de droit »*[156]. Bien que la rédaction de l'article soit différente de celle de la France, la philosophie est la même. Le Québec prévoit, comme la France, l'exigence d'intégrité afin qu'un document électronique puisse avoir une valeur juridique.

59. **Une définition de la notion d'intégrité**. Contrairement au droit Français, la Loi[157] québécoise va plus loin en précisant comment garantir l'intégrité d'un document : *« l'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue »*[158]. Afin qu'un document soit intègre, il faut donc :

i. que l'information contenue dans le document ne soit pas modifiée et qu'elle soit complète. Cela signifie notamment que le contenu du document ne doit pas être altéré.

ii. le support sur lequel se trouve l'information doit garantir sa stabilité et sa pérennité *« (c.-à-d. que l'information n'est pas volatile ou susceptible de disparaître ou d'être modifiée sans que l'on puisse s'en apercevoir) »*[159]. A la lecture de cet article, on s'aperçoit que l'intégrité se

[153] Loi concernant le cadre juridique des technologies de l'information entrée en vigueur le 1er novembre 2001 (Québec).
[154] Le Droit et la doctrine française ont depuis longtemps influencé le Droit québécois expliquant notamment les similitudes entre les deux Droits. Il est légitime de s'appuyer du Droit québécois pour en la matière. (Pierre-Gabriel JOBIN, « L'influence de la doctrine française sur le droit civil québécois : Le rapprochement et l'éloignement de deux continents », *Revue internationale de droit comparé*, 1992, pp. 381-408).
[155] Loi concernant le cadre juridique des technologies de l'information (Québec), art. 5.
[156] *Ibid.*
[157] Loi concernant le cadre juridique des technologies de l'information entrée en vigueur le 1er novembre 2001 (Québec).
[158] Loi concernant le cadre juridique des technologies de l'information (Québec), art. 6.
[159] Secrétariat du Conseil du trésor Québec, Loi concernant le cadre juridique des technologies de l'information entrée en vigueur le 1er novembre 2001, Loi annotée par article, article 6.

rapporte donc au contenu même du document qui ne doit pas être altéré mais cette non-altération est notamment garantie par le support. Aussi, *« dans l'intégrité du document, […] une relation symbiotique semble de mise entre les deux composantes qui le constituent »*[160], l'information et le support.

60. **L'application de cette définition à la France**. Au regard des similitudes entre la volonté pour le Québec et la France d'accorder la même valeur au document papier qu'au document électronique, et la condition d'intégrité à respecter pour y parvenir, on peut légitimement penser que la définition d'intégrité définie par la Loi québécoise peut s'appliquer également au Droit français.

2) La définition de l'intégrité introduite par le Droit et la doctrine en France

61. **Les premiers éléments en France.** A la suite de la Loi du 13 mars 2000[161], deux décrets du 10 août 2005[162] ont été publiés au journal officiel permettant aux huissiers de justice et aux notaires, d'établir des actes sur support électronique selon certaines conditions. Ces décrets viennent notamment donner davantage d'éléments permettant de garantir l'intégrité des actes : « *l'acte établi sur support électronique doit être conservé dans des conditions de nature à en préserver l'intégrité et la lisibilité. L'ensemble des informations concernant l'acte dès son établissement, telles que les données permettant de l'identifier, de déterminer ses propriétés et d'en assurer la traçabilité, doit être également conservé »*[163]. Deux critères ont été identifiés afin de permettre de garantir l'intégrité d'un écrit à long terme, la lisibilité et la traçabilité.

62. **Les sous-critères définis par le Forum des Droits sur l'Internet[164] (FDI)**. Le FDI en 2005, s'est penché sur la notion d'intégrité des écrits électroniques car *« aucun texte*

[160] Loi concernant le cadre juridique des technologies de l'information (LCCJTI), définition de l'intégrité. Disponible à l'adresse : https://www.lccjti.ca/definitions/integrite/

[161] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62, 14 mars 2000, texte n°1.

[162] Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JORF n°186, 11 août 2005, texte n°34 et Décret n° 2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, JORF n°186, 11 août 2005, texte n°33.

[163] Décret n°56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, art. 29 et Décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JORF, 3 décembre 1971, art. 28.

[164] Le forum des droits sur l'internet était un organisme créé en 2001 par les pouvoirs publics, au regard du développement croissant de l'internet. Sa mission principale était de se pencher sur les questions de droit que l'internet entraînait. A ce titre le FDI a formulé de nombreuses recommandations, y compris juridiques, en concertation avec les différents intéressés : les pouvoirs publics, les entreprises, et les utilisateurs finaux. Le but était d'avoir une réflexion commune permettant d'établir des usages à respecter. Le FDI s'est notamment penché, en 2005 sur la question de la conservation électronique des documents et notamment sur la notion

ne précise les critères permettant de juger de cette intégrité […] [et] *il est apparu nécessaire de choisir des critères issus de la pratique des professionnels de l'archivage et pris en considération par les juristes* »[165]. Pour cela le FDI a notamment repris les deux critères énoncés par les deux décrets de 2005, la lisibilité et la traçabilité et en a ajouté un troisième, la stabilité. Le respect de ces trois critères cumulatifs permet de garantir l'intégrité d'un écrit pendant sa conservation.

63. **La stabilité de l'information**. La stabilité « *désigne la nécessite de pouvoir garantir que les informations véhiculées par le document restent les mêmes depuis l'origine, et qu'aucune n'est mise ou rajoutée au cours du processus de conservation* »[166]. La condition de stabilité fait écho à la définition de l'intégrité. Comme cela a été vu ci-dessus, l'intégrité s'entend comme la non-altération du contenu du document, ce que la stabilité du contenu informationnel implique. « *Le contenu informationnel s'entend de l'ensemble des informations, quelle que soit leur nature ou leur origine, issues du document et le cas échéant, de sa mise en forme* »[167]. Le contenu du document est plus large que la simple information écrite contenue dans le document. La mise en forme de ce dernier, comme les entêtes, les couleurs, ou encore le format de la police utilisé doit également être identique dans le temps par rapport au document d'origine. Lors du choix du support utilisé pour la création d'un document électronique, il est impératif d'en choisir un dont le contenu ne sera pas susceptible d'être modifié, afin de garantir la stabilité de l'information et donc l'intégrité du document.

64. **La lisibilité de l'écrit**. La lisibilité « *désigne la possibilité d'avoir accès, au moment de la restitution du document, à l'ensemble des informations qu'il comporte* »[168]. C'est la première condition apportée par les décrets de 2005 : le contenu de l'écrit doit pouvoir être restitué afin que ce dernier puisse être utilisé, notamment en tant que preuve. Au regard de l'évolution constante des technologies de l'information et de la communication, on s'aperçoit que la restitution d'un document informatique n'est pas chose aussi aisée que celle d'un document papier[169]. En effet, *« l'affichage d'une information numérique est le résultat*

---

d'intégrité. Des critères permettant de garantir l'intégrité d'un écrit ont été posés. Le FDI a finalement été dissout en décembre 2010.

[165] Isabelle FALQUE-PIERROTIN, « Forum des droits sur l'internet : rapport d'activité – année 2005 », *Forum des Droits sur l'Internet,* décembre 2005, pp-203-204.

[166] Isabelle FALQUE-PIERROTIN, « Forum des droits sur l'internet : rapport d'activité – année 2005 », *op. cit.*, p-204.

[167] *Ibid.*

[168] *Ibid.*

[169] François BANAT-BERGER, « De l'écrit à internet : comment archive-t-on l'immatériel ? », *Pouvoirs,* 2015/2, n°153, pp. 109-124.

d'une suite complexe de traitement intervenant dans différentes couches de l'ordinateur (couches physiques, de structure, sémantiques…). C'est par le biais d'une superposition de matériels, de logiciels, de systèmes d'exploitation, de périphériques, que à un moment donné, pourra être affiché de par leur interaction harmonieuse, un écrit. Or, ces différents composants évoluent à des rythmes différents […]. Par conséquent, conserver une information numérique et permettre sa représentation dans un laps de temps X c'est conserver la capacité à la représenter dans l'environnement matériel et logiciel qui sera alors utilisé. […] Il convient par conséquent de rendre l'information à conserver la plus indépendante possible de son environnement technologique »[170]. Le choix du format du document utilisé aura un impact sur sa lisibilité et donc son intégrité. Choisir un format fermé dont la lisibilité dépendra d'un certain type de composants techniques ne permet pas de lire le document simplement, et risque au fil du temps, de le rendre illisible et donc d'en perdre l'intégrité. Dès la création du document, le choix du support utilisé est donc primordial.

On s'aperçoit également que la lisibilité n'est pas simplement la possibilité de lire un document, mais également de « *pouvoir interpréter ce que l'on vient de lire »*[171]. L'interprétation du document *« est facilitée par les métadonnées associées au document »*[172]. Les métadonnées jouent un rôle essentiel sur la restitution des informations, elles servent « *à caractériser une autre donnée, physique ou numérique »*[173]. Il arrive qu'un document seul ne permette pas d'apprécier la teneur de l'information contenue dans celui-ci, sans éléments de descriptions ou encore de contexte. En effet, un document dont le contenu peut être lu, ne signifie pas pour autant que celui-ci est compréhensible. Les métadonnées servent notamment[174] à rendre le contenu d'un document intelligible par tous.

Prenons l'exemple d'un document au format Excel contenant un tableau. Dans ce tableau, se trouve une suite de données brutes, pour lesquelles, aucun élément ne permet d'en déterminer la signification :

---

[170] Françoise BANAT-BERGER, Anne CANTEAUT, « Intégrité, signature et processus d'archivage », *op. cit.* p-9.

[171] Jean-Louis PASCON, Nathalie MORAND-KHALIFA et Jean-Marc RIETSCH, *Mise en œuvre de la dématérialisation – De l'étude préalable à la certification du système*, Dunod, 2010.

[172] Isabelle FALQUE-PIERROTIN, « Forum des droits sur l'internet : rapport d'activité – année 2005 », *op. cit.*, p-204.

[173] Larousse, *V° « métadonnée », nom. fém.*

[174] Les métadonnées ne servent pas seulement à rendre intelligible un document ; elles servent aussi à le caractériser ou encore à donner davantage d'informations nécessaires à la réalisation d'une tâche. Par exemple, les métadonnées peuvent permettre de renforcer la valeur probante d'un document en associant des données de traçabilité. Ou encore, elles permettent de donner des informations supplémentaires à un document ; dans le cadre d'une lettre à envoyer, les données principales sont les mots contenus dans la lettre. Les métadonnées sont l'adresse postale et le nom du destinataire se trouvant sur l'enveloppe, informations nécessaires pour envoyer la lettre.

	A	B	C	D
1	SCHMITT	1	89	O
2	PETIT	2	97	N
3	LEMARCHAND	1	56	N
4	DUPOND	1	76	O

En l'espèce, le contenu est bien accessible puisque que l'on peut visualiser les données, pour autant elles ne sont pas intelligibles, car nous ne savons pas à quoi elles correspondent. En revanche, un autre document associé à ce tableau expliquant à quoi correspondent ces données, permet de les rendre intelligibles :

Chaque ligne du tableau correspond à un patient.

Chaque colonne du tableau correspond aux données suivantes :

- En colonne A : le nom d'usage
- En colonne B : le sexe (1 pour un homme, 2 pour une femme)
- En colonne C : l'année de naissance
- En colonne D : l'allergie à un aliment (O pour oui et N pour non)

Aussi, afin qu'un document soit intègre, celui-ci doit donc tout d'abord être lisible, c'est-à-dire que son contenu doit pouvoir être accessible mais également intelligible.

65. **La traçabilité des opérations**. La traçabilité « *désigne la faculté de présenter et de vérifier l'ensemble des traitements opérés sur le document lors du processus de conservation* »[175]. Cette traçabilité permettra de laisser des marques sur le document[176], permettant de déterminer toutes les actions réalisées sur celui-ci, et de savoir si le document créé à un instant *t* et ouvert à un instant *t+1* possède bien le même contenu. A titre d'exemple, l'évolution constante des technologies de l'information et de la communication nécessite obligatoirement une migration des documents, permettant de garantir leur lisibilité. Cette migration ainsi que toutes les opérations effectuées sur les documents doivent impérativement être tracées afin de ne pas faire perdre l'intégrité d'un document.

66. **L'application de ces critères.** Ces trois critères permettent de définir ce qu'est l'intégrité et comment y parvenir. En effet, pour qu'un document soit intègre celui-ci ne doit pas être altéré et doit donc être stable dans son contenu. Pour garantir la stabilité du contenu informationnel du document, toutes les opérations réalisées sur celui-ci doivent être visibles. Pour finir, le document doit permettre l'intelligibilité et l'accès à l'information qu'il contient. Le respect de ces trois critères implique nécessairement leur prise en compte dès la création

[175] Isabelle FALQUE-PIERROTIN, « Forum des droits sur l'internet : rapport d'activité – année 2005 », *op. cit.*, p-204.
[176] Raphaël LARSEN, *Traçabilité et intégrité de l'information au sein de systèmes critiques : analyse et proposition de méthodes statistiques*, Thèse dactylographiée, Nantes, 2022.

du document en format numérique. En effet, un document créé, ne permettant pas le respect de ces critères signifie inévitablement que ce document ne sera pas intègre, ni à sa création, ni pendant sa conservation. Pour autant, l'inverse n'est pas vrai ; un document peut être intègre dès sa création, mais perdre son intégrité pendant sa durée de conservation. Aussi, il est nécessaire d'appréhender ces critères différemment au moment de la création du document, et pendant sa conservation.

67. **L'Echo avec le Québec.** Les critères avancés par le Droit français et la doctrine font écho à la définition de l'intégrité énoncée par le Québec. Pour rappel, *« l'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue »*[177]. Le critère de stabilité est expressément nommé, quant aux critères de traçabilité et lisibilité, ceux-ci sont induits dans la notion de pérennité.

68. **L'absence de définition de l'intégrité dans l'ordonnance de 2016.** On peut s'interroger sur les raisons pour lesquelles l'ordonnance de 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations n'est pas venue donner davantage d'éléments sur cette notion d'intégrité concernant l'écrit électronique. L'absence de définition précise implique une méconnaissance des modalités attendues permettant de garantir l'intégrité d'un document, mais cette absence donne également une plus grande latitude au juge afin que ce dernier puisse apprécier le respect de ce critère. De plus, le Code civil prévoit tout de même un cas dans lequel l'intégrité d'un document est garantie : dès lors qu'une signature électronique qualifiée est apposée sur celui-ci.

[177] Loi concernant le cadre juridique des technologies de l'information (Québec), art 6.

Section 2 : La mise en œuvre des conditions d'identification et d'intégrité

69. **La mise en œuvre des critères.** Tous les écrits ne possèdent pas la même valeur juridique. Tout d'abord, une différence apparaît selon que l'écrit soit sur support papier ou sur support électronique. Le Code civil prévoit une même force probante pour les deux supports, sous réserve que certaines conditions, pour l'écrit électronique, soient remplies. Cela signifie donc que, par principe, l'écrit papier est considéré comme fiable, contrairement à l'écrit électronique qui doit démontrer sa fiabilité en respectant les conditions énoncées par l'article 1366 du Code civil. La seconde différence concerne l'écrit même qui doit, pour un écrit électronique, identifier la personne dont il émane, et être créé et conservé dans des conditions permettant son intégrité. Les méthodes d'identification et de maintien de l'intégrité utilisées détermineront le niveau de fiabilité accordé à un écrit ainsi que sa valeur juridique par rapport à un autre écrit.

70. **La signature permettant l'identification de l'auteur.** Le Code civil énonce très clairement un moyen permettant l'identification de la personne dont émane un écrit : « *la signature nécessaire à la perfection d'un acte juridique identifie son auteur* »[178]. Cet article va plus loin en précisant que cette signature est nécessaire pour les actes juridiques, impliquant implicitement que ce n'est pas le cas pour les faits juridiques. Tous les documents n'ont donc pas vocation à être signés.

Il en est de même pour les documents contenant des données de santé. Le Code de la santé publique définit les documents devant être signés. A titre d'exemple, il est prévu que « *tout certificat, ordonnance, attestation ou document délivré par un médecin doit être rédigé lisiblement en langue française et daté, permettre l'identification du praticien dont il émane et être signé par lui* »[179]. Pour autant, de très nombreux écrits vont être nécessaires pour la prise en charge d'un patient ou comme preuve lors d'un contentieux, mais ne seront pas signés.

71. **La signature n'est qu'un moyen**. Il apparaît donc qu'une distinction doit être réalisée entre les écrits signés (§1) et les écrits non-signés (§2) afin de déterminer les moyens nécessaires pour respecter les conditions énoncées par l'article 1366 du Code civil.

[178] C. civ., art 1366.
[179] C. santé publ., art R.4127-76.

§1 La signature électronique garantissant le respect des deux conditions

72. **La signature électronique : la signature de l'écrit numérique**. Avec le développement des technologies de l'information et de la communication, de plus en plus de documents sont créés nativement de manière électronique, nécessitant une adaptation de la signature. *« La signature manuscrite sur support papier était, jusqu'à récemment, le moyen reconnu par la loi pour assurer la « perfection de l'acte juridique ». Le développement de l'informatique et la dématérialisation des actes habituellement établis sous forme papier ont conduit le législateur à étendre les moyens d'authentification de l'auteur des actes juridiques à la signature électronique »*[180]. La signature manuscrite que l'on connaît traditionnellement et que l'on appose sur un document papier a trouvé son équivalent pour les documents natifs électroniques : la signature électronique.

73. **Les débuts de la signature électronique.** La signature électronique a été introduite en France par la loi du 13 mars 2000[181] ; elle n'a pas rencontré un franc succès à cette époque, jugée trop immature sur le procédé à utiliser. En effet, les écrits électroniques étaient considérés comme imparfaits car « *ils sont toujours manipulables, réversibles, des erreurs restent possibles, leur fiabilité dépend d'un système de sécurité non maîtrisé (cryptologie ou certification), ils sont soumis aux aléas techniques* »[182]. La loi a notamment été critiquée en l'apparentant à une loi-cadre ; l'appréciation de la valeur de l'écrit électronique et de la signature électronique dépendant en grande partie des moyens technologiques utilisés. Cela a été qualifié de saut vertigineux dans le vide[183]. Un an après sa promulgation, les réticences ont perduré, il a été jugé « *difficile de prévoir une utilisation de la signature électronique pour des contrats majeurs* »[184], montrant le manque de confiance en ce procédé.

---

[180] Olivier DUPUY, « La signature électronique et la communication des données de santé informatisées », *RDS,* 2006, n°9, pp. 60-62.

[181] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62, 14 mars 2000, texte n°1.

[182] Judith ROCHEFELD, « Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique », *RTDCiv.*, Dalloz, 2000, p-423.

[183] « *Au rebours de l'expérimentation et de la sécurité, et derrière le caractère courageux et irrévocable de son choix, se profile, en effet, le véritable traitement de l'incertitude retenu par le législateur : ce n'est pas au temps qu'il a demandé de valider son choix, mais à la technique. Le texte est, en effet, une loi-cadre qui, ignorant les difficultés, renvoie à une coopération. Coopération des textes tout d'abord : la loi du 13 mars 2000 pose un cadre général destiné à être complété par diverses autres mesures plus techniques assurant sa mise en œuvre* ». Judith ROCHEFELD, « Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique », *op. cit.*

[184] Thierry ABALLEA, « La signature électronique en France, état des lieux et perspectives », *Dalloz,* 2001, n°35, p-2835.

74. **La signature électronique indispensable**. Plus de vingt ans après, la signature électronique est finalement largement utilisée dans de nombreux domaines tels que les banques[185], la commande publique ou encore la santé. Les effets de cette signature sont multiples (A) et permettent notamment, en plus d'identifier de la personne dont émane le document, de garantir l'intégrité du document selon la signature choisie (B).

A) Les effets de la signature électronique

75. **La signature permettant l'identification de l'auteur d'un écrit[186].** L'utilité première d'une signature est d'identifier la personne qui l'appose sur un document. Cela est confirmé par la définition même de la signature : « *toute marque distinctive et personnelle manuscrite, permettant d'individualiser, sans doute possible, son auteur […]* »[187] ou encore « *l'inscription de son nom, sous une forme particulière et reconnue, ou d'une marque spécifique apposée par une personne sur un écrit afin d'en attester la responsabilité »*[188]. Elle est réalisée librement par la personne qui choisit le style que celle-ci arborera. L'identification de la personne par la signature est initiée dès le plus jeune âge, notamment dès que l'enfant commence à apprendre à écrire. Une des premières choses qu'un adulte lui apprend est l'écriture de son prénom. L'enfant écrira son prénom sur chaque dessin qu'il réalisera afin que toute personne puisse identifier qu'il est l'auteur de ce dessin. Au fil des années, cette signature se personnalisera en substituant le prénom par le nom ou nom/prénom, tout en le/les couplant avec un style graphique personnel. La signature d'une personne évolue tout au long de sa vie, par le changement de nom dû à un mariage ou encore par l'évolution du style d'écriture qui lui est personnel. Cette définition ne peut s'appliquer en l'état pour une signature électronique car cette dernière ne peut être « une marque distinctive et personnelle manuscrite ». Aussi, le dictionnaire définit la signature électronique comme étant une « *information codée permettant d'authentifier l'émetteur d'un message électronique »*[189]. Bien que l'utilisation du mot « message » soit très réducteur quant à la portée de l'utilisation de la signature électronique, on peut constater qu'autant pour la signature manuscrite que pour

[185] CA, Nancy 2e ch. civ., 10 mars 2022, n°21/0101223. Dans le cas d'espèce, le crédit renouvelable a été conclu de manière numérique avec la signature électronique du client. *« Rien, en l'état des pièces produites, ne permet de remettre en cause la fiabilité de ces opérations de signatures électroniques »,* aussi, le contrat de crédit a été valablement formé.
[186] Luc GRYNBAUM, « Preuve », *Répertoire de droit commercial »,* 2010 (actualisation en octobre 2020). En effet, *« la signature qui parachève un écrit permet donc l'identification des parties et constate leur adhésion au contenu de l'acte. C'est la fonction identifiante de la signature qui est ainsi consacrée ».*
[187] Larousse, *V° « signature »,* nom fém.
[188] TLFi, *V° « signature »,* subst. fém.
[189] Larousse, *V° « signature électronique ».*

la signature électronique, une notion est bien commune : elle permet d'identifier l'auteur du contenu et même de l'authentifier.

76. **Les effets de la signature en droit commun**. En droit commun, la signature, en plus d'identifier l'auteur de l'écrit, revêt deux intérêts :

i. La signature est « *nécessaire à la perfection d'un acte juridique* »[190].Toute personne est titulaire de droits dont elle peut se prévaloir pour défendre ses intérêts. Ces droits peuvent provenir d'actes juridiques ou de faits juridiques. « *Les actes juridiques sont des manifestations de volonté destinées à produire des effets de droit »*[191], qui ont été voulus par la personne. Par exemple, sont des actes juridiques, les contrats de vente ou encore les testaments, car la réalisation des effets notamment juridiques produits par leur contenu ont été voulus par la personne. Tandis que « *les faits juridiques sont des agissements ou des évènements auxquels la loi attache des effets de droit »*[192] mais dont les effets n'ont pas été recherchés par la personne[193]. Un accident de voiture est un fait juridique car ce dernier va produire des effets juridiques définis par la Loi, tels que l'indemnisation des passagers ou l'activation des assurances. Pour autant, cet accident, qu'il se soit produit de manière volontaire ou involontaire, ses conséquences et ses effets juridiques n'ont pas été recherchés par l'individu à l'origine du fait. La différence majeure entre l'acte et le fait juridique est la volonté de l'individu concernant les effets juridiques qui s'y attachent. Aussi, les modes de preuves admissibles pour un acte juridique et un fait juridique vont être différents.

La preuve de l'acte juridique est une exception à la liberté de la preuve. En principe, la preuve d'un acte juridique doit être réalisée par une preuve écrite[194] sauf exceptions prévues par la Loi telles que l'« *impossibilité matérielle ou morale de se procurer un écrit, s'il est d'usage de ne pas établir un écrit, ou lorsque l'écrit a été perdu par force majeure »*[195], dans ce cas, l'écrit pourra être suppléé par une autre preuve parfaite ou « *un commencement de preuve par écrit corroboré par un autre moyen de preuve »*[196]. Le Code civil prévoit notamment que la signature est « *nécessaire à la perfection d'un acte juridique* »[197] impliquant qu'une signature

[190] C. civ., art. 1367.
[191] C. civ., art. 1100-1.
[192] C. civ., art. 1100-2.
[193] Marc NICOD, *Les affres de la qualification juridique*, Presses de l'Université Toulouse 1 Capitole, 2018, p. 34.
[194] C. civ., art. 1359.
[195] C. civ., art. 1360.
[196] C. civ., art. 1361.
[197] C. civ., art. 1367.

est nécessaire[198] pour valider l'écrit[199]. Un arrêt du 7 octobre 2020[200] vient pourtant de confirmer un contrat, qui plus est, solennel, par échange de courriers électroniques en l'absence de signature. En l'espèce, un club de football avait mandaté un agent sportif afin de négocier le transfert d'un joueur d'un autre club par courriel. Plusieurs échanges de mails entre l'agent sportif et le club de football ont eu lieu, notamment pour proroger le mandat. En principe, le contrat de mandat impose un formalisme particulier[201] rendant le contrat nul si l'une des conditions n'est pas respectée. Cependant, la Cour de cassation a tout de même validé le contrat de mandat. En effet, elle a estimé que bien que la signature électronique *« constitue l'une des conditions de validité du contrat, son absence, alors que ne sont contestées ni l'identité de l'auteur du courriel ni l'intégrité de son contenu, peut être couverte par une exécution volontaire du contrat en connaissance de la cause de nullité, valant confirmation »*[202]. Ainsi, la Cour de cassation a justifié sa décision en se basant sur le fait que le contrat avait été confirmé notamment par sa prorogation par le club de football. Donc même en l'absence de signature électronique qui est en principe une condition de validité de l'acte, le contrat a tout de même été validé puisque celui-ci a été confirmé par les parties par son exécution.

ii. La signature apposée par son auteur *« manifeste son consentement aux obligations qui découlent de cet acte* »[203]. Grâce à sa signature, une personne identifiée accepte les effets que pourront produire le contenu d'un document[204]. Par exemple, les parties signent un contrat afin que le contenu de celui-ci soit exécuté. Le contenu expose notamment les obligations de toutes les parties, qu'elles vont s'engager à respecter. La manifestation de cet engagement, de ce consentement, est réalisée par l'apposition de leurs signatures respectives.

77. **La signature en droit « spécial ».** Le Code de la santé publique précise davantage la signification de la signature apposée sur un document contenant des données de santé[205], et fait une distinction de sa signification en fonction de la personne qui l'appose.

---

[198] Luc GRYNBAUM, « Preuve », *op.cit. « La définition de la preuve littérale et de l'écrit électronique, conforte cette idée que la signature est un acte en soi, accessoire indispensable du « corps » de l'acte, afin que ce dernier devienne un instrumentum valant preuve littérale ».*

[199] Cass. civ. 1ère, 30 avril 1970, 68-13.534, Publié au bulletin. Depuis 1970, la jurisprudence estimait que la signature était nécessaire pour conférer une valeur juridique à un écrit. Sans cette dernière, elle n'était qu'un commencement de preuve par écrit.

[200] Cass. Civ 1ère, 7 octobre 2020 n°19-18.135, publié au bulletin.

[201] C. sport, art. L. 222-17.

[202] Cass. Civ 1ère, 7 octobre 2020 n°19-18.135, publié au bulletin.

[203] C. civ., art. 1367.

[204] Luc GRYNBAUM, « Preuve », *op.cit.*

[205] C. santé publ., art. L. 1111-25. Sont concernés, les « documents comportant des données de santé à caractère personnel produits, reçus ou conservés, à l'occasion d'activités de prévention, de diagnostic, de soins, de

Lorsque la signature est apposée sur un de ces documents par une personne prise en charge, notamment un patient, cela signifie que la personne a pris connaissance du contenu du document et y consent[206]. Dans le cas présent, la personne n'est pas l'auteur du document, en revanche elle accepte le contenu, notamment les conditions, l'informationnel, ou encore les obligations au sein du document. Cela sera le cas lorsqu'une personne doit bénéficier d'une intervention chirurgicale. Le document signé par le patient attestera son consentement à la réalisation de l'intervention.

Lorsque la signature est apposée par un des professionnels mentionnés à l'article L. 1111-25 du Code de la santé publique, celle-ci signifie que le professionnel « *valide le contenu du document* »[207]. Lorsqu'un médecin rédige une prescription pour un de ses patients, celle-ci est signée, impliquant sa validation par le médecin. En cas d'erreur sur la prescription, notamment sur la posologie, le médecin engage sa responsabilité.

A l'instar des actes juridiques, certains documents contenant des données de santé ont l'obligation d'être signés pour être valides, tels que les certificats, les ordonnances[208] ou encore certains consentements patients. A titre d'exemple, toute recherche impliquant la personne humaine doit faire l'objet d'un consentement écrit[209]. Pour être valable, ce consentement écrit doit être signé, afin de pouvoir identifier la personne ayant consenti, et pour prouver que cette dernière a pris connaissance du document et qu'elle y consent[210].

On peut en conclure que la signature est exigée dès lors que le contenu informationnel d'un écrit revêt un haut degré d'importance. En effet, la signature est imposée pour les actes juridiques car ils impliquent des effets de droits voulus par la personne. Pour les documents contenant des données de santé, la signature est exigée pour tous les documents dont les contenus auront un impact sur la prise en charge du patient, et qui pourraient mettre en cause la responsabilité de celui qui les a produits. L'utilisation de la signature permettrait donc de donner davantage de valeur juridique à un document écrit signé, qu'à un document non signé. Cela est confirmé par la pratique qui parfois demande un écrit signé alors que le Droit ne l'exige pas. Par exemple, il est prévu que « *les actes de télémédecine sont réalisés avec le*

---

compensation du handicap, de prévention de perte d'autonomie, ou de suivi social et médico-social réalisées par […], un professionnel de santé, un établissement ou service de santé, un professionnel ou organisme concourant à la prévention ou aux soins […], le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ».

[206] C. santé publ., art. L. 1111-28.

[207] *Ibid.*

[208] C. santé publ., art. R. 4127-76.

[209] C. santé publ., art. L.1122-1-1.

[210] C. santé publ., art. L. 1111-28.

consentement libre et éclairé de la personne »[211]. La forme du consentement est libre, l'oral pourrait donc suffire. Cependant, la pratique veut que, pour donner davantage de valeur au consentement, celui-ci soit réalisé de manière écrite, notamment pour avoir une preuve signée de la personne prise en charge.

78. **La signature électronique garante de l'intégrité du document**. Les effets de la signature présentés ci-dessus sont communs, que la signature soit manuscrite ou électronique. En effet, aucune distinction quant à la signification de la signature par rapport à son format matérialisé ou dématérialisé n'est introduite. Cependant, il apparaît que la signature électronique puisse permettre un effet supplémentaire à la signature manuscrite : la garantie de l'intégrité du document.

B) La signature électronique garantissant l'identité de la personne et l'intégrité du document

79. **La signature électronique garante de la force probante du document au moment de sa création.** L'article du code civil prévoit que la signature électronique « *consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État* »[212]. Le seul fait d'utiliser comme moyen la signature électronique permet donc d'identifier l'auteur d'un écrit et d'en garantir son intégrité remplissant ainsi les deux conditions nécessaires pour garantir la force probante d'un écrit électronique au moment de sa création[213]. Il existe plusieurs signatures électroniques, ayant des niveaux de fiabilité différentes, allant de la signature qualifiée qui est présumée fiable (1) aux autres signatures électroniques (2).

1) <u>La présomption de fiabilité</u>

80. **La signature électronique présumée fiable**. Les textes ont introduit une présomption de fiabilité, permettant de donner un niveau de confiance supérieur au procédé utilisé. En effet, cette présomption permet de retourner la charge de la preuve ; *« la partie qui*

[211] C. santé publ., art. R. 6316-2.
[212] C. civ., art. 1367.
[213] CASSAR Bertrand, *La transformation numérique du monde du droit*, Thèse dactylographiée, Strasbourg, 2020, p. 74. Bertrand CASSAR va même plus loin en attestant que la signature électronique permet également de manifester le consentement du signataire : *« La signature électronique est donc le moyen de parfaire un acte juridique sur un support écrit (dématérialisé), en apportant la preuve de l'identité, de l'intégrité et le consentement du signataire ».*

entend contester un écrit électronique devra fournir au juge des éléments justifiant le renversement de la présomption[214] *car une simple dénégation ne suffit pas à provoquer un incident de vérification »*[215]. Ce n'est plus à celui qui produit l'écrit avec la signature présumée fiable, qu'il incombe de prouver sa fiabilité mais à celui qui la conteste de prouver l'absence de fiabilité. Afin de bénéficier de cette présomption de fiabilité, le procédé utilisé doit être conforme à un décret. Un premier décret datant de 2001[216] est venu préciser les conditions à mettre en place s'agissant de la signature électronique. Ce décret a été abrogé par le décret de 2017[217] dont l'article 1 prévoit qu'elle est présumée fiable, si une signature électronique qualifiée est mise en place. Ce seul article du Décret donnant des indications sur la fiabilité de la signature électronique renvoie au Règlement eIDAS[218], entré en vigueur le 17 septembre 2014, visant *« à établir un cadre d'interopérabilité pour les différents systèmes mis en place au sein des États membres afin de promouvoir le développement d'un marché de la confiance numérique. Le règlement formule des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique ainsi qu'à celle des signatures électroniques, pour les échanges entre les organismes du secteur public et les usagers »*[219]. Le renvoi à ce Décret permet de bénéficier d'une signature électronique fiable, reconnue au sein du territoire national, mais également au sein des autres Etats membres[220].

81. **Le concept de la signature électronique qualifiée**[221]**.** Une signature qualifiée est une signature avancée ; elle doit notamment respecter les conditions suivantes : « *être liée au signataire de manière univoque ; permettre d'identifier le signataire ; avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable* »

[214] C. proc. civ., art. 288-1.
[215] Frédérique FERRAND, « Preuve », *op. cit.*
[216] Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, JORF n°0077, 31 mars 2001, texte n°19.
[217] Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, JORF n°0229, 30 septembre 2017, texte n°8.
[218] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014.
[219] ANSSI, *Règlement EIDAS – champ d'application et destinataires*. Disponible à l'adresse : https://www.ssi.gouv.fr/ (consulté le 06/06/2021).
[220] Corinne BLERY, « Communication par voie électronique », *Dalloz action Droit et pratiques de la procédure civile »*, 2021-2022.
[221] Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, JORF n°0229, 30 septembre 2017, texte n°8, art. 1 : Est une signature électronique qualifiée une signature électronique avancée, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 de ce règlement.

[222]. La signature doit notamment être créée grâce à un dispositif de création de signature électronique qualifié respectant notamment les exigences suivantes : la confidentialité des données, ou encore la non-modification des données[223]. Ce dispositif doit lui-même reposer sur un certificat de signature électronique qualifié. Une signature électronique qualifiée permet donc de présumer la fiabilité de la signature, et son effet juridique « *est équivalent à celui d'une signature manuscrite »*[224].

82. **La signature qualifiée difficilement applicable dans le domaine de la santé.** L'emploi d'une signature électronique qualifiée n'est pas utilisée dans de nombreux domaines, au regard de la complexité de mise en œuvre[225]. Il n'y aura d'intérêt à utiliser ce procédé que si le Droit l'impose ou si l'utilité de l'écrit est tel qu'une signature avec un haut niveau de garantie et de sécurité est nécessaire. A titre d'exemple, l'acte authentique électronique établi et signé par un notaire doit l'être « *au moyen d'un procédé de signature électronique qualifiée conforme aux exigences du décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique »*[226], l'utilisation d'un autre niveau de signature électronique n'est pas possible. Cela s'explique par la nature même des actes établis par les notaires et des effets juridiques que ces derniers entraînent.

A l'heure actuelle dans le domaine de la santé, aucune signature électronique qualifiée n'est utilisée[227]. Pour autant, cela ne signifie pas que la création d'une telle signature dans ce domaine soit impossible. Cependant la question se pose de savoir si cela est pertinent au regard des enjeux liés aux documents produits.

83. **Le parallèle avec la signature électronique des décisions juridictionnelles en matière civile.** Bien que la signature électronique qualifiée soit pour l'instant difficilement applicable en santé, on constate que d'autres domaines ont réussi à y parvenir ; un arrêté du

---

[222] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 26.

[223] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, annexe II.

[224] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 25.

[225] Gwendoline LARDEUX, « Preuve : modes de preuves », *op. cit. « De manière générale, l'utilisation d'une signature électronique présumée fiable dénommée signature « qualifiée » par les décrets précités – est rare car la technique est complexe et coûteuse*.

[226] Décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JORF, 3 décembre 1971, art. 17.

[227] ANS, *Référentiel force probante des documents de santé – Annexe 3 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques,* PGSSI-S, 2021.

20 novembre 2020 est venu définir les règles permettant de signer électroniquement les décisions juridictionnelles en matière civile[228]. Cette signature électronique qualifiée reposant sur le Règlement eIDAS contient : *« l'identification du signataire ; un jeton d'horodatage garantissant l'intégrité du document et la date de signature ; un certificat de signature électronique qualifié et valide, délivré par le ministère de la justice »*[229]. Cette signature électronique permet de garantir que toute modification ultérieure est détectable, prouvant ainsi l'intégrité de la décision.

L'intégrité du document est également garantie pendant toute sa durée de conservation ; *« La décision juridictionnelle signée électroniquement est conservée dans un minutier électronique placé sous la responsabilité du directeur du greffe pendant les durées d'utilisation comme archives courantes et de conservation comme archives intermédiaires prévues à l'article R. 212-13 du code du patrimoine. Pendant ces durées, ce minutier garantit l'accessibilité, la lisibilité, l'intégrité, la sécurité et la confidentialité des décisions juridictionnelles signées électroniquement »*[230].

Thomas CASSUTO souligne à juste titre que *« cet arrêté constitue une étape importante dans la digitalisation de la justice civile. En effet, ce processus de signature électronique permet l'édition de décisions civiles […] sans qu'il soit nécessaire de les imprimer, de les signer manuellement puis de les numériser pour notification et archivage »*[231]. Cela permettra un gain de temps certain ainsi qu'une simplification des *« formalités de notification et pour les avocats de gestion du courrier et de leurs archives »*[232].

On ne peut qu'espérer prochainement un texte de la même teneur proposant une signature qualifiée pour les professionnels de santé.

2) Les autres signatures électroniques

84. **Admission de la signature électronique autre que qualifiée**. En plus de la signature électronique qualifiée, le Règlement eIDAS prévoit deux autres formes de signatures : la signature électronique dite simple et la signature électronique avancée. Ces

[228] Arrêté du 20 novembre 2020 relatif à la signature électronique des décisions juridictionnelles rendues en matière civile, JORF n°0283, 22 novembre 2020, texte n°13. *« A l'exception des décisions rendues par les tribunaux de commerce et les tribunaux mixtes de commerce ».*
[229] Arrêté du 20 novembre 2020 relatif à la signature électronique des décisions juridictionnelles rendues en matière civile, JORF n°0283, 22 novembre 2020, texte n°13, art. 2.
[230] Arrêté du 20 novembre 2020 relatif à la signature électronique des décisions juridictionnelles rendues en matière civile, JORF n°0283, 22 novembre 2020, texte n°13, art. 7.
[231] CASSUTO Thomas, « Signature électronique des décisions juridictionnelles rendues en matière civile : nouvel arrêté », *Dalloz actualité*, 2020.
[232] *Ibid.*

dernières ne bénéficient pas de la présomption de fiabilité, pour autant, cela ne signifie pas qu'elles n'ont aucune valeur juridique. « *Tout écrit disposant d'une signature électronique simple est admissible devant les tribunaux au même titre qu'un écrit disposant d'une signature électronique qualifiée bénéficiant de la présomption de fiabilité, sous réserve de rapporter la preuve que les exigences de fiabilité sont respectées (identification de l'auteur et intégrité de l'acte), la différence se situant uniquement au niveau de la charge de la preuve* »[233]. La signature électronique simple mais également la signature électronique avancée sont donc admises en tant que preuve à l'instar de la signature électronique qualifiée. En revanche, elles ne bénéficient pas d'une présomption de fiabilité, leur fiabilité devra donc être démontrée par celui qui souhaite s'en prévaloir. Il y a donc un renversement de la charge de la preuve. La preuve de la fiabilité pourra être démontrée par tout moyen, et devra emporter la conviction du juge, ce qui sera plus aisé pour la signature avancée que pour la signature électronique simple.

85. **La signature électronique simple.** La signature électronique simple correspond à « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer »*[234]. Cette signature simple correspond au plus faible niveau de sécurité et de fiabilité puisque la seule exigence posée est un lien entre deux ensembles de données : des données constituant le contenu d'un document et des données constituant la signature de la personne telles que les prénom et nom de la personne, ainsi qu'une mention du type « document signé par ». Cette seule signature électronique permet tout au plus d'identifier la personne ayant signé le document mais ne permet pas d'en garantir son intégrité. Il sera nécessaire de mettre en place d'autres moyens permettant en plus de la signature électronique simple, de garantir l'intégrité du document tels que le scellement du document permettant ainsi sa non-altération. L'identification même de la personne par la signature électronique simple n'est pas certaine. Comment s'assurer que la personne qui signe est bien la personne identifiée ? Une signature simple ne le permet pas totalement. Des méthodes sont mises en place afin de s'assurer de l'identité du signataire, comme l'utilisation d'un login et d'un mot de passe, couplés avec un système d'OTP permettant au signataire de valider sa signature grâce à un mot de passe à usage unique envoyé sur son téléphone. Ce système permet de garantir un lien entre le

[233] Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *AJC*, octobre 2016.
[234] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 3

signataire et le téléphone, mais ne permet pas forcément de garantir que la personne identifiée sur le document est bien la propriétaire du téléphone et donc le signataire. De plus, il n'y a aucun moyen de s'assurer que la personne qui se trouve dernière le téléphone est bien la personne à qui il appartient. Cependant ce système d'OTP bien que non fiable à 100% permet de garantir davantage de sécurité qu'une signature réalisée sans OTP. Cette signature électronique simple n'est certes pas la plus fiable, mais est la plus répandue au regard de sa simplicité d'usage et de sa rapidité de mise en œuvre[235].

86. **La signature électronique avancée.** Quant à la signature avancée, il s'agit d'une « *signature électronique qui satisfait aux exigences énoncées à l'article 26*[236] *»*[237] du Règlement eIDAS, permettant d'une part d'identifier de manière certaine la personne et d'autre part de garantir l'intégrité des données, soit le respect des conditions énoncées par le Code civil. Pour quelles raisons cette signature n'est-elle pas présumée fiable ? Bien que le Règlement eIDAS définit les conditions à remplir, la mise en place de ces conditions reste assez libre ne permettant pas de présumer de la fiabilité de la signature. Cependant, même si elles ne bénéficient pas d'une présomption de fiabilité, les signatures électroniques avancées bénéficient d'un haut niveau de fiabilité notamment en santé.

L'Agence du Numérique en Santé (anciennement Asip Santé) est chargée de l'élaboration de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) qui « *fixe les exigences de sécurité des services numériques en santé »*[238]. Cette PGSSI-S définit

---

[235] Bertrand CASSAR, « Données – Gouvernance des données », *Répertoire IP/IT et Communication*, 2022. *« d'autres procédés permettent actuellement de rapporter la preuve d'un consentement, soit par la mise en œuvre d'un processus sécurisé (à l'instar de la théorie du « double-clic », l'usage d'un téléservice ou le recours à l'identité numérique), soit par l'usage d'une technique informatique (telle que les chaînes de blocs [ou BlockChain] utilisant la signature électronique dans la validation des blocs ou encore l'intelligence artificielle avec l'utilisation de la reconnaissance faciale afin de valider, hors processus sécurisé, une identité numérique). À partir du moment où le processus ou la technique mis en œuvre permettent de démontrer l'identité, l'intégrité et le consentement de l'utilisateur, ils peuvent être utilisés pour engager juridiquement l'utilisateur ou les parties concernées ».*

[236] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 26 : *« Une signature électronique avancée satisfait aux exigences suivantes :*

a) être liée au signataire de manière univoque;

b) permettre d'identifier le signataire;

c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif; et

d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ».

[237] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 3.

[238] ANS, « Qu'est-ce que le corpus documentaire de la PGSSI-S ? », 17 novembre 2021, disponible à l'adresse : http://esante.gouv.fr/ (consulté le 07/10/2021).

notamment les moyens d'identification et d'authentification en santé, comme par exemple la Carte Professionnelle de Santé (CPS). La CPS « *est une carte d'identité professionnelle électronique dédiée aux secteurs de la santé et du médico-social. Elle permet à son titulaire d'attester de son identité et de ses qualifications professionnelles. Elle contient les données d'identification de son porteur : identité (n° d'identification, nom patronymique, nom d'exercice…), profession, spécialité, identification du mode d'exercice, identification du lieu d'exercice* »[239]. Cette CPS est disponible pour les professionnels de santé tels que les médecins, les pharmaciens, les sage-femmes etc. Elle permet à ces professionnels de transmettre des feuilles de soins électroniques, s'authentifier auprès de services nationaux, mais aussi d'apposer une signature électronique. Cette signature électronique n'est pas à ce jour qualifiée mais avancée. Pour autant, cette dernière, fournie par l'ANS bénéficie d'un haut niveau de fiabilité. Pour s'adapter aux nouveaux usages et aux nouveaux outils numériques à la disposition des professionnels de santé permettant la mobilité, la CPS a évolué en e-CPS permettant « *au professionnel de santé ou du médico-social de s'authentifier directement auprès d'un service en ligne avec son mobile ou sa tablette, sans passer par un poste configuré et équipé d'un lecteur de carte* »[240].

87. **La valeur de la signature manuscrite numérisée.** La signature manuscrite étant équivalente à la signature électronique qualifiée, elle bénéficie également d'une présomption de fiabilité. Se pose la question de la valeur juridique de cette signature fiable si celle-ci est scannée et introduite sur un document électronique.

Le Code civil prévoit qu'une signature permet d'identifier l'auteur d'un document et est la manifestation de son consentement « *aux obligations qui découlent de cet acte »*[241], or une signature scannée ne permet pas de remplir ces deux effets. En effet, « *une signature scannée s'analyse comme le graphisme de la marque personnelle de son auteur converti par un processus de numérisation* »[242] ce que toute personne, sachant utiliser, même *a minima,* les technologies de l'information et de la communication, est en capacité de faire. Cette signature manuscrite scannée ne permet donc pas d'identifier la personne et de manifester son consentement au contenu de l'acte, car il n'y a aucune certitude que la personne qui a réalisé cette signature soit la même que celle qui l'a introduite sur le document[243]. Les juges ont donc

[239] ANS, « Cartes de Professionnels de Santé », disponible à l'adresse : http://esante.gouv.fr/ (consulté le 10/07/2021).
[240] ANS, « e-CPS », disponible à l'adresse : http://esante.gouv.fr/ (consulté le 10/07/2021).
[241] C. civ., art 1367.
[242] Pierre-Xavier CHOMIAC DE SAS, « La signature scannée et sa valeur juridique », *PCS Avocat,* 2018.
[243] Jérôme HUET, « Efficacité d'une signature scannée », *RDC,* 2021/1, n°117m1, p. 63.

très régulièrement jugé que la signature électronique scannée était insuffisante pour s'assurer de l'identification du signataire[244]. En revanche, un document contenant une signature scannée, ne sera pas dépourvu de valeur juridique, mais pourra être utilisé comme commencement de preuve par écrit. D'autres éléments de preuves devront venir étayer le contenu du document.

Pour autant, on constate depuis quelques années, une évolution de la position des juridictions sur la valeur de la signature scannée, dont un des derniers arrêts a validé une contrainte revêtue d'une signature scannée[245]. Cependant, *« même si la Cour de Cassation reconnaît en l'espèce que le scan d'une signature n'est plus une cause systématique d'invalidité d'un acte, nous ne pouvons en déduire que la solution s'appliquera à tout type d'acte ou courrier »*[246]. Il est donc nécessaire de rester prudent sur l'utilisation d'une signature scannée[247], cette dernière ayant manifestement moins de valeur qu'une signature manuscrite apposée sur un document papier ou qu'une signature électronique, bien que la pratique actuellement tend à utiliser cette méthode, notamment dans les entreprises.

88. **Le choix de la signature à utiliser.** Plusieurs choix de signatures électroniques sont disponibles présentant plus ou moins de garantie quant à leur fiabilité. La signature électronique avancée semble être le bon compromis entre une signature qualifiée présentant une présomption de fiabilité mais difficile à mettre en place et une signature simple dont la fiabilité peut facilement être remise en cause. Mais le choix de la signature à utiliser ne se limite pas à cela. D'une part, il est nécessaire de déterminer si le Droit impose l'utilisation d'un certain type de signature, comme la signature qualifiée pour les notaires. D'autre part, il est nécessaire de déterminer la valeur du document à signer en fonction de son contenu et l'impact que ce dernier pourrait avoir pour l'établissement de santé, l'établissement ou encore la personne prise en charge. En fonction de sa valeur, le choix de la signature utilisée sera différent. Aussi, l'utilisation d'une signature simple pourrait tout à fait être justifiée et suffisante pour certains documents, plutôt que l'utilisation d'une signature avancée, plus compliquée à utiliser et pas forcément toujours pertinente.

[244] CA, Fort de France, 14 décembre 2012, n°12/00311, CA Besançon, ch. soc., 20 oct. 2000, D. 2001, IR p. 432, CA Rouen, ch. Soc., 20.09.2017, n°16/05131.
[245] Cass. Civ., 2ème, 28 mai 2020, 19-11.744, Publié au bulletin.
[246] Emmanuelle DUGUE-CHAUVIN, « Droit du travail : une signature scannée apposée sur une contrainte a-t-elle une valeur juridique ? », *emo avocats*, 30 juin 2020. Disponible à l'adresse : https://emo-avocats.com/ (consulté le 23/07/2021).
[247] Jérôme HUET, « Efficacité d'une signature scannée », *op. cit.*

§2 La valeur juridique des écrits non signés

89. **La signature électronique n'est qu'un moyen**. La signature électronique est donc un moyen pouvant présenter de nombreux avantages selon le choix du niveau de signature, comme permettre l'identification de la personne dont émane le document et la garantie de son intégrité. Ce seul moyen permet donc au moment de la création du document, de respecter les conditions énoncées à l'article 1366 du Code civil. Or tous les écrits n'ont pas l'obligation d'être signés. En effet, l'apposition d'une signature, qu'elle soit manuscrite ou électronique, est seulement obligatoire lorsque les textes l'exigent comme pour les actes juridiques[248] ou encore les ordonnances médicales[249].

90. **La preuve d'un fait juridique.** En effet, si le Droit prévoit textuellement que certains documents doivent être signés, cela signifie que les écrits pour lesquels les textes ne prévoient pas la signature de manière expresse n'ont pas l'obligation de l'être. Prenons l'exemple du fait juridique. Il est prévu que la preuve d'un acte juridique doit être par principe, réalisée par écrit, contrairement au fait juridique dont la preuve peut être apportée par tout moyen. « *Ces règles de preuve spécifiques découlent du fait que l'obligation a été anticipée dans l'acte juridique »*[250] contrairement au fait juridique, dont l'événement n'était pas prévu et dont les effets n'ont pas été voulus. La preuve d'un fait juridique pouvant être apportée par tout moyen signifie que des écrits pourront être produits, dès lors qu'ils respectent les conditions donnant une valeur juridique à l'écrit. Or on constate une différence entre la preuve écrite d'un acte juridique et celle d'un fait juridique. En effet, il est prévu que la signature est nécessaire pour « *la perfection d'un acte juridique »*[251], impliquant implicitement que cela n'est pas le cas pour les faits juridiques.

91. **La valeur probante de l'écrit non signé.** Il apparaît donc que de nombreux écrits ne sont pas signés mais ne sont pas pour autant dépourvus de valeur probante. Pour cela, les écrits non-signés, doivent également respecter les deux conditions suivantes : prouver l'identification de la personne auteur du document (A) et l'intégrité du document produit (B), mais sans signature.

[248] C. civ., art. 1367.
[249] C. santé publ., art R.4127-76.
[250] Bérénice de BERTIER-LESTRADE, « Les affres de la qualification juridique – La frontière entre l'acte juridique et le fait juridique », *Presses de l'Université Toulouse 1 Capitole,* mars 2018, p-36.
[251] C. civ., art. 1367.

A) L'identification par tout moyen

92. **La preuve écrite électronique.** Avec l'émergence des technologies de l'information et de la communication, la production d'écrits papier est délaissée pour laisser place aux écrits électroniques présentant de nombreux avantages : la rapidité d'envoi et de réception d'écrits, l'accès instantané à des documents en simultané avec d'autres personnes, ou encore le partage d'informations. Ce constat est autant réalisé dans la sphère personnelle que professionnelle avec les réseaux sociaux, l'utilisations d'applications, ou encore l'envoi de SMS et de mails. En moyenne, un Français enverra trente-trois mails par jour (en 2021), que ce soit pour un usage personnel ou professionnel[252]. Les technologies de l'information et de la communication n'ont pas que favorisé l'utilisation de l'écrit électronique par rapport à l'écrit papier, mais ont également augmenté le nombre d'écrits produits par une personne. Tous ces écrits pourront potentiellement être utilisés en tant que preuve. Pour autant, cela nécessite de pouvoir identifier l'auteur de l'écrit par d'autres moyens que la signature (1). En santé, au regard de la sensibilité des données traitées, des modes d'identification ont été mis en place et sont en cours d'évolution pour garantir encore davantage l'identification de la personne et la sécurité des données (2).

1) L'identification moderne

93. **Le mode de preuve moderne.** L'évolution technologique a engendré inévitablement le développement de nouveaux supports de preuves qui sont admis devant les juridictions[253] : le SMS[254], le mail[255], les réseaux sociaux[256], ou encore les applications. Ces modes de preuves ne permettent pas toujours de signer le contenu produit, pour autant, cela ne signifie pas que l'identité de la personne, auteur du contenu n'est pas connue. A titre d'exemple pour un SMS, on peut estimer que celui qui l'envoie est la personne à qui appartient le numéro émetteur. Cependant, la personne pourra toujours nier être la personne ayant envoyée le SMS en invoquant qu'une autre personne aurait pu utiliser son téléphone à son insu. Celui qui se prévaut du SMS devra en prouver l'auteur. Peu importe la technologie utilisée pour produire l'écrit, celui-ci pourra toujours être utilisé comme preuve, en revanche c'est sa valeur probante qui est à graduer en fonction de la technologie choisie. Un outil

[252] Bastien CORTHESY, « Le nombre de Mails envoyés par jour en 2021 », *Le monde du mail*, décembre 2021. Disponible à l'adresse : https://mondedumail.com/ (consulté le 05/02/2022).
[253] Dahlia ARFI-ELKAIM, « e-mails, SMS, captures d'écran des réseaux sociaux : quelle valeur probante ? », *JDB Avocats*, 2018.
[254] Cass. Com., 23 mai 2007, 06-43.209, Publié au bulletin.
[255] Cass. Civ. 1ère, 18 mai 2005, 04-13.745, Publié au bulletin.
[256] Cass. Civ. 1ère, 10 avril 2013, 11-19.530, Publié au bulletin.

possédant la même finalité, pourra se voir attribuer un niveau différent de fiabilité en fonction des technologies utilisées et notamment la fiabilité de l'identité de l'auteur des contenus.

94. **La fiabilité du mail.** Prenons l'exemple du mail. Le mail est un courrier envoyé de manière électronique, par le biais d'une boîte mail. Il existe de très nombreuses boîtes mail disponibles avec différents opérateurs bénéficiant de caractéristiques différentes : la gratuité, la capacité de stockage, l'interopérabilité avec d'autres applications etc. Certaines de ces différences vont permettre de déterminer le niveau de fiabilité que l'on peut accorder à l'une ou l'autre messagerie en fonction de ce qui est recherché comme garanties. En l'espèce, est cherché le niveau de fiabilité concernant l'identification de la personne auteure des mails.

Le niveau 1 correspond aux mails personnels. En effet, toute personne peut créer et choisir son adresse mail, notamment en utilisant des pseudonymes ou en mettant un nom et un prénom. A titre d'exemple, une personne peut créer une adresse mail du type pierre.dupond@gmail.com (soit prénom.nom), pour autant, cette personne ne s'appelle pas réellement Pierre Dupond. L'identité de la personne derrière cette adresse mail est donc incertaine. Le niveau 2 concerne le domaine professionnel dont l'identification de la personne derrière une adresse mail est plus fiable. Dans la plupart des entreprises, le service informatique est en charge de créer une adresse mail pour les nouveaux collaborateurs (sous la forme prenom.nom) dont le login et le mot de passe temporaire seront donnés directement au collaborateur en question. Il est possible d'imputer une adresse mail à une personne puisqu'elle lui a été attribuée personnellement, par l'intermédiaire d'un tiers qui a vérifié l'identité de la personne. L'identité du détenteur de l'adresse mail semble donc fiable. Or le détenteur pourra toujours nier avoir envoyé un mail en affirmant qu'une autre personne s'est connectée à sa place et a envoyé ce mail à son insu.

Le niveau 3 qui est le plus fiable, correspond aux boîtes mail créées et dédiées à certaines professions. Prenons l'exemple des boîtes mail des professionnels de santé. Par principe, les professionnels de santé vont être amenés à échanger des informations concernant la santé d'un patient. Au regard de la nature des informations échangées, les professionnels de santé n'ont pas la possibilité d'utiliser n'importe quelle messagerie électronique ; celle-ci doit respecter le cadre légal applicable, notamment concernant l'échange et le partage d'informations de santé[257], l'hébergement des données de santé par un tiers[258] ainsi que la règlementation sur les

[257] C. santé publ., art. L. 1110-4 et s.
[258] C. santé publ., art. L. 1111-8 et s.

données à caractère personnel[259]. A titre d'exemple, « *les messageries sécurisées de l'Espace de Confiance MSSanté intègrent le respect de ces obligations »*[260] *;* cet espace de confiance prévoit un mode d'identification permettant de « *garantir au récepteur de la messagerie l'identité de l'émetteur du message avec un fort niveau d'imputabilité du message et donc de son contenu »*[261]. Pour qu'une messagerie sécurisée entre dans l'espace de confiance MSSanté[262], celle-ci doit être conforme aux spécifications fonctionnelles et techniques établies[263]. Ces spécifications exposent notamment les moyens d'identification et d'authentification à respecter. Pour pouvoir bénéficier d'une messagerie dans le domaine MSSanté, l'identité de la personne doit être vérifiée afin d'attribuer, de relier la messagerie à une personne en particulier ; par exemple grâce à l'utilisation de la CPS comportant un certificat électronique d'authentification, ou bien sous la responsabilité d'une autorité d'enregistrement, en charge de certifier l'identité de la personne à qui sera attribuée la messagerie. Il y a donc une fiabilité sur l'identité de la personne utilisant la messagerie attribuée. De plus, il est imposé, pour pouvoir se connecter à la messagerie, d'utiliser des moyens d'authentification forts tels que la CPS ou encore l'association d'un login, d'un mot de passe, et d'un code OTP. Ces modes d'authentification reposent sur la combinaison de plusieurs facteurs d'authentification (une carte + un mot de passe ou un login + un mot de passe + un téléphone) rendant plus compliquée mais pas impossible, l'authentification d'une personne souhaitant se connecter à une messagerie qui n'est pas la sienne.

95. **L'identification et l'authentification garante de l'identité de la personne**. Il apparaît que l'identification de la personne peut être réalisée par d'autres moyens que la signature électronique. En revanche, le procédé utilisé permettra au juge de déterminer le niveau de fiabilité que l'on peut accorder sur l'identité de la personne auteure de l'écrit.

Il apparaît que deux facteurs entrent en jeu, l'identification et l'authentification de la personne. En effet, même si le procédé d'authentification est fort, mais que l'identification de la personne au préalable n'est pas garantie, il pourra y avoir un doute sur l'identité de la

---

[259] 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, JOUE, L 119, 04 mai 2016.
Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[260] MSSanté, « Comprendre MSSanté », 2021. Disponible à l'adresse : https://mssante.fr/ (consulté le 08/03/2021).

[261] *Ibid.*

[262] Claire DEBOST, « Les établissements de santé dans le viseur du ministère pour imposer la MSSanté », *RDS*, 2015, n°64, pp. 328-329. Les enjeux d'une telle messagerie est *« un décloisonnement entre la ville et l'hôpital et une meilleure coordination des soins dans le respect de la confidentialité et la sécurité des données ».*

[263] MSSanté, « Industriels », 2021. Disponible à l'adresse : https://mssante.fr/ (consulté le 08/03/2021).

personne auteure de l'écrit, et vice versa. C'est donc la combinaison des modes d'identification et d'authentification appliqués qui permettra de prouver l'identité de la personne et d'emporter la conviction du juge.

2) Une évolution de l'identification en santé

96. **L'identification et l'authentification en santé**. Initialement en santé, l'ANS avait établi au sein de la PGSSI-S deux référentiels concernant l'identification[264] et l'authentification[265] des acteurs de santé au sein des systèmes d'informations, permettant de garantir l'identité du professionnel personne physique, grâce à la mise en place d'un niveau de sécurité adéquat et permettant ainsi de lui imputer les actions qu'il a pu réaliser.

97. **Une évolution permettant davantage de sécurité**. L'Ordonnance du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie[266] est venue remanier les modalités d'identification pour accéder aux services numériques en santé[267], dont l'identification doit reposer « *sur un moyen matériel ou immatériel, qui garantit un niveau adapté de sécurité et de protection des données à caractère personnel* »[268] par rapport au type de service numérique en santé, dont les spécifications seront définies au sein de référentiels.

98. **Les référentiels d'identification[269]**. L'ANS a donc mis en concertation du 4 juin au 30 juillet 2021 trois référentiels[270], dont l'un concerne l'identification des

[264] Asip santé, *Référentiel d'identification des acteur sanitaires et médico-sociaux,* 2014. Disponible à l'adresse : https://esante.gouv.fr/ (consulté le 08/05/2021). *« L'identification a pour but de déterminer l'identité d'un acteur via un identifiant qui lui a été attribué préalablement lors de la vérification et de l'enregistrement de ses traits d'identité. Dans le contexte de la sécurité, l'identification est notamment liée à l'authentification, par exemple pour la mise en œuvre des droits d'accès au système d'information ».*

[265] ANSSI, *Référentiel Général de Sécurité,* 2010. Disponible à l'adresse : https://www.ssi.gouv.fr/ (consulté le 08/05/2021). *« L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. L'authentification est toujours précédée ou combinée avec une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté : un identifiant. En résumé, s'identifier c'est communiquer un identifiant présumé, s'authentifier c'est apporter la preuve que l'entité s'est vue attribuer cet identifiant ».*

[266] Ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie, JORF n°0111, 13 mai 2021, texte n°38.

[267] C. santé publ., art. L. 1470-1. Les services numériques en santé « sont les systèmes d'information ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités ».

[268] C. santé publ,. art. L. 1470-2.

[269] Margo BERNELIN, « Le référentiel d'identification électronique en santé approuvé », *Editions Législatives,* 2022. *« l'Agence a tenté de « trouver le juste équilibre entre, d'une part, la nécessaire sécurité dans le traitement des données de santé et, d'autre part, la réalité des usages par les professionnels qui prennent en charge les patients » ».*

[270] L'un concernant l'identification électronique des acteurs de santé personne physique, un autre concernant les

professionnels personne physique. Ces référentiels ont été finalement publiés au sein de la PGSSI-S le 01 avril 2022 dans leur version 1.0. Le référentiel sur l'identification des professionnels personne physique décrit les modalités d'identification électronique (et d'authentification) « *ainsi que les différents identifiants et dispositifs d'authentification utilisables […] en fonction du cadre d'usage* »[271]. A ce titre, une distinction est réalisée entre les services numériques dits « sensibles »[272], et les autres services considérés comme non sensibles engendrant des différences sur le mode d'identification.

Pour les services sensibles, les seuls moyens d'identification électronique autorisés sont : les moyens d'identification disponibles sur Pro Santé Connect[273], la carte CPx ou e-CPS, les moyens d'identification électronique homologués ainsi que les moyens d'identification électronique certifiés de niveau eIDAS substantiel ou élevé[274]. En effet, ces services numériques en santé, tels que le dossier patient informatisé étant sensibles au regard du type de donnée traitées et de leur utilisation (accès à distance, service partagé, traitement à grande échelle etc.), nécessitent une identification forte et sécurisée, pour s'assurer de l'identité de la personne et pour minimiser les risques d'accessibilité à la donnée de manière indue.

Les services numériques en santé existants qui entrent dans la catégorie « sensible » vont bénéficier d'un délai pour mettre en place ces nouveaux modes d'identification et abandonner les autres solutions moins sécurisées :

---

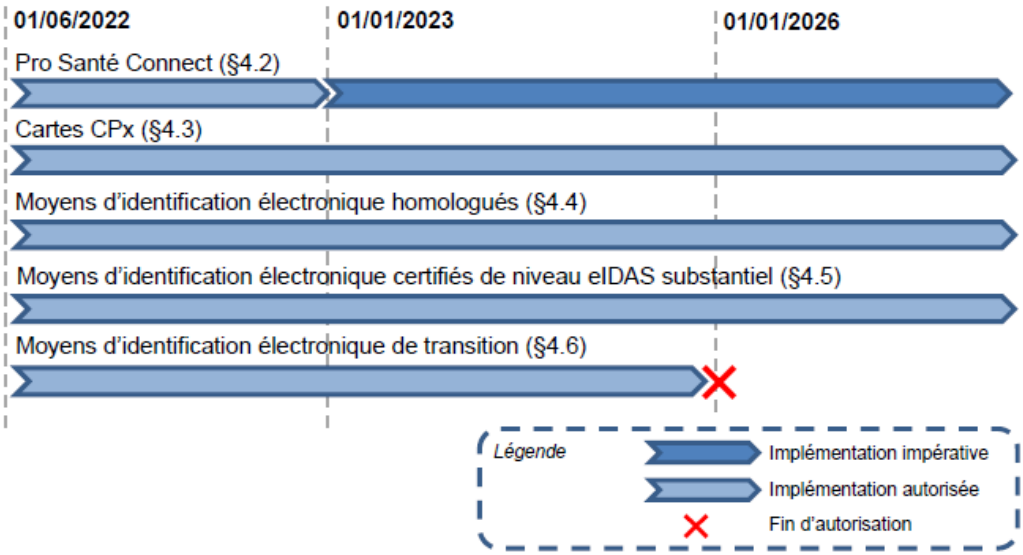
acteurs de santé personnes morales et pour finir les usagers.

[271] ANS, *Référentiel d'identification électronique – Acteurs des secteurs sanitaire, médico-social et social [personnes physiques],* PGSSI-S, 2022. Disponible à l'adresse : https://esante.gouv.fr/ (consulté le 15/09/2022).

[272] ANS, *Référentiel d'identification électronique – Acteurs des secteurs sanitaire, médico-social et social [personnes physiques],* PGSSI-S, 2022. Disponible à l'adresse : https://esante.gouv.fr/ (consulté le 15/09/2022). Les services sensibles sont les services traitant des données de santé à caractère personnel et *« qui appartiennent à l'une des catégories suivantes : - Les services partagés, définis comme dépassant le cadre d'une personne morale et/ou mis en œuvre à l'échelle d'un territoire ou au niveau national (ex : dossier médical partagé, plateforme de e-parcours, dossier pharmaceutique, etc.) ; - Par transitivité, les services numériques qui intègrent des services partagés (ex : dossier patient informatisé, système de gestion de laboratoire, système d'information de radiologie, boites de messageries sécurisées de santé, etc.) ; - Les services proposant un accès web externe aux SI, pour les professionnels d'un établissement (ex : services accessibles en mobilité ou télétravail) ou leurs correspondants de ville ; - Les services non partagés mais qui intègrent des traitements ou des accès à grande échelle, définis comme les situations où : 1. Soit le nombre de patients dont les données sont nouvellement référencées dépasse 10 000 par an ; soit le nombre de professionnels distincts s'identifiant électroniquement dépasse 1 000 par an ».*

[273] Arrêté du 4 avril 2022 relatif à des moyens d'identification électronique immatériels mis à disposition des professionnels, personnes physiques des secteurs sanitaire, social et médico-social pour l'utilisation des services numériques en santé, JORF n°0087, 13 avril 2022, texte n°18. *« Pro Santé Connect (PSC) est le fédérateur d'identités des professionnels des secteurs sanitaire, médico-social et social enregistrés au Répertoire partagé des professionnels de santé (RPPS). Ce service socle est proposé par l'Agence du numérique en santé (ANS). Il leur offre une manière simple, sécurisée et unifiée de se connecter à tous leurs services numériques en santé, en pouvant passer de l'un à l'autre de manière particulièrement fluide ».*

[274] ANS, *Référentiel d'identification électronique – Acteurs des secteurs sanitaire, médico-social et social [personnes physiques],* PGSSI-S, 2022.



En tout état de cause, même s'il reste une tolérance quant à l'utilisation des moyens d'identification moins élevés jusqu'à ces dates, les services numériques en santé existants devront tout de même garantir un niveau minimal de sécurité quant à l'identification, au risque de devoir être abandonnés. *A minima, « les services sensibles devront […] avoir implémenté l'identification électronique par Pro Santé Connect au 1er janvier 2023 au plus tard »*[275].

Quant aux autres services numériques en santé, ceux-ci n'ont pas l'obligation d'utiliser ces méthodes d'identification, bien qu'il soit recommandé de les appliquer, « *en particulier pour préparer un probable renforcement du niveau de sécurité attendu* »[276].

On constate que dans le cadre de ces référentiels, l'identification et l'authentification sont intimement liées puisque les moyens d'identification exigés permettent également l'authentification[277]. Aussi, grâce à ces moyens, l'identité de la personne est garantie.

B) La preuve de l'intégrité à la création de l'écrit

99. **L'intégrité présumée pour le papier**. *« Historiquement, l'intégrité d'un document est induite par son support. Altérer les informations revient la plupart du temps à altérer leur support, ce qui est le plus souvent visible »*[278]. En effet, toute modification

[275] *Ibid.*
[276] *Ibid.*
[277] Jessica MORALY, et Marie TORELLI, « Référentiel sur l'identification électronique : ce qui change pour la e-santé », *HAAS Avocats*, 2021.
[278] Locarchives, « L'intégrité, un critère central pour instaurer la confiance numérique », 2015. Disponible à l'adresse : https://locarchives.fr/ (consulté le 08/07/2021).

réalisée sur un document papier sera visible (rature, différence d'écriture, changement de stylo etc.), contrairement au support électronique[279]. L'altération d'un document électronique étant plus aisée et moins identifiable que pour le support papier, l'article 1366 du Code civil prévoit expressément la condition d'intégrité, propre à l'écrit numérique afin que celui-ci ait la même force probante que l'écrit papier ; cette condition étant sous-entendue pour l'écrit papier au regard de la nature même du support. Aussi, en cas de remise en cause de l'intégrité du document, celui qui souhaite s'en prévaloir devra démontrer la non-altération du document entre le moment de sa création, et de son utilisation ou de sa production. Or, comment démontrer cette intégrité ?

100. **L'élément majeur de l'intégrité**. Comme vu précédemment, le Code civil ne donne pas beaucoup d'indications permettant de garantir l'intégrité d'un document, sauf s'agissant des documents signés. En effet, une des conditions exigée pour qu'une signature électronique soit avancée ou qualifiée, est qu'elle doit « *être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable* »[280]. Cela implique par principe qu'un document avec l'une de ces signatures permet d'en affirmer son intégrité puisque toute altération serait visible.

Il apparaît que l'élément déterminant de l'intégrité est donc la non-altération d'un document par la détectabilité des éventuelles modifications ultérieures. C'est cette absence de modification qui induit la fiabilité du contenu informationnel du document. On retrouve bien ici deux critères énoncés ci-dessus (sect.1 §2, A, 2) définissant la notion d'intégrité : la stabilité et la traçabilité qui sont des critères complémentaires.

101. **Les moyens et l'intégrité.** L'intégrité d'un écrit passe par la mise en place et l'utilisation de moyens permettant de convaincre le juge, en cas de contestation de l'intégrité de l'écrit, que le contenu qui lui est présenté est en tout point identique à celui produit au moment de sa création. Les critères de stabilité et de traçabilité, bien qu'ayant le même objectif global, c'est-à-dire garantir l'intégrité du document, n'ont pas le même objectif individuel et vont être mis en place par des moyens différents mais complémentaires.

---

[279] Paul-Aymeric LLOAN, « La signature électronique : garantie des exigences légales d'identification », *Village de la justice*, 2019. *« Il est facile de prouver l'intégrité d'un document sur support papier. En effet, un écrit altéré sur support papier laissera des traces visibles à l'œil nu ou par une étude approfondie. En revanche, les documents électroniques sont aisément modifiables à l'insu de tous ».*

[280] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 26.

L'objectif du critère de stabilité, est de figer l'écrit pour qu'il ne puisse pas subir de modifications. Les moyens utilisés pour cela, peuvent se présenter sous plusieurs formes comme le choix du support de l'écrit, ou encore la mise en place d'un scellé sur le document.

Quant au critère de traçabilité, son objectif est de détecter toutes les modifications éventuelles, réalisées sur l'écrit. Pour pouvoir détecter les modifications au fil du temps, il est nécessaire de mettre en place des moyens techniques permettant cette traçabilité et cette détection. Les traces doivent pouvoir démontrer que le contenu du document créé à un instant *t* est bien le même que celui produit à un instant *t+1*. Pour cela, des traces doivent être recueillies au moment de la création du document[281] pour permettre la comparaison ou prouver la non-modification, comme l'apposition d'un horodatage sur le document[282]. Cet horodatage pourra permettre notamment de prouver à quelle date et à quelle heure l'écrit a été créé, lui donnant une date certaine et une antériorité. Cet horodatage permettra également d'identifier la date et l'heure de toute modification survenue ultérieurement sur cet écrit.

Le cumul des moyens de stabilité et de traçabilité est nécessaire pour garantir l'intégrité du document au regard de leur complémentarité.

102. **La signature électronique n'est qu'un moyen**. L'intégrité d'un document peut être démontrée par de nombreux moyens ; la signature électronique n'est que l'un d'entre eux[283]. Un écrit n'a donc pas besoin d'être signé pour être intègre. En revanche, l'avantage de la signature électronique, lorsqu'elle est qualifiée, est que cette intégrité est présumée, contrairement aux autres moyens utilisés.

[281] Raphaël LARSEN, *Traçabilité et intégrité de l'information au sein de systèmes critiques : analyse et proposition de méthodes statistiques, op. cit.*

[282] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 3. L'horodatage électronique est défini comme étant « *des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant* ».

[283] Paul-Aymeric LLOAN, « La signature électronique : garantie des exigences légales d'identification », *op cit.*

Conclusion du chapitre. Depuis une vingtaine d'années, le Droit français reconnaît explicitement une valeur probante à l'écrit natif électronique, dont la force probante est équivalente à celle de l'écrit papier, « *sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* »[284]. Deux critères sont donc nécessaires pour avoir une valeur juridique équivalente à l'écrit papier, critères qu'il est nécessaire d'appréhender sur deux temporalités différentes : au moment de la création de l'écrit, et pendant sa conservation. Cela est nécessaire pour deux raisons :

i. si un document n'a pas de valeur juridique au moment de sa création, il n'en aura pas davantage au moment de sa conservation, même si cette dernière est réalisée conformément à la règlementation et, vice versa, un document peut avoir une valeur juridique à sa création, mais la perdre par la suite.

ii. le choix des moyens mis en place dès la création du document pour permettre l'identification de la personne l'ayant créé et la garantie de son intégrité aura un impact sur la valeur juridique du document.

En effet, il apparaît que l'apposition d'une signature électronique qualifiée permette le respect de ces deux critères simultanément (y compris pour la signature électronique avancée) et que sa fiabilité est présumée impliquant un renversement de la charge de la preuve. Cette signature électronique qualifiée est le moyen le plus fiable de garantir à l'écrit électronique la même force probante que l'écrit papier, d'autant plus qu'elle est obligatoire pour les écrits les plus importants, comme les actes authentiques.

Pour autant, l'utilisation d'autres moyens que la signature qualifiée n'entraîne pas une absence de valeur juridique à l'écrit produit. En revanche, sa fiabilité n'est pas présumée, il sera donc nécessaire de la démontrer en cas de contestation. Aussi, toute personne utilisant ces moyens prend le risque, plus ou moins grand, de voir son écrit dépourvu de valeur juridique.

Pour permettre de donner davantage de valeur juridique à un écrit, qu'il soit signé, ou non, il est possible et recommandé d'établir une convention de preuve[285]. Une convention de preuve est un contrat conclu entre plusieurs parties définissant les règles de preuves entre elles : le mode de preuve admissible, la charge de la preuve etc. Cette convention de preuve permet aux

[284] C. civ., art. 1366.
[285] C. civ., art. 1356.

parties d'aménager les règles sur la preuve lors de leurs relations et permettra notamment d'aider le juge à apprécier la force probante de la preuve présentée en cas de litige entre les parties. Il serait donc possible par exemple, d'établir qu'une identification soit présumée fiable, afin de renverser la charge de la preuve, peu importe le procédé utilisé. Cette présomption ne peut, en revanche être irréfragable, aussi, une preuve contraire pourra toujours être présentée.

Prenons à nouveau l'exemple d'une messagerie MSSanté, la messagerie Mailiz, dont l'opérateur est l'ANS (qui est également gestionnaire de l'espace de confiance MSSanté). Par principe, un mail envoyé, c'est-à-dire un écrit, n'est pas signé, ne permettant pas d'en présumer sa fiabilité. Or, au sein des CGU de la messagerie[286], il est prévu un article intitulé « convention de preuve » prévoyant « *la même valeur probante aux écrits électroniques transmis via la MSSanté qu'aux écrits sur support papier »*[287]. Cela implique par principe, que l'utilisateur de la messagerie reconnaît la fiabilité des écrits envoyés et reçus. En cas de contestation par un utilisateur, ce dernier sera en charge de prouver le manque de fiabilité.

La convention de preuve, semble être un moyen permettant de s'assurer du niveau de fiabilité d'un écrit dès sa création. Cependant, le juge n'est pas lié par une convention de preuve et pourra toujours contester sa validité. Il pourra notamment juger ses clauses abusives si celles-ci créent un déséquilibre entre les parties.

De plus, une convention de preuve ne pourra produire ses effets que si elle est valablement conclue. *« Pour prouver qu'un contrat a été passé, on ne peut pas se référer à une convention de preuve figurant dans ledit contrat, car elle ne pourra produire ses effets que… s'il est prouvé qu'elle a été acceptée : c'est une boucle de raisonnement. Le mécanisme n'a donc d'intérêt que s'il figure dans un premier contrat-cadre dont l'assise probatoire est, quant à elle, d'une solidité incontestable au regard des règles légales »*[288]. A titre d'exemple, signer un contrat avec une signature électronique simple contenant une clause prévoyant que cette signature permet d'établir que l'identité du signataire est garantie n'a pas d'intérêt.

Qu'en est-il du service de messagerie Mailiz ? Il est prévu que *« l'acceptation par les Utilisateurs des présentes conditions générales d'utilisation a pour conséquence la*

[286] M@iliz, « conditions générales d'utilisation du service messagerie sécurisée de la santé Mailiz », 2020. Disponible à l'adresse : https://mailiz.mssante.fr/ (Consulté le 11/04/2021).
[287] *Ibid.*
[288] Emmanuel NETTER, *Numérique et grandes notions du droit privé – la personne, la propriété, le contrat*, Ceprisca, coll. Essais, 2019, pp. 417 à 418.

conclusion d'une convention de preuve au sens de l'article 1368 du code civil »[289]. Or l'acceptation de ces CGU sera réalisée dès la première connexion à la messagerie via le mode de connexion imposée. S'il y a une contestation sur l'identité de la personne titulaire de la messagerie ou sur l'identité de la personne qui s'est connectée pour valider les CGU, la validité de la convention de preuve pourra également être remise en cause.

[289] M@iliz, « conditions générales d'utilisation du service messagerie sécurisée de la santé Mailiz », *op. cit.*

Chapitre 2 : L'écrit en tant que copie

103. **La notion de copie**. Dans le langage courant, une copie est une reproduction à l'identique de quelque chose de tangible que ce soit la copie d'un document, d'un objet particulier ou encore d'un son. Ces copies sont utilisées au quotidien, tant dans la sphère privée que professionnelle. Prenons l'exemple d'une souscription à une assurance voiture en ligne. Pour la conclusion d'un contrat d'assurance, l'assureur doit récupérer un certain nombre de documents de la part du futur assuré, comme son permis de conduire, la carte grise et son relevé d'informations. Ces informations devront être transmises sous forme de copies de ces documents ; copie papier lorsque l'assuré peut les donner directement à l'assureur, soit copie électronique, notamment pour une assurance en ligne. Ces copies sont autant nécessaires pour le client afin qu'il puisse bénéficier d'une assurance personnelle, que pour le professionnel pour conclure le contrat.

Comme on peut le constater, ces copies peuvent prendre plusieurs formes, soit matérielles ou immatérielles grâce à la dématérialisation. L'étude qui nous intéresse ici est la copie d'un écrit, produite sous format électronique.

104. **Les finalités des copies**. Ces copies électroniques sont aujourd'hui omniprésentes et utilisées pour différentes finalités. Soit pour leurs avantages (rapidité du traitement d'envoi de documents et de traitement des demandes), soit pour la réalisation d'un objectif déterminé (la souscription à une assurance), soit parce que leur production est nécessaire (réponse à une condition déterminée ou une obligation légale), voire les trois en même temps. C'est notamment le cas des documents produits par un établissement de santé, et tout particulièrement les documents contenant des données de santé :

i. Un des avantages majeurs de la copie en santé est la possibilité de bénéficier pour chaque patient, d'un dossier patient unique regroupant au même endroit l'intégralité des données le concernant[290]. En effet, l'évolution des technologies depuis les années 2000 a permis la création des dossiers patients informatisés (DPI), impliquant progressivement la fin des anciens dossiers papiers. Pour pouvoir avoir une exhaustivité des données d'un patient dans

[290] Corinne BAUJARD et Iman BEN HAMOUDA, « La gestion du projet à l'Hôpital : dossier patient informatisé et qualité de soins », *Recherches en Sciences de Gestion*, 2015/4, n°109, pp 147-164. *« Aujourd'hui, afin d'accéder aux données médicales du patient et d'améliorer la qualité des soins, le système d'information hospitalier encourage la circulation du dossier patient entre tous les professionnels médicaux dans la prise en charge du patient consultant ou hospitalisé ».*

un dossier informatisé et ne pas avoir à consulter deux dossiers (papier et informatique), une copie de son dossier papier est réalisée afin de l'implémenter dans son dossier unique informatisé. Les anciens dossiers ne sont pas les seuls documents ayant besoin d'être copiés pour que le DPI soit exhaustif. Il y a notamment les documents fournis par le patient tels que les ordonnances des médecins généralistes pour la consultation d'un spécialiste.

ii. Au-delà des avantages, la copie est parfois nécessaire, notamment pour la bonne prise en charge d'un patient ou l'exercice des droits du patient. Le Code de la santé publique prévoit que « *toute personne a accès à l'ensemble des informations concernant sa santé* »[291] en consultation sur place ou par la production d'une copie de ces informations. Un établissement de santé ne peut pas refuser à un patient de lui communiquer par copie ses informations, en revanche, il peut laisser les frais liés à cette copie, à la charge du patient (coût de reproduction et d'envoi).

iii. Des copies peuvent également être faites pour la réalisation d'un objectif déterminé, tel que le gain financier grâce à la destruction des documents originaux. Un dossier médical est « *conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein* »[292] sauf cas particuliers[293]. Cela signifie qu'il y a autant de dossiers médicaux qu'il y a de patients pris en charge par un établissement de santé, et que chaque dossier doit être conservé pour une durée minimale de vingt ans ; le délai courant à compter de la dernière prise en charge du patient. Les dossiers créés en version papier peuvent contenir pour certains plusieurs centaines de pages. Un dossier d'une centaine de pages multiplié par le nombre de dossiers que possède un établissement représente plusieurs kilomètres de dossiers à conserver au sein d'une salle des archives pouvant contenir cette capacité, avec des systèmes de sécurité et de conservation adéquats. La mise en place de dossiers patient 100% dématérialisés grâce à la copie électronique des documents papiers, permet de diminuer, voire d'arrêter l'archivage de

[291] C. santé publ., art. L. 1111-7.
[292] C. santé publ., art. R. 1112-7.
[293] C. santé publ., art. R. 1112-7 : « *Le dossier médical mentionné à l'article R. 1112-2 est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein. Lorsqu'en application des dispositions qui précèdent, la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. Dans tous les cas, si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de dix ans à compter de la date du décès. 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* ».

dossiers patients papiers en les détruisant après reproduction et ainsi ne plus supporter les coûts de cet archivage papier.

105. **La valeur probante de la copie.** Bien que les bénéfices de la copie ne soient plus à démontrer, la question se pose quant à la valeur probante de cette copie. La reconnaissance de la valeur probante de la copie présente deux intérêts :

i. D'une part pour l'établissement, afin qu'il puisse utiliser les copies produites en tant que preuve. En effet, une copie est un écrit à l'instar d'un document original, or se pose la question de la différence de valeur probante entre les deux[294]. Depuis 2016, le Code civil accorde à la copie, la même force probante que l'écrit original, sous réserve qu'elle soit fiable[295]. Aussi, pour que l'établissement ne prenne aucun risque juridique, les copies réalisées doivent être fiables.

ii. D'autre part, cette reconnaissance de la valeur probante profite aux utilisateurs finaux de la copie, et notamment aux professionnels de santé. Comme pour l'écrit natif électronique, les professionnels utilisent les écrits comme base pour la prise en charge du patient. Ils doivent pouvoir avoir une confiance absolue en leur contenu.

Dès lors que le critère de fiabilité imposé par le Code civil est respecté et donc la valeur juridique de la copie garantie, le professionnel de santé peut naturellement avoir confiance en la copie.

Pour garantir la valeur juridique de la copie, il est nécessaire de déterminer les conditions juridiques à respecter (section 1) afin de pouvoir préparer la mise en place d'un processus de dématérialisation adapté aux besoins et aux attentes de l'établissement de santé (section 2).

[294] Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *op. cit.*
[295] C. civ., art. 1379.

Section 1 : La valeur juridique de la copie

106. **L'évolution de la place de la copie en tant que preuve.** La reconnaissance de la valeur juridique de la copie d'un document, c'est-à-dire toute *« reproduction manuscrite, mécanique ou électronique d'un contrat ou d'un document quelconque »*[296] ou encore une « *reproduction fidèle »*[297], a été introduite dès 1804. En revanche sa force probante était moindre par rapport à l'écrit original puisque la valeur probante d'un écrit, lorsque l'écrit original n'existait plus, était limitée. Elle était reconnue en tant que preuve, pour les actes ayant une valeur supérieure aux actes sous seing privé, comme la grosse[298]. Il a fallu attendre la Loi de 1980[299] pour qu'elle puisse être reconnue en tant que preuve par un créancier. L'ancien article 1348[300] prévoyait une exception à la règle, permettant d'accorder davantage de valeur à la copie, même en l'absence du document original sous réserve qu'elle en soit une « *reproduction non seulement fidèle mais aussi durable »*[301].

L'Ordonnance de 2016 portant réforme notamment sur la preuve des obligations a unifié le régime juridique de la copie en ne laissant plus aucun doute sur la place et la valeur juridique de la copie en affirmant textuellement que *« la copie fiable a la même force probante que l'original »*[302]. Il apparaît à la lecture de cet article, qu'une copie peut avoir la même valeur juridique devant un juge qu'un écrit original, lui conférant *« un statut probatoire sérieux »*[303], et donc lui permettant de se substituer à ce dernier. En revanche, pour que la copie ait la même force probante que l'original, la copie doit respecter un critère primordial, être fiable.

107. **La fiabilité comme seul critère.** La fiabilité est le seul critère énoncé par le Code civil permettant de déterminer *in fine* si la copie réalisée bénéficie de la même force probante que l'original. Cette notion de fiabilité n'est pas nouvelle puisqu'elle est également utilisée pour la signature électronique : *« lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle*

---

296 Serge BRAUDO, *Dictionnaire du droit privé,* disponible à l'adresse : https://www.dictionnaire-juridique.com/ (consulté le 26/03/2021).
297 TLFi, *V° « copie »*, subst. fém.
298 Serge BRAUDO, *Dictionnaire du droit privé,* disponible à l'adresse : https://www.dictionnaire-juridique.com/ (consulté le 26/09/2022). *« La "grosse" était naguère le nom donné à la copie d'une décision de justice ou d'un acte notarié comportant la formule exécutoire. Dans le Code des procédures civiles d'exécution cette appellation a été remplacée par celle de Titre exécutoire ».*
299 Loi n°80-525 du 12 juillet 1980, v.init., art. 7.
300 C. civ., art. 1348 version en vigueur du 13 juillet 1980 (Loi n° 80-525 du 12 juillet 1980) au 01 octobre 2016.
301 *Ibid.*
302 C. civ., art. 1379 al. 1.
303 Emmanuel PIERRAT, « La validité juridique des copies numériques », *lagbd*, 2017.

s'attache »[304]. Pour autant, il apparaît que la mise en œuvre de ce critère sera différente selon l'objet de la fiabilité. En l'espèce, il s'agit du procédé d'identification utilisé, alors que pour la copie, son application ne semble pas se restreindre à un procédé. Pour pouvoir appliquer cette notion à la copie, il est nécessaire de déterminer ce qu'elle implique (§1) afin de pouvoir la mettre en œuvre et garantir sa fiabilité devant un juge (§2).

§1 L'appréciation du critère de fiabilité de la copie

108. **L'évolution des critères d'appréciation de la copie.** L'Ordonnance de 2016, en plus d'affirmer la valeur juridique de la copie équivalente à l'écrit original est également venue modifier les critères permettant de garantir cette valeur, en passant des critères de fidélité et durabilité au critère de fiabilité.

Ce nouveau critère pose des difficultés dans son application au regard de son caractère subjectif laissant ainsi une grande marge d'appréciation quant à son application.

Les critères de fidélité et durabilité bien que retirés de la nouvelle rédaction de l'article 1367 du Code civil semblent pour autant toujours applicables (A) et permettent d'appréhender ce nouveau critère de fiabilité et le rendre davantage objectif (B).

A) L'ancêtre de la fiabilité : la fidélité et la durabilité

109. **La copie avant 2016**. La véritable reconnaissance de la copie en tant que preuve a été introduite à partir de 1980 par l'ancien article 1348 alinéa 2 du Code civil qui prévoyait qu'en cas de perte d'un titre original par la partie qui souhaite s'en prévaloir, celle-ci peut présenter en tant que preuve *« une copie qui en est la reproduction non seulement fidèle mais aussi durable »* [305]. Seuls ces deux critères permettaient de déterminer la valeur probante de la copie mais en aucun cas sa force probante.

Les juges ont pu interpréter largement la valeur juridique, en affirmant qu'une « *reproduction fidèle et durable […] ne constituait pas un commencement de preuve par écrit, mais faisait pleinement la preuve de l'existence du contrat* »[306]. Cette position permet d'accorder une haute valeur probante à la copie, sans pour autant la mettre sur le même pied d'égalité que

[304] C. civ., art. 1367.
[305] C. civ., art. 1348 version en vigueur du 13 juillet 1980 (Loi n° 80-525 du 12 juillet 1980) au 01 octobre 2016.
[306] Cass. Civ. 1ère, 25 juin 1996, 94-11.745, Publié au bulletin.

l'original puisque la production d'une copie fidèle et durable n'était possible que sous réserve de n'avoir pas conservé le titre original.

110. **La notion de fidélité.** Le Code civil n'a pas défini la notion de fidélité laissant une marge d'appréciation de ce critère. La fidélité peut être définie comme la « *qualité de ce qui est conforme à la réalité, à un modèle, à un original* »[307] impliquant que la copie devait être la reproduction exacte du document d'origine. Se pose la question de ce qui devait être fidèle, est-ce simplement le contenu informationnel de l'écrit ou également son apparence. Certains auteurs ont estimé que la copie fidèle est celle « *faite sans la moindre retouche, et qui ainsi ne trahit pas la vérité contenue dans l'original. A partir de là, peu importe qu'il n'y ait pas une identité absolue d'apparence : la pagination, la couleur des feuilles, les dimensions peuvent varier* »[308]. La fidélité ne s'appliquerait qu'au contenu informationnel de la copie.

La deuxième chambre civile de la Cour de cassation a rendu un arrêt le 4 décembre 2008[309] cassant un arrêt rendu par la cour d'appel de Reims, dont un des motifs était « *que la Cour d'appel a constaté que le document litigieux présenté par la Caisse, qui ne comportait pas la signature de son auteur, comme la copie d'un courrier d'information prétendument envoyé par la CPAM de la MARNE le 20 janvier 2003 avait été « édité sur un papier à en-tête revêtu d'un logo diffusé en 2004 » ; qu'en ne tirant pas les conséquences de cette constatation dont il résultait que le document n'était pas une copie fidèle du prétendu courrier d'information original, la Cour d'appel a violé les articles 1334 et 1348 du Code civil* »[310]. La fidélité du document a été remise en cause d'une part, par l'absence de la signature de son auteur qui devait être présente sur le courrier original, et d'autre part, par l'impression de ce courrier d'information sur du papier à entête datant d'après l'envoi de ce courrier. Ces deux éléments ont permis d'attester que la copie n'était pas fidèle au document original, car celle-ci ne pouvait pas garantir que la copie produite était de la même teneur que le document envoyé[311].

Cet arrêt a notamment permis de reconnaître la possibilité d'utiliser une copie électronique en tant que preuve dès lors que l'original n'existait plus, sous réserve que cette copie soit fidèle et durable.

---

[307] TLFi, *V° « fidélité »*, subst. fém.
[308] Eric GARAUD, « Quelle valeur accorder à la copie fidèle et durable... d'un écrit imparfait ? », *Dalloz* , 2013, n°15, p-1041.
[309] Cass. Civ. 2ème, 4 décembre 2008, 07-17.622, Publié au bulletin.
[310] *Ibid.*
[311] Isabelle RENARD et Jean-Marc RIETSCH, *Aide-mémoire de droit à l'usage des responsables informatique,* Dunod, 2012.

111. **La notion de durabilité.** Contrairement à la notion de fidélité, la notion de durabilité a été définie par le Code civil : *« Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support »*[312]. *« La formule* [était] *volontairement imprécise pour permettre l'élargissement à toute nouvelle technique de reproduction qui apparaîtrait »*[313]. Cette définition implique donc que la copie devait être une reproduction ne permettant pas l'effacement dans le temps de son contenu notamment grâce au choix du support utilisé. Dans le cas contraire, la copie pourrait ne plus être fidèle à l'original.

La durabilité de la copie fait écho au sujet de la conservation de la copie bien que cela ne soit pas clairement exprimé. En effet, une copie pour être valable doit être fidèle à l'original, cette fidélité doit pouvoir être démontrée dans le temps, notamment pour garantir qu'aucun effacement n'ait eu lieu. L'indélébilité de la copie doit donc s'apprécier dans le temps.

B) Le nouveau critère : la fiabilité

112. **L'absence de définition du critère de fiabilité**. Les critères de fidélité et de durabilité ont laissé la place depuis l'Ordonnance de 2016, au critère de fiabilité. Celui-ci, introduit dès la première phrase du premier alinéa de l'article 1379 du Code civil n'est pas expressément défini laissant une grande marge d'appréciation au juge pour son application. Cette appréciation est quant à elle explicitement prévue dès la seconde ligne : « *la fiabilité est laissée à l'appréciation du juge »*[314] rendant l'interprétation et l'application de ce critère totalement subjective[315]. Or, un des objectifs de la copie est de pouvoir détruire les originaux tout en s'assurant de la valeur probante des copies produites en amont. Mais si l'interprétation et l'application de ce critère sont subjectives et dépendantes du juge, se prémunir d'une copie fiable semble difficile à assurer sans le définir et déterminer son objectif principal.

113. **La fiabilité regroupant le critère de fidélité et de durabilité**. La doctrine tend à dire que *« copie fidèle + copie durable = copie fiable »*[316]. La fiabilité de la copie serait l'accumulation des deux anciens critères énoncés par le Code civil décomposée comme suit : « *Le processus FI-ABLE est composé d'une première partie qui consiste à créer un processus de production d'une copie FIdéle. Mais à quoi pourrait servir la fidélité seule ? C'est en*

[312] C. civ., art. 1348 version en vigueur du 13 juillet 1980 (Loi n° 80-525 du 12 juillet 1980) au 01 octobre 2016.
[313] Frédérique FERRAND, « Preuve », *op. cit.*
[314] C. civ., art. 1379.
[315] Cass. civ. 1re, 30 mai 2000, n° 98-16519.
[316] ScanCenter, *Quelles sont les différences entre une copie fidèle et une copie fiable ?*, janvier 2020. Disponible à l'adresse : https://www.scancenter.fr/ (consulté le 25/07/2021).

ajoutant un processus de conservation de la copie fidèle qu'il est possible de créer une copie durABLE. Ainsi la fiabilité repose sur une copie fidèle et durable c'est-à-dire intègre et conserver dans un Système d'Archivage électronique capable d'assumer la pérennité et la sécurité de la copie numérique »[317]. Cette analyse est confirmée par le rapport au président de la République concernant l'ordonnance du 10 février 2016 venant donner des précisions sur le critère de fiabilité à appliquer au moment de la reproduction de la copie et pendant sa conservation. *« La fiabilité d'une copie s'entend des qualités de fidélité à l'original d'une part, et de durabilité dans le temps d'autre part »* [318]. En revanche on constate que le critère de fiabilité est envisagé sur deux plans : la copie elle-même doit être fiable à l'original, mais pour pouvoir l'être, le processus utilisé semble également jouer un rôle sur sa fiabilité.

Bien qu'aucune définition de la fiabilité ne soit définie par l'article 1379 du Code civil, *« le deuxième alinéa du texte présume fiable jusqu'à preuve du contraire, la copie simple résultant d'une reproduction à l'identique de la forme et du contenu de l'acte (critère de fidélité à l'original) et dont l'intégrité est garantie dans le temps (critère de durabilité). Les caractéristiques techniques des procédés utilisés, destinés à garantir la fidélité à l'original et la durabilité de la copie, et entraînant le bénéfice de cette présomption, seront définies par décret en Conseil d'état »*[319]. Cela implique d'une part que pour être fiable, la copie doit être une reproduction fidèle de l'original c'est-à-dire une reproduction à l'identique de la forme et du contenu de l'acte et que cette copie doit être durable dans le temps. De plus, l'application de ce critère ne se limite pas seulement au seul résultat de la copie, mais concerne également le processus mis en place pour la reproduction, au moins pour que la copie soit présumée fiable.

114. **Les raisons de l'évolution des critères**. Aucune différence majeure n'apparaît clairement quant à la différence entre les anciens et le nouveau critère, d'autant que pour définir et appliquer le critère de fiabilité, on se base sur les anciens critères. Pour autant, l'évolution était nécessaire pour deux raisons :

i. L'ancien article 1348 du Code civil était rédigé de telle sorte que le support utilisé de la copie n'était pas mentionné laissant la place à des modes de preuves écrits pouvant être présentés sur d'autres supports que le papier tels que les microfilms. En revanche, depuis 1980, l'évolution technologique exponentielle et la multiplication des procédés de

[317] Christian DUBOURG, « Copie fidèle + copie durable = copie fiable », *spark archives*, 2017.
[318] Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[319] *Ibid.*

reproduction ont très rapidement montré les limites de l'application de ces critères, bien que les juges aient continué à admettre des copies produites sous forme électronique[320]. A titre d'exemple, il est impossible aujourd'hui, d'exiger d'une copie sur support électronique, qu'elle soit durable, c'est-à-dire une « *reproduction indélébile de l'original qui entraîne une modification irréversible du support* »[321]. Le critère de durabilité est toujours appliqué, car induit dans la fiabilité mais cette absence de définition permet de prendre en compte l'évolution informatique.

ii. De plus, *« la différence rédactionnelle entre la copie fidèle et durable et la copie fiable induit une différence technique soulignée par le décret d'application »*[322] tant quant aux garanties à mettre en place lors du processus de reproduction, que pendant la conservation de la copie. Ces processus techniques n'étaient pas envisagés par l'ancien article or, au regard des évolutions croissantes des technologies et des compétences humaines, des critères techniques doivent être mis en place pour garantir la fiabilité de la copie.

§2 La garantie de la fiabilité devant le juge

115. **La définition du critère de fiabilité**. L'appréciation du critère de fiabilité a permis de déterminer ce qui est attendu d'une copie fiable, afin que celle-ci puisse avoir la même force probante qu'un document original. En revanche, la notion même de fiabilité n'est pas définie. Dans le langage courant, le mot fiable est défini comme quelqu'un ou quelque chose « *en qui ou en quoi on peut avoir toute confiance, auquel on peut se fier* »[323], *« qui est digne de confiance »*[324]. La copie bénéficiera donc d'une valeur juridique dès lors que toute personne peut lui faire confiance. Mais quel est l'objet de cette confiance ? A l'instar de l'écrit natif électronique, ce qui compte est la confiance que l'on peut avoir envers le contenu informationnel du document. En effet, c'est le contenu du document qui permettra d'être utilisé comme preuve. Or pour pouvoir se fier au contenu, il faut également pouvoir s'assurer qu'une altération du contenu n'ait pas eu lieu pendant la réalisation de la copie, ou ne puisse avoir lieu par la suite, au regard du support de reproduction choisi ou des modalités de sa conservation. La fiabilité s'étend donc au-delà même du contenu de l'écrit comme cela a pu être démontré précédemment.

[320] Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *op. cit. « Les techniques de reproduction et de numérisation ne pouvaient rester en l'état et la modification du code civil répond à une nécessité »*.
[321] C. civ., art. 1348 version en vigueur du 13 juillet 1980 (Loi n° 80-525 du 12 juillet 1980) au 01 octobre 2016.
[322] Polyanna BIGLE, « Quand la numérisation de document intègre le droit français », *Lexing*, 2017.
[323] Le Robert, *V° « fiable »*, adj.
[324] TLFi, *V° « fiable »*, adj.

116. **Le niveau de fiabilité.** L'article 1379 du Code civil prévoit expressément trois niveaux de fiabilité de la copie : la simple copie fiable, la copie réputée fiable, et la copie présumée fiable. Ces niveaux de fiabilité permettent de déterminer le degré de confiance qu'une personne, notamment un juge peut avoir envers une copie mais également le degré de confiance qu'accorde le Droit à la copie (A). Bien que trois niveaux soient envisagés, seulement deux seront réellement applicables pour les documents contenant des données de santé. En outre, la copie présumée fiable donne de nombreuses indications permettant de déterminer ce qui est attendu du procédé de reproduction à mettre en place (B).

A) Les trois niveaux de fiabilité définis par les textes

117. **La confiance accordée envers la copie par le Droit**. Les trois niveaux de fiabilité énoncés par l'article 1379 du Code civil permettent de déterminer le niveau de confiance qui peut être accordé à la copie se traduisant en Droit par le mode de preuve à apporter pour contester la fiabilité d'une copie, ou encore la charge de la preuve.

118. **La copie réputée fiable[325].** Le plus haut niveau de fiabilité est la copie réputée fiable. « *Est réputée fiable la copie exécutoire ou authentique d'un écrit authentique* »[326]. Le Code civil prévoit une présomption irréfragable de la copie exécutoire ou authentique, d'un acte lui-même authentique, c'est-à-dire « *celui qui a été reçu, avec les solennités requises, par un officier public ayant compétence et qualité pour l'instrumenter* »[327], tel que l'acte réalisé par un notaire. A ce titre, cette copie est une preuve incontestable. Cette preuve est irréfragable « *en raison de l'auteur de cette copie »*[328]. Ce type de copie n'est pas le mode le plus répandu de preuve, au regard de la spécificité du document original et de la copie qui doivent tous deux être authentiques. Au sein des établissements de santé, les documents produits ne sont pas des actes authentiques ; la copie ne pourra pas l'être non plus. Les copies des documents ne bénéficient donc pas d'une présomption irréfragable.

119. **La copie fiable dans les établissements de santé.** Au sein des établissements de santé, seules les copies présumées fiables et/ou simplement fiables sont envisagées. Comme vu précédemment, savoir si une copie bénéficie de la présomption de fiabilité, se détermine au moment même de la réalisation de la copie et pendant toute sa conservation (la

[325] Alexandra BERG-MOUSSA et Mahasti RAZAVI, « Publication de l'ordonnance portant réforme du droit des contrats », *AD article*, 2016.
[326] C. civ., art. 1379.
[327] C. civ., art. 1369.
[328] Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

conservation sera envisagée dans le titre 2 de la partie 1). Les procédés organisationnels et techniques mis en place pour réaliser la copie permettront de déterminer le niveau de fiabilité à accorder à la copie et donc la charge de la preuve en cas de contestation.

120. **La copie fiable.** La simple copie fiable est le plus bas niveau de fiabilité accordé par le Code civil. En cas de contestation de la fiabilité d'une simple copie fiable, celui qui souhaite s'en prévaloir doit apporter la preuve de sa fiabilité qui sera appréciée *in fine* par le juge. Il faut donc emporter la conviction du juge, sa confiance. Or aucune indication n'est donnée par le Code civil pour garantir la fiabilité simple de la copie. Cette absence d'indication permet de pouvoir prouver la fiabilité de la copie par tout moyen sans avoir nécessairement à remplir certaines conditions. En revanche, cette largesse entraîne une insécurité juridique puisque l'appréciation de la fiabilité de la copie et des preuves apportées pour prouver la fiabilité, sera faite par le juge. Il existe donc un risque de voir sa copie reléguée au rang de commencement de preuve par écrit.

121. **La présomption simple de fiabilité.** Pour finir, les copies peuvent bénéficier d'une présomption simple de fiabilité, sous réserve de respecter certaines conditions[329]. Cette présomption implique qu'une partie contestant la fiabilité d'un acte doit en apporter la preuve contraire, à l'inverse de la simple copie fiable. Le Code civil, à l'instar de la signature électronique, prévoit expressément les conditions à respecter pour qu'une copie soit présumée fiable. Celle-ci doit résulter « *d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'État* »[330]. Il apparaît que pour qu'une copie soit présumée fiable, celle-ci doit être une reproduction identique de la forme et du contenu de l'écrit original. Ce critère n'est pas nouveau puisque déjà présent auparavant avec le critère de fidélité. En revanche, ce qui est nouveau est la mention d'un procédé, défini par Décret, permettant de garantir l'intégrité du document dans le temps, tant au moment de sa création par l'utilisation d'un procédé de reproduction, que pendant sa conservation, et qui aura un impact pour déterminer la fiabilité de la copie.

Le Décret fait une distinction selon la nature du procédé utilisé pour la réalisation de la copie : la reproduction par voie électronique ou la reproduction par un procédé entraînant « *une modification irréversible du support de la copie* »[331]. Ce dernier fait écho à une des

[329] Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *op. cit.*
[330] C. civ., art. 1379.
[331] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article

anciennes[332] conditions devant être respectées pour pouvoir utiliser une copie en tant que preuve, la durabilité de la copie. On constate que les conditions de fiabilité des copies réalisées par un autre procédé que par voie électronique sont expressément les mêmes que les anciennes dispositions de l'article 1348 ; la copie pour être fiable doit être fidèle et durable, ni plus, ni moins.

Or il apparaît que ces seuls critères ne sont plus suffisants pour les copies réalisées par un procédé électronique bien que jusqu'en 2016, ils aient servi de base pour en admettre la valeur juridique[333]. En effet, « *l'évolution des technologies impliquant une conception plus large de l'écrit qui ne se matérialise plus nécessairement sur papier, et consécutivement une multiplication des techniques de reproduction, le régime juridique de la copie devait impérativement être revu* »[334]. Aussi, des conditions spécifiques doivent être remplies dès lors qu'une reproduction a lieu avec un procédé électronique.

B) La reproduction électronique présumée fiable

122. **La garantie de l'intégrité sur deux temporalités**. Dès lors qu'une reproduction a lieu par voie électronique, huit conditions doivent être respectées afin que la copie en résultant soit présumée fiable. Ces conditions peuvent être scindées en deux temporalités : au moment de la création de la copie et pendant sa durée de conservation à l'instar de l'écrit natif numérique[335].

123. **La fiabilité à la création de la copie**. Sur ces huit conditions, cinq d'entre elles sont à mettre en œuvre au moment de la création de la copie :

i. Le procédé utilisé pour la production de la copie doit « *produire des informations liées à la copie et destinées à l'identification de celle-ci* »[336]. Une liste exhaustive des informations attendues n'est pas communiquée, mais il doit y avoir *a minima* « *le contexte de la numérisation, en particulier la date de création de la copie* »[337]. Ces informations sont des métadonnées, c'est-à-dire des données « *servant à caractériser une autre donnée, physique ou*

1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 1.
[332] C. civ., art. 1348 version en vigueur du 13 juillet 1980 (Loi n° 80-525 du 12 juillet 1980) au 01 octobre 2016.
[333] Cass. Civ. 2ème, 4 décembre 2008, 07-17.622, Publié au bulletin
[334] Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[335] Comme pour l'écrit natif numérique, les modalités de conservation seront traitées dans le titre 2 de la partie 1.
[336] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 2.
[337] *Ibid.*

numérique »[338]. Le choix des métadonnées à produire est libre mais doit permettre de garantir la fiabilité de la copie produite mais également la valeur du document en tant que preuve. En effet, nous avons vu que la personne dont émane un document doit être identifiée afin que ce dernier puisse avoir une valeur juridique et que cette identification n'est pas forcément faite par l'apposition d'une signature mais par des données non visibles sur le document. Donc, en cas de reproduction d'un document numérique dépourvu de signature, il est nécessaire de réunir les métadonnées relatives au document d'origine notamment pour pouvoir identifier son auteur[339].

ii. *« La qualité du procédé doit être établie par des tests sur des documents similaires à ceux reproduits et vérifiée par des contrôles »*[340] permettant de garantir que toutes les copies réalisées, peu importe les spécificités du document d'origine et le moment de la réalisation des copies, sont identiques à l'original. La qualité du procédé doit être vérifiée en deux temps, avant et après la reproduction.

D'une part, le procédé utilisé doit être testé en amont afin de vérifier que tous les types de documents copiés le soient de manière fiable. A titre d'exemple, il est apparu que des mentions écrites en stylo bille vert[341] pouvaient être très peu, voire non visible après reproduction au scanner ou sous certaines résolutions. D'autre part, au fil de l'utilisation du procédé choisi, il est nécessaire de s'assurer qu'il n'y ait aucune baisse de la qualité de la copie, par le dérèglement d'un paramètre.

iii. La copie doit être *« attestée par une empreinte électronique qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable »*[342]. A l'instar de la signature électronique, le Décret donne des indications quant à l'application de ce critère notamment pour que le procédé utilisé soit présumé fiable. *« Cette condition est présumée remplie par l'usage d'un horodatage qualifié, d'un cachet électronique qualifié ou d'une signature électronique qualifiée »*[343] conformément au Règlement eIDAS. On constate ici une difficulté supplémentaire dans la mise en œuvre de ce critère. Autant, les quatre autres critères sont rédigés de telle sorte que leur application soit libre et pas trop orientée, autant, ce

[338] Larousse, *V° « métadonnées »*, nom fém.
[339] Olivier LE DEUFF, « Contrôle des métadonnées et contrôle de soi », *Etudes de communication*, 2011/1, n°36, pp. 23-38.
[340] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 2.
[341] Retour d'expérience constaté au sein d'un l'institut de cancérologie de Lorraine lors de la dématérialisation de leurs dossiers patients.
[342] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 3.
[343] *Ibid.*

dernier critère implique l'utilisation de dispositifs spécifiques, dont la non-utilisation implique des conséquences sur la preuve de leur fiabilité et notamment sur la charge de la preuve. Il y a donc ici des conditions en cascade à satisfaire pour bénéficier d'une présomption de fiabilité pour la copie.

iv. Des « *mesures de sécurité appropriées* »[344] quant à l'accès aux différents dispositifs de reproduction doivent être mises en place. Ces mesures permettent de garantir qu'aucune altération, qu'elle soit volontaire ou involontaire ne puisse avoir lieu tant au niveau des documents (copies et originaux) qu'au niveau du matériel lui-même. Prenons l'exemple d'un dispositif mis à disposition d'une entreprise pour la dématérialisation en masse de documents papiers. Ce dispositif doit pouvoir être accessible aux seules personnes autorisées et habilitées afin qu'aucune erreur, volontaire ou non, ne vienne dérégler le dispositif, ce qui pourrait entraîner une altération du contenu des documents.

v. Tous les dispositifs et mesures nécessaires mis en place pour la reproduction d'originaux doivent être décrits au sein d'une documentation[345]. Cette documentation sert à décrire le processus de dématérialisation choisi par l'établissement. Il décrit notamment les types de dispositifs utilisés avec leur caractéristiques, les mesures de sécurité permettant de garantir la fiabilité du processus et des dispositifs, le processus humain mis en place pour réaliser la dématérialisation (réalisation en interne par la structure, ou externalisation) etc. Cette documentation permet de démontrer, au moins théoriquement, le respect des impératifs exigés par la Loi ou par la pratique.

124. **Une présomption de fiabilité difficile à mettre en œuvre**. On le voit déjà au moment de la création de la copie, ces exigences cumulatives peuvent être très difficiles à mettre en œuvre. *« Les exigences en matière de copie numérique sont […] nombreuses et nécessitent l'application de technologies sûres. Les contraintes posées ne doivent* [pour autant] *pas occulter les nombreux avantages que peut présenter la copie électronique »*[346]. De plus, à l'instar de la fiabilité présumée de la signature électronique qualifiée, ce n'est pas parce qu'une copie ne respecte pas les conditions énoncées par l'article 1379 du Code civil et de son Décret d'application, que celle-ci est dépourvue de valeur probante. La copie sera une

[344] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 6.
[345] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 7.
[346] Gérard HAAS et Jean-Philippe SOUYRIS, « Qu'est-ce qu'une copie numérique fiable ? », *HAAS avocats*, 2017.

simple copie fiable en renversant la charge de la preuve, ou un commencement de preuve par écrit.

Même si ces conditions sont difficiles à mettre en œuvre, elles permettent de donner des indications sur ce qui est attendu notamment en termes de mesures de sécurité, pour garantir la fiabilité de la copie. Afin de pouvoir prouver la fiabilité de la copie simplement fiable, il est intéressant de s'inspirer de ce Décret.

Section 2 : La préparation à la mise en place d'un processus de dématérialisation

125. **Une conception large de la copie.** L'article 1379 est écrit de telle sorte qu'aucune mention de format, que ce soit pour l'original ou la copie ne soit envisagé. Cela implique que le document original peut se présenter sur différents support (papier, électronique etc.) et que le support de la copie peut être dématérialisé ou non, sous réserve que cette copie soit fiable. Il est donc envisagé la copie papier d'un document papier, que ce soit par voie électronique ou non, la copie électronique d'un document électronique ou encore, la copie électronique d'un document papier, qui est aujourd'hui le nerf de la guerre car il présente le plus de risque pour un établissement. En effet, la dématérialisation d'un document papier entraîne par bien des façons, la possibilité de faire perdre la valeur juridique de la copie. Pour autant, c'est une pratique extrêmement répandue, notamment dans les établissements de santé, au regard des enjeux.

126. **L'enjeu majeur de la copie**. Les enjeux de la dématérialisation pour les établissements de santé sont multiples, dont un des principaux, est de pouvoir dématérialiser les documents papiers et notamment les documents contenant des données de santé concernant un patient. Cette dématérialisation permettra d'une part, d'implémenter le DPI du patient, afin d'avoir un seul et même dossier pour chaque patient avec toutes ses données, permettant sa bonne prise en charge et d'autre part de pouvoir archiver les données exclusivement ou presque, de manière informatique, permettant de détruire *in fine* les archives papiers[347].

127. **La copie de documents contenant des données de santé.** La question se pose quant à l'application des règles du Code civil. L'article L. 1111-25 du Code de la santé publique prévoit que la copie d'un document comportant des données de santé à caractère personnel doit remplir *« les conditions de fiabilité prévues par le deuxième alinéa de l'article 1379 du code civil »*[348] afin de bénéficier de la même force probante que le document original papier. Le Code de la santé publique se base sur les critères énoncés par le Code civil pour déterminer si une copie contenant des données de santé est fiable, malgré la typologie particulière de ces documents.

[347] Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *op. cit. « Comme le souligne le rapport au président de la République, la destruction des originaux papier est désormais consacrée ».*
[348] C. santé publ., art L. 1111-26.

128. **La mise en place d'un processus de dématérialisation**. Comme on a pu le voir, la réalisation de copie fiable passe tout d'abord par son procédé, qui doit garantir une reproduction identique à l'acte copié. Pour déterminer le procédé de reproduction à mettre en place, qui ne se limite pas qu'à des procédés techniques, il est nécessaire de définir au préalable le niveau de fiabilité devant être accordé au document (§1) ainsi que l'organisation que souhaite mettre en place l'établissement pour réaliser cette reproduction (§2). Cette analyse préalable et ces choix vont permettre à l'établissement de santé d'établir un processus de dématérialisation décrivant les étapes de reproduction des documents. Autant l'analyse que le processus se doivent d'être documentés afin de pouvoir prouver la fiabilité les copies réalisées.

§1 La valeur des copies numériques pour l'établissement de santé

129. **Une présomption de fiabilité toujours nécessaire ?** Le Code civil et son Décret d'application prévoient des conditions, notamment techniques à respecter afin que la copie soit présumée fiable jusqu'à preuve du contraire, impliquant un processus pouvant être lourd à mettre en place. Or, les documents produits au sein d'un établissement de santé n'ont pas tous la même valeur probatoire. Certains n'ont pas vocation à être utilisés en cas de contentieux ; d'autres auront une valeur plus ou moins importante selon leur contenu, ou encore leur utilité. Il n'est donc pas toujours pertinent, ni même possible, pour un établissement de santé, de respecter les conditions permettant de présumer de la fiabilité d'un document ; une fiabilité simple pouvant suffire.

130. **Une classification des documents.** Pour déterminer le niveau de fiabilité à appliquer à un document, il est nécessaire de s'interroger au préalable sur l'objectif premier du document (A) afin d'en déterminer son niveau d'importance et sa valeur permettant de le classifier (B) et ainsi définir les moyens à déployer et à mettre en place pour la réalisation de sa dématérialisation.

A) L'objectif principal des documents

131. **La notion de document.** Un document est couramment défini comme étant une « *pièce écrite servant d'information ou de preuve* »[349], indépendamment de son support. Qu'il soit réalisé sur support papier ou sur support numérique, la caractéristique du document est de pouvoir mettre par écrit des éléments servant à plusieurs usages. La définition de

[349] TLFi, *V° « document »*, subst. masc.

l'usage du document en tant qu'information ou preuve est quant à elle très limitative. L'objectif de chaque document peut être plus large.

132. **L'objectif principal du document.** Un document est produit pour une utilité qui est propre à son auteur et à ses besoins, notamment en santé tels que :

i. La transmission d'une information : un document peut être rédigé afin de transmettre une information à une autre personne. Il peut permettre de transmettre toutes les informations relatives à la prise en charge d'un patient, soit à un autre professionnel prenant également en charge le patient, ou au patient lui-même. Cette information peut également être une exigence imposée par la Loi. A titre d'exemple, en cas d'échange et de partage d'informations de données de santé, entre un professionnel de santé et un non-professionnel de santé, une information préalable doit être communiquée au patient. Cette information[350] doit obligatoirement être remise sur un support écrit[351].

ii. La manifestation de la volonté : un document écrit peut permettre de manifester la volonté de quelqu'un. Une personne majeure peut rédiger des directives anticipées permettant d'exprimer sa volonté *« relative à sa fin de vie en ce qui concerne les conditions de la poursuite, de la limitation, de l'arrêt ou du refus de traitement ou d'acte médicaux »*[352].

iii. Un aide-mémoire : Un document peut être rédigé par une personne, en tant qu'aide-mémoire ou de pense bête, permettant ainsi de ne pas oublier ce qui a traversé son esprit. Une assistante médicale peut inscrire sur un papier un mémo permettant de lui rappeler d'appeler Madame X, afin de décaler son rendez-vous.

133. **L'usage effectif du document.** Quand une personne rédige un document, par exemple un médecin, celui-ci le rédige avec un objectif précis :

Soit parce que sa rédaction et ses usages sont prédéfinis par les textes. Prenons l'exemple du certificat de décès dont les objectifs sont multiples et différents selon la personne : Un certificat doit être rédigé par un médecin pour chaque décès afin d'attester le décès d'une personne. Ce certificat permettra, à la famille du défunt de réaliser les différentes obligations

[350] Céline DUCHENE, « Question du secret partagé », *Encyclopédie des collectivités locales*, 2020. L'information comprend notamment pour la personne *« son droit d'exercer une opposition à l'échange et au partage d'informations la concernant et elle peut exercer ce droit à tout moment. Cette information est attestée par la remise, par le professionnel qui a recueilli le consentement, d'un écrit reprenant cette information ».*
[351] C. santé publ., art. D. 1110-3-2.
[352] C. santé publ., art. L. 1111-11.

administratives inhérentes au décès et, à la l'officier d'état civil chargé de fermer le cercueil, de procéder à sa fermeture[353].

Soit, bien que le document ait été rédigé dans un but précis, il pourra être utilisé à d'autres fins. Lorsqu'un médecin généraliste demande l'avis d'un médecin spécialiste afin d'apporter un diagnostic médical, ce dernier lui fournit un compte-rendu. Sur la base de ce compte-rendu le médecin généraliste pourra prendre en charge le patient selon le diagnostic établi. L'utilité de ce compte-rendu va au-delà de cela, en permettant à ces médecins de l'utiliser en tant que preuve en cas d'erreur de diagnostic par exemple. Pour autant, cet usage n'était pas le but premier du document établi.

134. **Les conséquences de l'usage du document.** Le contenu d'un document et l'usage qui en est fait, permet de déterminer sa valeur pour son auteur et pour l'établissement de santé, mais également sa valeur en tant que preuve. Celle-ci peut être bien différente en fonction de son utilité. Le pense-bête réalisé par la secrétaire médicale a une grande valeur pour elle, c'est ce qui lui permet de ne pas oublier d'effectuer une de ses missions. En revanche pour l'établissement de santé, il n'aura aucune utilité, ni en tant qu'information, ni en tant que preuve. L'intérêt de déterminer les usages par document et la valeur de ceux-ci en fonction des personnes, permet d'établir le niveau de fiabilité nécessaire, afin qu'un document puisse avoir une valeur probante. Si le document, par son contenu, n'a pas vocation à être présenté comme preuve, il n'est pas nécessaire de garantir sa valeur. La copie de ce pense-bête n'a donc pas besoin d'être fiable car n'a aucune utilité en tant que preuve.

B) La valeur juridique à accorder aux documents

135. **Le référentiel de l'Agence du Numérique de Santé[354]**. L'ANS a expressément été chargée[355] de préciser les conditions d'application des dispositions prévues aux articles L. 1111-25 et suivants concernant la « *reconnaissance de la force probante des*

[353] C. gén. coll. ter., art. L. 2223-42. *« L'autorisation de fermeture du cercueil ne peut être délivrée qu'au vu d'un certificat attestant le décès ».*

[354] L'ANS *« accompagne la transformation numérique de notre système de santé, devenue aujourd'hui incontournable. L'Agence assure trois grandes missions. La première vise à réguler la e-santé en posant les cadres et les bonnes pratiques, notamment en terme de sécurité et d'interopérabilité pour faciliter le partage et les échanges de données de santé en toute confiance. La deuxième mission consiste à conduire les projets d'intérêt national sous l'égide des pouvoirs publics. Enfin, l'Agence du Numérique en Santé accompagne le déploiement national et territorial des outils et projets numériques en santé afin de développer les usages et de favoriser l'innovation ».* Elle a également en charge d'établir des référentiels d'interopérabilité et de sécurité notamment PGSSI-S *« afin de garantir l'échange, la partage, la sécurité et la confidentialité des données de santé à caractère personnel »,* conformément à l'article L. 1470-5 du Code de la santé Publique. Cette PGSSI-S comprend entre autres, le référentiel force probante.

[355] C. santé publ., L. 1111-31.

documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique »[356] tant au niveau technique qu'organisationnel. Pour répondre à sa mission, un référentiel force probante des documents de santé a été produit et mis en concertation de novembre 2019 à mi-janvier 2020 ; sa version définitive a été publiée en mars 2021. Ce référentiel concerne « *tous les processus liés à la production ou l'échange de documents de santé comportant des données de santé à caractère personnel, dans le domaine de la santé, du suivi social et du médico-social »*[357]. Ce dernier donne notamment des indications quant à la classification des différents documents contenant des données de santé, en octroyant des paliers permettant de déterminer le degré de fiabilité et les modalités techniques à mettre en place en fonction du document (1). Cependant la portée de ce référentiel possède tout de même des limites (2).

1) Les paliers établis par l'ANS

136. **Un niveau de force probante acceptable en fonction du document**. Un établissement de santé produit chaque jour un très grand nombre de documents que ce soit en version papier ou en version numérique. Dès lors que la création d'un document papier est réalisée, se pose inévitablement la question de sa dématérialisation en vue de pouvoir le conserver au sein d'une gestion électronique des documents (GED), du logiciel de dossier patient informatisé ou encore pour l'envoyer par messagerie. Il a été établi qu'en fonction du contenu du document et de son usage, il n'était pas toujours pertinent de mettre en œuvre les mesures maximales permettant à la copie de bénéficier du plus haut niveau de fiabilité. « *C'est pourquoi ce référentiel définit un ensemble alternatif de mesures de sécurité capables de donner aussi un niveau de force probante acceptable pour une copie numérique »*[358] qui n'est pas présumée fiable.

137. **Une destruction possible des documents de santé.** La définition des paliers et le respect des conditions à mettre en place définis par l'ANS revêt une importance toute particulière. En effet, le Code de la santé publique prévoit que *« lorsque une copie numérique fiable a été réalisée, le document original peut être détruit avant la fin de la durée légale de conservation ou, à défaut, de celle prévue au 5° de l'article 4 de la loi n° 78-17 du 6 janvier*

[356] C. santé publ., L. 1111-25 et s.
[357] ANS, *Référentiel force probante des documents de santé – Annexe 1 – Socle commun de principes techniques et organisationnels*, PGSSI-S, 2021.
[358] ANS, *Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation*, PGSSI-S, 2021.

1978 relative à l'informatique, aux fichiers et aux libertés ».[359] Aussi, la copie n'aura pas seulement vocation à simplifier le quotidien des praticiens dans leur pratique, ou à communiquer des informations, mais pourra également se substituer à l'original, qui pourra être détruit de manière volontaire[360]. Or si le document original est détruit et qu'il y a un doute sur la fiabilité de la copie, il ne sera plus possible de fournir l'original pour prouver sa fiabilité. Le respect du référentiel produit par l'ANS par un établissement de santé permet de lui assurer un niveau de fiabilité acceptable pour ses copies.

138. **Trois paliers**[361]. L'ANS décrit trois paliers, dont le niveau de sécurité à appliquer est croissant :

- ***« Palier 1 : Copie numérique « simple »*** *: scan simple d'un document respectant au minimum les impératifs de l'identitovigilance et de la protection des données personnelles ;*
- ***Palier 2 : Copie numérique « sécurisée »*** *: numérisation d'un document réalisée dans des conditions maîtrisées, apportant des éléments d'intégrité et de traçabilité suffisants pour autoriser la destruction du document original, sans pour autant imposer la qualification du service de protection de l'intégrité ni la certification du service de conservation afin d'optimiser les coûts ;*
- ***Palier 3 : Copie numérique « fiable »*** *: réalisation d'une copie numérique conforme aux exigences du décret d'application pour la copie fiable stipulées par le code civil, bénéficiant de la présomption de fiabilité et autorisant la destruction de l'original. L'intérêt principal de ce palier est d'offrir toutes les garanties nécessaires sur le plan juridique puisque la copie numérique fiable a, selon la loi, une force probante identique à son original papier (cf. article 1379 du code civil)* »[362].

En d'autres termes, les copies associées au palier 1 sont celles n'ayant pas une grande valeur en tant que preuve ou pour l'établissement. La mise en place des mesures décrites par ce palier ne permet pas de détruire l'original. Le palier 2 est un palier intermédiaire permettant de copier les documents avec un degré de fiabilité acceptable. La fiabilité des copies ne sera

[359] C. santé publ., art. L.1111-26.
[360] Cette possibilité était déjà consacrée par le Code Civil. Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *op. cit.*
[361] Christian DUBOURG, « Introduction à la force probante des documents de santé », *spark archives,* 2020. « *Le référentiel "Force probante" préconise clairement la mise en place de trois niveaux d'exigences (3 paliers) selon la typologie des documents traités et les risques associés. Il propose une méthodologie permettant d'analyser le contexte juridique propre au cas d'usage métier et d'adapter les moyens aux enjeux* ».
[362] ANS, *Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation*, PGSSI-S, 2021.

pas présumée, en revanche, l'établissement bénéficiera de tous les éléments permettant de prouver la fiabilité de la copie en cas de contestation. Bien que la fiabilité ne soit pas présumée, une destruction de ces documents est tout de même possible. Quant au palier 3, il s'agit de celui présentant le maximum de garantie et dont la fiabilité des copies est présumée. Dès lors que les règles relatives à ce palier sont respectées, il est considéré que la copie possède la même valeur que l'écrit original.

139. **La détermination du palier par document**. Afin de déterminer quel palier minimum appliquer à un document, l'ANS a classifié les documents en fonction de leurs catégories, dont le tableau récapitulatif est le suivant[363] :

Type de document	Palier minimum à mettre en œuvre		
	Palier 1	Palier 2	Palier3
Expression de la volonté du patient			X
Information communiquée par la personne prise en charge	X		
Autre document du périmètre (traitement par défaut)		X	

Très schématiquement, la classification peut être réalisée en trois grandes catégories :

i. La première correspond aux documents dont le plus haut niveau de fiabilité est nécessaire. Il s'agit de l'expression de la volonté du patient lorsque celle-ci aura « *des conséquences sur sa prise en charge* »[364] comme le recueil du consentement du patient, notamment lorsque celui-ci doit obligatoirement être recueilli de manière écrite.

ii. La seconde correspond aux documents dont le niveau de fiabilité attendu est le plus faible : les informations communiquées par la personne prise en charge. « *Cette catégorie rassemble les documents permettant à la personne prise en charge de s'exprimer sans que cela ait de conséquences d'ordre médical sur sa prise en charge* »[365]. Il peut s'agir par exemple d'un « *questionnaire de satisfaction nominatif,* [d'un] *document formulant les préférences culinaires ou les services demandés lors d'un séjour en établissement* »[366].

iii. Et la troisième qui correspond à tous les autres documents de santé qui n'entrent pas dans la catégorie une ou deux et dont la réalisation de la copie n'a pas à être présumée fiable, mais

[363] ANS, *Référentiel force probante des documents de santé – Annexe 6 – Classification des documents de santé,* PGSSI-S, 2021.
[364] *Ibid.*
[365] *Ibid.*
[366] *Ibid.*

dont on doit tout de même être en capacité de démontrer la fiabilité. Il s'agit par exemple d'un compte-rendu médical, des feuilles de soins etc.

Ce tableau est une version simplifiée de celui envisagé dans la version mise en concertation [367]. Cette simplification rend plus aisée le choix du palier minimum à attribuer aux différents documents en ne les classifiant qu'en trois grandes catégories.

Cependant, l'ANS précise que d'autres critères peuvent être pris en compte afin de choisir le palier le plus adéquat tels que : « *le contenu du document d'origine […], les conditions de réalisation de la copie numérique […], l'usage de la copie numérique […], les contraintes et risques juridiques attachés au document* »[368].

140. **Trois critères de choix manquants**. Trois autres critères doivent impérativement être pris en compte pour choisir le palier le plus adéquat.

i. La réalisation d'un document est imposée par la Loi : dès lors qu'un formalisme est imposé par les textes, il est important de le prendre en compte afin de déterminer le choix du palier. En effet, le code de la santé publique n'impose que rarement un formalisme. On peut donc légitimement considérer que lorsque c'est le cas, le document requiert un niveau tel d'importance, qu'il est nécessaire de garantir sa valeur[369].

ii. La confiance de la personne envers le contenu du document : il est impératif que la personne se servant du document copié puisse avoir confiance en son contenu. Prenons

[367]

Type de document	*Palier minimum à mettre en œuvre*		
	Palier 1	*Palier 2*	*Palier3*
Certificat et déclaration		X	
Expression de la volonté du patient			X
Prescription		X	
Avis médical		X	
Suivi des soins		X	
Document lié à l'obtention d'un remboursement		X	
Information transmise par un intervenant		X	
Données issues de l'appareillage médical	X		
Information communiquée par la personne prise en charge	X		
Autre document du périmètre (traitement par défaut)		X	

[368] ANS, *Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation*, PGSSI-S, 2021.

[369] A titre d'exemple, *« tout certificat, ordonnance, attestation ou document délivré par un médecin doit être rédigé lisiblement en langue française et daté, permettre l'identification du praticien dont il émane et être signé par lui »* (C. santé publ., art. R. 4127-76). Un formalisme particulier est demandé pour la réalisation de ces documents impliquant un haut niveau d'importance, d'autant plus qu' *« un document médical signé d'un médecin engage sa responsabilité »* (Hervé LECLET (Dr) et Martine MADOUX, « Signature des prescriptions médicales et des comptes-rendus », *Santopta*, 2016). Aussi, il est nécessaire de les mettre au sein d'un palier élevé.

l'exemple d'un dossier patient intégré dans le DPI afin de faciliter l'usage professionnel, mais dont l'original papier est conservé par l'établissement. On pourrait considérer qu'une copie avec un faible niveau de fiabilité est possible. Cependant, bien que cette copie ne soit pas nécessairement utilisée en tant que preuve, celle-ci sera utilisée par les professionnels de santé afin de prendre en charge le patient. Aussi, les professionnels doivent avoir une confiance absolue quant au contenu du dossier. La réalisation d'une copie fiable des dossiers est impérative.

iii. L'ensemble indissociable des documents : bien que chaque typologie de document corresponde à un palier, il n'est pas toujours pertinent de le respecter à la lettre. En effet, il est par exemple précisé que l'expression de la volonté du patient doit correspondre au palier 3, le suivi des soins au palier 2 et « *un document formulant les préférences culinaires* »[370] au palier 1. A la lecture de ceci, chaque document suivrait des modalités techniques de dématérialisation différentes. Cependant, cela n'est pas pertinent alors que ces documents sont rassemblés dans un seul et même ensemble, tel que le dossier médical. Si l'on souhaite dématérialiser ce dossier, il n'est pas opportun et serait même source d'erreur d'employer des modes de dématérialisation différents pour chaque document. Aussi, l'ensemble dans lequel se trouve le/les documents doit être pris en considération pour choisir le meilleur palier à appliquer.

2) Les limites de ce référentiel

141. **Le référentiel : une portée contraignante ?** L'application du référentiel est obligatoire bien qu'il soit laissé une grande latitude quant à sa mise en œuvre et son application. A titre d'exemple, l'ANS prévoit le cas d'une structure de santé ne respectant pas ce référentiel : « *le non-respect des exigences du référentiel force probante doit être justifié par chaque structure de santé à l'appui d'un argumentaire documenté. Celui-ci prendra un format conforme aux processus de décision internes propres à la structure de santé concernée et pourra être complété par un plan d'action de mise en conformité au référentiel »*[371]. Aussi, bien que ce référentiel fasse partie de la PGSSI-S établie par l'ANS et devant être respectée, sa non-application n'entraîne pas la perte totale de la valeur probante des documents. En revanche, le juge accordera un niveau de confiance supérieur aux établissements ayant suivi les instructions et préconisations de ce référentiel.

[370] ANS, *Référentiel force probante des documents de santé – Annexe 6 – Classification des documents de santé, PGSSI-S*, 2021.
[371] ANS, *Référentiel force probante des documents de santé – Document introductif*, PGSSI-S, 2021.

142. **La valeur juridique de l'original.** Une autre limite de l'application du référentiel est la valeur juridique du document original. Avant de déterminer le palier du document et/ou les modalités à respecter afin qu'une copie ait la même force probante que le document original, il est nécessaire de s'assurer au préalable que ce dernier possède lui-même une valeur juridique. En effet, une copie d'un document original ne possédant aucune valeur juridique, même si celle-ci est réalisée dans des conditions permettant de garantir sa fiabilité, ne pourra avoir une valeur supérieure au document original. Il ne sera donc pas nécessaire d'en assurer un niveau de fiabilité aussi élevé que si l'original avait une valeur probante. Cette détermination en amont n'est vraiment pertinente que si la réalisation des copies n'est faite que sur un nombre très restreint de documents. En effet, dès lors qu'un projet de copie en masse d'un très grand nombre de documents est mis en place, par exemple pour la dématérialisation de dossiers patients papier, il est plus pertinent et aisé, de réaliser toutes les copies dans les mêmes conditions techniques.

143. **Les documents ne contenant pas des données de santé**. Le référentiel force probante ne concerne que les documents contenant des données de santé. Or, au sein d'un établissement de santé, un grand nombre de documents ne contiennent pas que des données de santé : les documents RH, les contrats (salariés, prestataires, coopération), les documents administratifs (PV d'organes institutionnels). Pour autant, leur dématérialisation est un enjeu tout aussi important pour ces établissements de santé. Concernant ces documents, les établissements devront appliquer d'autres modalités et mécanismes de dématérialisation que ceux prévus par ce référentiel bien qu'il soit intéressant de s'en inspirer.

144. **L'appréciation du juge**. Pour terminer, la dernière limite à ce référentiel est que, même si l'ensemble des exigences est mis en place par l'établissement de santé afin de dématérialiser des documents papiers contenant des données de santé, le juge aura toujours le pouvoir d'en apprécier les résultats quant à leur fiabilité[372].

§2 La mise en place de la reproduction des documents

145. **Le préalable à la mise en place du processus de dématérialisation.** La garantie de la fiabilité de la copie doit être envisagée sous trois aspects : la fiabilité doit être assurée pendant la reproduction, le résultat de la copie doit être conforme au document copié, et la fiabilité de la copie doit être garantie pendant toute sa conservation. Le processus de

[372] C. civ., art. 1379.

dématérialisation établi par l'établissement de santé devra prendre en compte ces aspects afin de déterminer toutes les étapes permettant de garantir la réalisation d'une copie fiable.

Comme on a pu le voir précédemment, le choix du procédé de reproduction pour la dématérialisation des documents contenant des données de santé dépendra du niveau de fiabilité que l'on souhaite lui accorder. Trois niveaux de fiabilité sont envisagés : un premier niveau dont la fiabilité est présumée mais qui n'est utilisé que pour un nombre très réduit de documents, au regard de la complexité de mise en œuvre ; les deux autres niveaux correspondant à une fiabilité simple (plus ou moins renforcée) dont les conditions de reproduction ne sont pas envisagées par le Code civil mais pour lesquels l'ANS, dans son référentiel force probante, expose les conditions techniques à respecter.

On constate donc que la plupart des copies réalisées au sein des établissements de santé ne bénéficieront pas d'une présomption de fiabilité. Au-delà des éléments fournis par l'ANS qui donnent déjà une très bonne base pour la reconnaissance de la valeur probante des copies, il est intéressant de découvrir le Droit applicable dans les autres pays, notamment au Luxembourg (A) pouvant permettre de garantir davantage cette valeur. Tous ces éléments permettront à l'établissement de santé de choisir s'il souhaite que le processus de dématérialisation soit réalisé en interne, externalisé ou les deux (B).

A) L'expérience d'un pays voisin : le Luxembourg

146. **Le Luxembourg précurseur**. Le Luxembourg a été, avec la Belgique, un des précurseurs en matière de législation sur la dématérialisation des écrits, en promulguant la Loi du 25 juillet 2015 relative à l'archivage électronique[373]. Cette Loi a permis de reconnaître la valeur probante d'un écrit électronique au même titre qu'un écrit papier y compris lorsque celui-ci est une copie. En effet, la Loi affirme textuellement que les copies « *peuvent bénéficier d'une présomption de conformité à l'original* »[374] sous réserve de respecter certaines conditions tant au moment de leur dématérialisation que pendant leur conservation[375].

[373] Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification : 1. De l'article 1334 du Code civil ; 2. De l'article 16 du Code de commerce ; 3. De la loi modifiée du 5 avril 1993 relative au secteur financier.
[374] Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification : 1. De l'article 1334 du Code civil ; 2. De l'article 16 du Code de commerce ; 3. De la loi modifiée du 5 avril 1993 relative au secteur financier, art. 1.
[375] Polyanna BIGLE, « Archivage électronique : le Luxembourg précurseur », *Lexing*, 2015.

147. **La copie à valeur probante.** La Loi définit la copie a valeur probante comme une « *reproduction fidèle et durable sous forme numérique ou micrographique d'un original* »[376], faisant écho aux anciens critères permettant à une copie d'avoir une valeur probante en France. On constate ici que la Loi du Luxembourg n'envisage que la valeur probante de la copie sur support numérique ou micrographique, alors que la France élargit sa vision en ne faisant aucune distinction sur le support de la reproduction ; elle s'attarde davantage sur le format de la reproduction, en ne le limitant pas à la reproduction électronique. Cela est d'autant plus troublant que la France a choisi de modifier ces critères de fidélité et de durabilité jugés trop réducteurs[377] pour la reproduction électronique, bien qu'ils soient tout de même à prendre en compte pour appréhender la notion de fiabilité.

Cette différence peut s'expliquer par le fait que *« le droit luxembourgeois ne présente pas toujours une grande spécificité par rapport au droit des pays voisins, et notamment du droit français. Ceci s'explique par deux raisons. D'abord, le droit commun des contrats, au Luxembourg, trouve ses assises dans le Code civil hérité de la France, et les juges luxembourgeois, formés majoritairement en France, s'inspirent habituellement des interprétations doctrinales et jurisprudentielles reçues en France, et ont gardé les manières de penser françaises […] »*[378]. Or au moment de la promulgation de la Loi du Luxembourg, les critères de fidélité et de durabilité n'avaient pas encore été modifiés et étaient appliqués, en l'état, par les juges français, y compris pour reconnaître la valeur probante d'une copie numérique.

La fiabilité n'est pourtant pas ignorée par la Loi du Luxembourg puisqu'elle définit la dématérialisation comme étant *« l'activité qui consiste à créer une copie à valeur probante d'un original existant sous forme analogique dans des conditions qui assurent des garanties fiables quant à la conformité de la copie ainsi créée à l'original »*[379]. C'est la technique même de reproduction qui doit montrer des garanties de fiabilité. Il en va de même pour la conservation.

---

[376] Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification : 1. De l'article 1334 du Code civil ; 2. De l'article 16 du Code de commerce ; 3. De la loi modifiée du 5 avril 1993 relative au secteur financier, art. 2.

[377] Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *op. cit.*

[378] Pascal ANCEL et Alexandre FIEVEE, « Contrat et immatériel – Rapport Luxembourgeois », *Travaux de l'Association Henri CAPITANT Bruylant*, 2014, tome LXIV, pp. 515-527.

[379] Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification : 1. De l'article 1334 du Code civil ; 2. De l'article 16 du Code de commerce ; 3. De la loi modifiée du 5 avril 1993 relative au secteur financier, art 2.

Bien que la terminologie diffère entre le Luxembourg et la France, il apparaît tout de même que la philosophie est la même. En effet, le procédé de reproduction au Luxembourg doit permettre « *d'assurer que des garanties fiables existent […] quant à la conformité des copies à valeur probante aux originaux, au caractère lisible des copies à valeur probante, à la confidentialité des originaux et copies à valeur probante ainsi qu'à l'intégrité des copies à valeur probante tant que celles-ci sont en la possession du prestataire de services de dématérialisation* »[380]. Ces conditions à respecter sont similaires voire identiques à celles établies par la France.

148. **Le prestataire de service de dématérialisation.** La grande différence entre les deux pays est la présomption de conformité de la copie par rapport à l'original. Pour qu'une copie soit présumée conforme à l'original au Luxembourg, la dématérialisation doit être réalisée par un prestataire de service de dématérialisation certifié[381]. Pour obtenir cette certification, les entreprises doivent être certifiées par un certificateur devant vérifier que l'ensemble des conditions énoncées par la Loi sont bien respectés. Puis, ces entreprises doivent demander auprès de l'Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (l'ILNAS), leur inscription sur la liste des prestataires de services de dématérialisation. Aujourd'hui, seuls quatre prestataires sont certifiés *« prestataire de service de dématérialisation »*[382].

149. **La fiabilité simple au Luxembourg.** En revanche, *« une copie ne peut être rejetée par le juge au seul motif qu'elle se présente sous forme électronique ou qu'elle n'a pas été réalisée par un PSDC-D »*[383]. La copie ne bénéficiera pas d'une présomption de conformité à l'original, renversant ainsi la charge de la preuve[384]. Pour autant, une conformité simple est prévue permettant de garantir une valeur probante à la copie : *« Une copie effectuée sous la responsabilité du détenteur a la même valeur probante que l'original lorsqu'elle a été réalisée dans le cadre d'une méthode de gestion régulièrement suivie qui réponde aux*

[380] Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification : 1. De l'article 1334 du Code civil ; 2. De l'article 16 du Code de commerce ; 3. De la loi modifiée du 5 avril 1993 relative au secteur financier, art 4.

[381] Isabelle RENARD, « Le Luxembourg crée un écosystème de confiance pour la dématérialisation et la conservation des documents dans le secteur financier », *Isabelle Renard – Cabinet d'Avocats.* Disponible à l'adresse : https://www.irenard-avocat.com/ (consulté le 23/09/2022).

[382] Le Gouvernement du GRAND-DUCHE de Luxembourg, « Liste des PSDC », *portail-qualite.lu* : Lab Luxembourg S. A., Victor Buck Services S. A., Numen Europe S. A.et KPMG Services S.à.r.l. Disponible à l'adresse https://portail-qualite.public.lu/fr/confiance-numerique/archivage-electronique/liste-psdc.html 'consulté le 17/09/2021).

[383] Projet de Loi relatif à l'archivage électronique et modifiant la loi modifiée du 6 avril 1993 relative au secteur financier, art. 3.

[384] Renaud VANDEROOST, « Archivage legal électronique et PSDC : renverser la charge de la preuve », *ICT Experts Luxembourg*, 2014.

conditions fixées par règlement grand-ducal »[385]. Contrairement à la France, le Luxembourg prévoit par le règlement grand-ducal du 25 juillet 2015[386] des dispositions à respecter pour garantir la fiabilité de la dématérialisation de la copie permettant au détenteur des documents originaux d'avoir un fil conducteur à suivre pour garantir la valeur juridique des copies réalisées.

B) La dématérialisation internalisée ou externalisée

150. **La normalisation en France**. Contrairement au Luxembourg, aucune certification n'est exigée par la France pour qu'une copie soit présumée fiable, permettant ainsi à toute personne détentrice de documents, de pouvoir réaliser des copies présumées fiables. Cela implique une largesse dans l'appréciation par les juges de la réalisation des critères de présomption de fiabilité, mais implique également une absence de certitude quant à cette présomption pour celui qui réalise les copies. La France bénéficie tout de même de cadres normatifs élaborés par l'AFNOR[387] permettant aux professionnels de connaître les standards en vigueur pour respecter l'état de l'art et/ou la législation en vigueur, en se basant notamment sur les normes ISO. L'une de ces normes est la norme NF Z42-026 homologuée en mai 2017 concernant la numérisation fiable de documents papier et prenant en compte les obligations légales prévues à l'article 1379 du Code civil et de son Décret d'application.

A la demande de certains acteurs de la numérisation, l'AFNOR a créé une certification NF 544 permettant aux professionnels respectant la norme NF Z42-026 et « *des critères additionnels sur la gestion des sous-traitants, du personnel, des documents, le suivi d'indicateurs, la gestion des réclamations et l'amélioration continue »*[388], d'être certifiés.

---

[385] Projet de Loi relatif à l'archivage électronique et modifiant la loi modifiée du 6 avril 1993 relative au secteur financier, art. 3.

[386] Règlement grand-ducal du 25 juillet 2015 relatif à la dématérialisation et à la conservation de documents, mémorial A n°150/2015.

[387] Afnor, Qui sommes-nous ? : « L'association AFNOR et ses filiales constituent un groupe international au service de l'intérêt général et du développement économique. Le groupe de 1250 collaborateurs, 40 implantations dans le monde et 77000 clients, conçoit des solutions fondées sur les normes volontaires, sources de progrès et de confiance depuis 1926. Sa vocation est d'accompagner les organisations et les personnes pour diffuser cette confiance. Un accompagnement qui s'effectue au travers de 4 domaines de compétences » notamment la normalisation pour accompagner et guider « les professionnels pour élaborer les normes volontaires nationales et internationales » et la certification. « AFNOR Certification réalise des prestations de services et d'ingénieries en certification et évaluation de produits, systèmes, services et compétences, délivrées sous des marques telles que AFAQ, NF ou écolabel européen ». Disponible à l'adresse : https://www.afnor.org/ (consulté le 30/08/2021).

[388] Le Mag AFNOR Certification, « numérisation fidèle : la certification NF 544 au scanner », 2018. Disponible à l'adresse : https://lemagcertification.afnor.org/ (consulté le 09/12/2021).

Pour obtenir cette certification, ces derniers doivent respecter un certain nombre d'exigences détaillées au sein d'un cahier des charges[389] et doivent faire l'objet d'un audit annuel.

151. **La portée de la norme**. La norme NF Z42-026 ne bénéficie d'aucune portée contraignante[390] puisqu'aucun arrêté ne prévoit expressément son application. En revanche les juges accordent une valeur aux copies respectant ces normes. A titre d'exemple, la troisième chambre de la Cour d'appel de Lyon a rendu un arrêt en date du 3 septembre 2015[391] reconnaissant la fiabilité et la durabilité des copies produites par la Caisse de Crédit Mutuel Enseignant du sud-est notamment grâce au respect de la norme AFNOR NF Z42-013 (qui à l'époque concernait l'archivage électronique mais également la réalisation des copies formelles). *« Cette jurisprudence est d'autant plus instructive qu'elle montre aussi la suffisance de la norme NF Z42-013 :2009 pour la création de copies fidèles et durables, mettant également au second plan la récente norme NF Z42-026 sur les prestations de numérisation fidèle* »[392]. Cela implique également que passer par un prestataire certifié NF 544 emporterait encore davantage la conviction du juge.

152. **Une dématérialisation internalisée ou externalisée ?** Le choix pour un établissement de santé de procéder à la dématérialisation de ses documents papiers en interne ou par un prestataire tiers, dépendra de plusieurs facteurs : son budget, la quantité de documents à dématérialiser, le niveau de fiabilité que doivent avoir les documents dématérialisés, la destruction (ou non) des originaux, ou encore l'envergure du projet de dématérialisation. Par exemple, si le projet de l'établissement de santé est de dématérialiser tous les dossiers patients papier, il peut être intéressant de faire appel à un prestataire. En revanche, pour la dématérialisation de documents au quotidien, comme l'ordonnance d'un médecin généraliste pour la consultation d'un spécialiste, une dématérialisation internalisée est beaucoup plus pertinente.

Ces choix réalisés vont permettre d'élaborer un processus de dématérialisation qui peut comporter plusieurs processus en fonction du type de copie ou d'usage. Il est notamment possible de prévoir, pour une dématérialisation en masse, un processus impliquant un prestataire tiers et pour la dématérialisation des documents quotidiens, un processus interne.

---

[389] Afnor, *Prestations de numérisation fidèle de documents sur support papier,* 2021. Disponible à l'adresse : http://cdn.afnor.org/download/reglements/FR/REGNF544.pdf (consulté le 22/09/2021).
[390] Christian DUBOURG, « La norme NF Z42-026 pour détruire le document papier original numérisé fait-elle loi ? », *spark archives,* 2017.
[391] CA, Lyon, 6e chambre, 3 septembre 2015 – n° 13/09407.
[392] Christian DUBOURG, « La norme NF Z42-026 pour détruire le document papier original numérisé fait-elle loi ? », *op. cit.*

Ce processus doit également être entièrement détaillé étape par étape, décrivant notamment le choix du procédé utilisé, ses caractéristiques, les personnes impliquées etc. Quel que soit le choix de l'établissement entre une dématérialisation internalisée ou externalisée, celui-ci devra être documenté et justifié. De la même façon, le processus de dématérialisation mis en place, le sera également, afin de pouvoir servir comme preuve en cas de contestation de la fiabilité de la copie.

L'ANS préconise que *« lorsque la numérisation est réalisée par une ressource externe, il est conseillé d'établir une convention de numérisation définissant l'objet de la prestation de numérisation, et précisant les différentes tâches, responsabilités et obligations des acteurs concernés (se reporter à la norme NF Z42-026 dans sa dernière version pour sa rédaction) »*[393]. Bien que la réalisation de la dématérialisation externalisée n'impose pas de passer par un prestataire certifié, à l'instar du Luxembourg, il est possible pour les établissements de l'exiger tout de même. Comme on a pu le voir précédemment, le respect de la norme NF Z42-026 permet d'apporter une preuve supplémentaire au juge que les copies réalisées sont fiables, preuve pouvant emporter sa conviction.

« Lorsque le processus de numérisation est réalisé en interne, il est conseillé de s'inspirer du contenu type de [la convention de numérisation] *pour définir les rôles et les responsabilités des différents intervenants »*[394]. Le processus de dématérialisation défini devra être porté à la connaissance de tout le personnel de l'établissement de santé via la charte information et la PSSI de l'établissement afin qu'il soit respecté par chacun et garantir la valeur juridique des copies ainsi réalisées. Ce processus peut être décliné dans une politique de numérisation à destination des professionnels afin que celle-ci soit davantage accessible.

[393] ANS, *Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation*, PGSSI-S, 2021.
[394] *Ibid.*

Conclusion du chapitre. La mise en place de la dématérialisation de documents papier est un projet à part entière pour un établissement de santé, qu'il s'agisse d'une dématérialisation en masse ou celle plus ponctuelle au quotidien. Cette dématérialisation peut entraîner pour l'établissement de santé, des risques pour la bonne prise en charge du patient, mais également des risques juridiques. Pour les pallier ou au moins les minimiser au maximum, l'établissement de santé doit :

i. Respecter le cadre légal général et notamment les dispositions prévues par le Code civil et son Décret d'application.

ii. Respecter la règlementation spécifique à certains domaines. A titre d'exemple, l'arrêté du 22 mars 2017[395], fixe les modalités de numérisation des factures papier en donnant davantage de directives notamment techniques, que le cadre général tel que le format du document qui doit être en PDF ou PDF A/3. Les spécificités de chaque domaine du Droit permettent de donner des indications sur ce qui peut être appliqué aux documents contenant des données de santé. Il est donc intéressant de pouvoir s'en inspirer.

Pour la dématérialisation des documents contenant des données de santé, il est impératif de respecter toutes les règlementations ou préconisations annexes à la santé telles que l'identitovigilance, la protection des données à caractère personnel, le secret professionnel ou encore la PGSSI-S établie par l'ANS et notamment le référentiel force probante.

iii. S'appuyer sur les normes en vigueur afin de pouvoir démontrer que la dématérialisation des documents s'appuie sur l'état de l'art en la matière et, idéalement, passer par un prestataire certifié ou que l'établissement le soit lui-même.

Dernier point restant à éclaircir : quelle est la valeur de la copie par rapport au document original ? Avant l'Ordonnance de 2016, la valeur juridique de la copie était conditionnée, par la présentation du document original[396], ou si ce dernier n'existait plus, par la présentation d'une copie qui soit une reproduction fidèle et durable. L'Ordonnance de 2016 est venue

---

395 Arrêté du 22 mars 2017 fixant les modalités de numérisation des factures papier en application de l'article L. 102 B du livre des procédures fiscales, JORF n°0076, 30 mars 2017, texte n°14.

396 LABBEE Xavier, *Introduction générale au droit – pour une approche éthique*, Presses Universitaires du Septentrion, 2010, p. 161. *« Dans le système du code civil, la copie n'avait de valeur que dans la mesure où l'on pouvait la confronter à l'original : l'article 1334 du code civil dispose en effet que « les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre dont la représentation peut toujours être exigée ». Ce qui veut dire qu'une copie d'acte sous seing privé peut toujours être produite en justice dès l'instant que la partie est capable, sur demande de son adversaire, d'en produire l'original pour vérification (Cass. civ. 30 avril 1969, D 1969 412, JCP 1969 II 16 057 note M.A.). Ce qui veut donc dire que pour le code civil, une copie n'a pas de force probante si l'original ne peut être produit (Cass. civ. 1ère, 27 avril 1978, Bul. Cass. civ. 1 n°160. Civ. 1ère 24 octobre 2006 AJ 2908 obs. Avena ROBARDET).*

donner davantage de valeur à la copie en posant « *un nouveau principe selon lequel la copie fiable a la même force probante que l'original, peu importe que celui-ci subsiste ou pas, et peu important l'origine, le cas échéant, de la disparition de l'original* »[397]. Pour autant, le dernier alinéa de l'article 1379 prévoit que « *si l'original subsiste, sa présentation peut toujours être exigée »*[398] laissant penser que même si la copie fiable bénéficie de la même valeur que l'original, en cas de contradiction entre les deux, l'original aurait davantage de valeur. Le rapport au Président de la République relatif à l'Ordonnance de 2016 est venu préciser qu' « *en tout état de cause, si l'original subsiste, sa production pourra toujours être ordonnée par le juge, mais sa subsistance ne conditionne plus la valeur probatoire de la copie* »[399]. On constate ici que la copie bénéficie à elle seule d'une valeur juridique, contrairement à l'ancienne législation. La production de l'original pourra certes être exigée, mais davantage pour comparer les deux écrits, que pour donner plus de valeur à l'original. Aussi, en cas de différence entre les deux, ce n'est pas tant l'original qui emportera la conviction du juge, mais plutôt la comparaison de la fiabilité entre l'original et la copie.

Conclusion du titre. La dématérialisation au sein des établissements de santé est un projet d'envergure devant au préalable être bien préparé pour garantir la valeur juridique des documents dématérialisés, qu'ils soient des originaux ou des copies électroniques. Que ces documents contiennent des données de santé ou non, l'établissement doit impérativement respecter le cadre légal général et spécifique à chaque type de document ainsi que l'état de l'art en la matière.

Chaque établissement de santé souhaitant dématérialiser ses documents sera confronté globalement à la même analyse des textes, des normes, des recommandations et devra mettre en place une politique de dématérialisation. N'est-il pas envisageable voire recommandé dans certains cas de mutualiser les efforts ? Prenons un exemple : à terme, tous les établissements auront vocation à utiliser un dossier patient informatisé, notamment avec la création des groupements hospitaliers de territoire (GHT)[400]. Un des objectifs de la mise en place des GHT

[397] Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[398] C. civ., art. 1379.
[399] Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.
[400] C. santé publ., art. L. 6132-1. : *« Chaque établissement public de santé, sauf dérogation tenant à sa spécificité dans l'offre de soins territoriale, est partie à une convention de groupement hospitalier de territoire. Le groupement hospitalier de territoire n'est pas doté de la personnalité morale. Le groupement hospitalier de territoire a pour objet de permettre aux établissements de mettre en œuvre une stratégie de prise en charge commune et graduée du patient, dans le but d'assurer une égalité d'accès à des soins sécurisés et de qualité. Il assure la rationalisation des modes de gestion par une mise en commun de fonctions ou par des transferts*

est d'installer *« un système d'information hospitalier convergent, en particulier la mise en place d'un dossier patient permettant une prise en charge coordonnée des patients au sein des établissements parties au groupement »*[401]. A ce titre, le GHT Cœur Grand Est[402] a créé un projet sur quatre ans pour installer un DPI unique pour l'ensemble des établissements du GHT. La création d'un DPI unique implique nécessairement le partage et l'utilisation de documents pouvant provenir d'autres établissements que celui dans lequel un professionnel exerce. Le professionnel mais également l'établissement doivent pouvoir avoir une confiance absolue en la fiabilité de ces documents. N'est-il pas pertinent d'envisager à l'échelle d'un GHT une politique commune concernant la dématérialisation afin de bénéficier des mêmes outils et pratiques au sein de tous les établissements ? Cela permettrait d'une part de mutualiser les coûts et d'autre part, de garantir la valeur juridique de tous les documents au sein du DPI unique. D'autant que, dès lors que les documents sont au sein de ce DPI unique, leur fiabilité devra être maintenue à long terme afin qu'ils ne perdent pas leur valeur probante.

d'activités entre établissements. Dans chaque groupement, les établissements parties élaborent un projet médical partagé garantissant une offre de proximité ainsi que l'accès à une offre de référence et de recours ». Olivier JONQUET, « Les GHT : de quoi s'agit-il ? Le point de vue d'un médecin et universitaire », 2019, n°92, pp. 912-914. *« Le principe du GHT est d'amener les établissements de santé à mutualiser et à coordonner, en fonction de leur taille et de leur positionnement, les prises en soins des patients de manière à établir les parcours de soins ou de santé les plus rationnels et efficaces ».*

[401] C. santé publ., art. L. 6132-3.

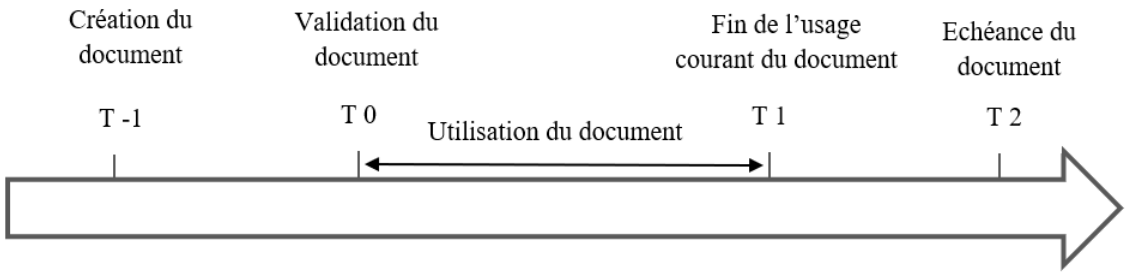
[402] Le GHT Cœur Grand Est correspond au GHT n°5 Marne – Haute-Marne – Meuse du Grand Est, composé de neuf centres hospitaliers : le CH de Verdun Saint-Mihiel, le CH de Bar-Le-Duc, le CHS de Fains-Véel, le CH de Saint-Dizier, le CH de Vitry-Le-François, le CH de la Haute-Marne, le CH de Wassy, le CH de Montier-en-Der et le CH de Joinville

TITRE 2 : La valeur juridique d'un document à long terme

153. **Deux temporalités**. Pour qu'un document numérique, qu'il soit natif ou copie, bénéficie d'une valeur probante, ce dernier doit être envisagé sur deux temporalités : au moment de sa création et plus particulièrement à sa validation (comme nous avons pu le constater lors du titre précédent), mais également pendant toute sa durée de conservation jusqu'à son élimination ou sa conservation définitive par les archives départementales ou nationales.

154. **Le cycle de vie d'un document**. Ces deux grandes phases énoncées par le Code civil (création/validation et conservation) font écho au cycle de vie d'un document, que l'on peut définir comme les différentes étapes de vie d'un document, de sa création jusqu'à sa destination finale. Selon le *records management*[403], le cycle de vie d'un document peut être fragmenté en cinq grandes étapes : la création du document, sa validation, son utilisation, la fin de son usage courant et son échéance qui est déterminée par la durée d'utilité administrative.

Cela peut être représenté de la manière suivante :



Les archivistes quant à eux estiment que les documents, qui sont par principe des archives[404], passent par trois âges tout au long de leur existence :

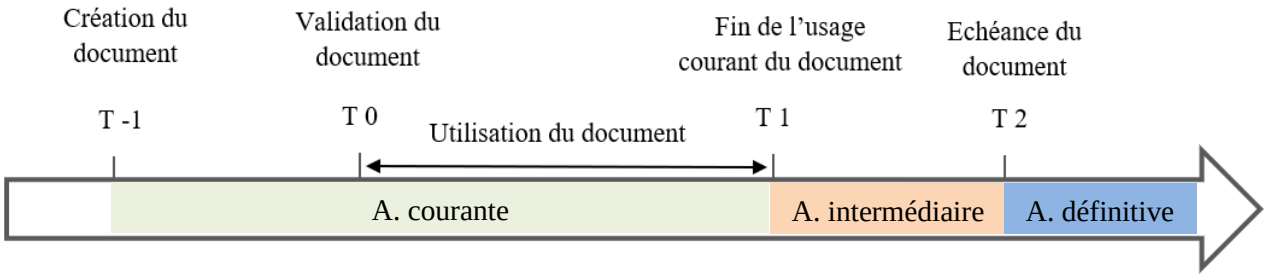
[403] « Comprendre et pratiques le records management. Analyse de la norme ISO 15489 au regard des pratiques archivistiques françaises », *Documentaliste-Sciences de l'Information*, 2005/2, vol. 42. *« Le records management est une fonction d'organisation et de gestion de l'ensemble des documents quels que soient leur forme ou leur support, produits ou reçus par toute personne physique ou morale dans l'exercice de ses activités ou de ses obligations légales. […] Le records management a pour finalité de permettre à l'organisme de disposer à tout instant du document dont il a besoin pour conduire ses activités, répondre aux exigences légales et réglementaires, et se protéger en cas de contentieux ».*

[404] Selon l'article L. 211-1 du Code de patrimoine, sont des archives « *l'ensemble des documents, y compris les*

i. Une archive est tout d'abord une archive courante[405] que l'on considère comme vivante ou encore active. L'archive est courante lorsqu'elle est utilisée de manière fréquente par la personne morale ou physique qui en est à l'origine ou qui l'a reçue.

ii. Dès lors que l'archive n'est plus utile dans l'immédiat par la personne morale ou physique, mais doit être conservée au regard d'une obligation administrative ou juridique et/ou de son intérêt, cette dernière devient une archive intermédiaire[406], que l'on considère comme semi-active.

iii. Une fois la fin du délai de conservation atteint, l'archive pourra être soit détruite, soit devenir une archive définitive[407], que l'on appelle également archive morte. Les archives définitives sont des archives qui sont conservées sans limitation de durée, présentant « *un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction* »[408].



On constate que les deux phases énoncées par le Code civil correspondent à deux phases du cycle de vie d'un document :

i. La première phase correspond à la validation du document puisque c'est à partir de ce moment que le document est figé et pourra engendrer des effets juridiques. Or, comme on a

---

données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité ».

[405] Selon l'article R.212-10 du Code du patrimoine, *« Sont considérés comme archives courantes les documents qui sont d'utilisation habituelle pour l'activité des services, établissements et organismes qui les ont produits ou reçus »*

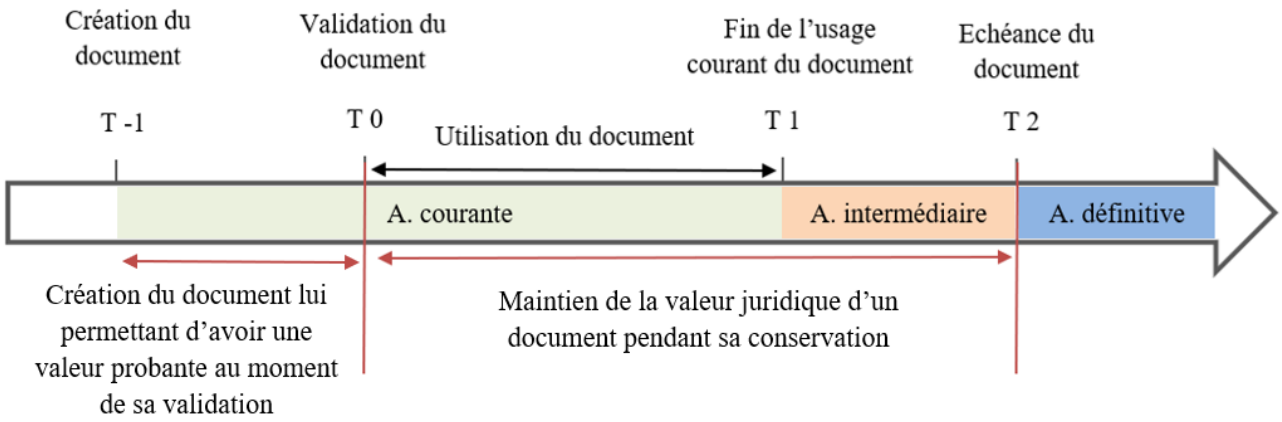
[406] Selon l'article R. 212-11 du Code du patrimoine, *« sont considérés comme archives intermédiaires les documents qui : 1° Ont cessé d'être considérés comme archives courantes ; 2° Ne peuvent encore, en raison de leur intérêt administratif, faire l'objet de sélection et d'élimination conformément aux dispositions de l'article R. 212-14 ».*

[407] Selon l'article R. 212-12 du Code du patrimoine, *« sont considérés comme archives définitives les documents qui ont subi les sélections et éliminations définies aux articles R. 212-13 et R. 212-14 et qui sont à conserver sans limitation de durée ».*

[408] Caroline ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé partagées*, Thèse dactylographiée, Nancy, 2009, p. 207.

pu le constater précédemment, la phase entre la création (ou transformation lorsqu'il s'agit d'une copie) jusqu'à sa validation, aura également un impact sur la valeur juridique du document et sur sa force probante en fonction du choix de la signature apposée, des modalités de sécurité mises en place lors de la reproduction, du format du document etc. Cette phase n'est donc pas à négliger. En effet, et rappelons-le, si un document, à sa validation, ne bénéficie que peu de valeur probante, peu importe les modalités mises en place pour sa conservation, sa valeur ne pourra en aucun cas être supérieure à sa valeur initiale. En revanche, elle pourra s'appauvrir si la conservation ne permet pas de garantir l'authenticité et l'intégrité du document.

ii. La seconde phase correspond au temps entre la validation du document et son échéance, c'est-à-dire pendant le temps de conservation du document. Aussi, c'est entre ces deux temps que la valeur juridique du document doit être maintenue afin que celle-ci ne soit pas diminuée à sa création et corresponde à la valeur souhaitée par l'établissement de santé.



155. **Le choix de l'établissement de santé**. Pour qu'un document validé puisse bénéficier et maintenir son niveau de valeur probante, ce dernier doit être conservé de manière à garantir son authenticité et son intégrité pendant toute sa durée de conservation (chapitre 1). Les choix faits et les modalités techniques mises en place par l'établissement de santé, tant pour créer les documents que pour les conserver, auront des effets juridiques sur ces derniers ; leurs impacts et leur portée sont encore aujourd'hui incertains (chapitre 2). Ces incertitudes juridiques doivent impérativement être prises en compte par l'établissement de santé lors de la mise en place d'un projet de dématérialisation.

Chapitre 1 : La conservation des documents électroniques contenant des données de santé

156. **La notion de conservation**. La conservation est définie comme l' « *action de conserver quelque chose intact, de le maintenir dans le même état* »[409] c'est-à-dire « *maintenir hors de toute atteinte destructive, s'efforcer de faire durer, de garder en bon état ou dans le même état* »[410]. Cela signifie que ce « quelque chose », en l'espèce, un document, doit être maintenu et gardé pendant une certaine durée, dans le même état (ou état équivalent) qu'au moment de sa création/validation, en vue de l'utiliser ultérieurement. En effet, si le document n'a plus vocation à être utilisé, il n'y a aucun intérêt à le conserver. Aussi, la conservation d'un document peut revêtir un ou plusieurs enjeux en fonction du type de document : organisationnel (documentation permettant la bonne marche de l'établissement), historique (préservation du patrimoine informationnel de l'entreprise)[411], de recherche (réalisation de recherche statistique ou autre) ou encore légal (permettre d'utiliser un document comme preuve en cas de contentieux ou conservation obligatoire à la suite d'une disposition légale).

157. **Le choix du délai de conservation**. Le délai de conservation d'un document dépendra de plusieurs facteurs dont le premier est la présence ou non de donnée à caractère personnel en son sein. En effet, par principe, un document contenant des données à caractère personnel[412] ne peut faire l'objet d'une conservation indéfinie[413] sauf exceptions[414], contrairement à des documents n'en contenant pas. Or, il parait très compliqué et inopportun

[409] Larousse, *V° « conservation »*, nom fém.
[410] CNRTL, *V° « conserver »*, verbe trans.
[411] C. pén., art. 226-20.
[412] 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, JOUE, L 119, 04 mai 2016, art. 4 : « *une donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».
[413] Caroline ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé partagées, op. cit.*, p. 269. *« La conservation au delà de la durée prévue. Le nouvel article 226-20 du Code pénal est une reprise de l'ancien article 226-20 dans ses deux alinéas. Le premier alinéa prévoit la sanction du fait « de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la [Cnil] ». Le second prévoit la sanction du fait de traiter ces données conservées au delà de la durée prévue ».*
[414] Tel que le versement des documents en tant qu'archives définitives auprès des archives publiques, à des fins statistiques, de recherches ou historiques.

de conserver indéfiniment tous les documents d'une société notamment au regard du nombre de documents produits. Ainsi, comment définir la durée de conservation la plus appropriée ?

Tout d'abord, il est nécessaire de se référer aux dispositions légales et règlementaires qui, pour certains types de documents, fixent des durées de conservation. A titre d'exemple, les bulletins de paie d'un salarié doivent être conservés pendant une durée de cinq ans[415]. En cas de silence du Droit, il est nécessaire de se référer aux référentiels spécifiques ou tout autre document relatif à certains secteurs, comme les référentiels/délibérations de la Cnil (concerne les documents contenant des données à caractère personnel)[416], la documentation des archives publiques (n'est applicable qu'aux personnes morales de droit public et aux personnes morales de droit privé investies d'une mission de service public, mais peuvent être utilisées également dans le secteur privé).

Dans le cas où aucune source documentaire ne permet de fixer une durée de conservation pour un type de document, c'est à la personne morale ou physique de déterminer sa durée de conservation, tout en n'excédant pas, pour les documents contenant des données à caractère personnel, la durée nécessaire pour la réalisation de la finalité du traitement[417]. Cela signifie que ce type de document ne pourra être conservé pour une durée plus longue que celle nécessaire pour la réalisation du/des but(s) ou du/des objectif(s) pour lequel/lesquels le document a été créé.

158. **Une conservation longue pour les documents contenant des données de santé**. La Loi impose une durée de conservation très longue pour les documents contenant des données de santé. A titre d'exemple : les établissements de santé publics et privés ont l'obligation de constituer un dossier médical pour chaque patient hospitalisé. Ce dossier doit être conservé[418] pour une durée minimale de vingt ans à compter du dernier passage du patient au sein de l'établissement. Cela implique que ce délai est remis à zéro dès que le patient est à nouveau pris en charge dans l'établissement. De plus, si ce délai arrive avant le vingt-huitième anniversaire du patient, « *la conservation du dossier et prorogée jusqu'à cette*

[415] C. trav., art. L. 3243-4.
[416] Cnil, « Référentiel sur les durées de conservation des données de santé - hors recherche », *Référentiel.* Disponible à l'adresse : https://www.cnil.fr/ (consulté le 11/11/2021).
[417] 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, JOUE, L 119, 04 mai 2016, art. 5.
[418] C. santé publ., art. R. 1112-7.

date »[419]. En cas de décès du patient, son dossier est alors conservé pour une durée de dix ans à compter de cette date.

On constate déjà avec le dossier médical, que le délai de conservation des documents est extrêmement long et peut l'être davantage par la suspension de ce délai en cas d'introduction d'un recours gracieux ou contentieux.

De plus, cette durée de conservation imposée par le Code de la santé publique est une durée minimale. *« Il peut donc être envisagé de garder les dossiers médicaux pendant une période plus longue. Gageons que les pratiques tiendront compte de l'intérêt médical et scientifique, au-delà de la seule considération défensive »*[420]. C'est généralement ce qui est appliqué au sein des instituts de cancérologie au regard des pathologies traitées.

Outre le dossier médical regroupant une grande partie des documents de santé d'un patient, certains documents bénéficient d'une durée de conservation différente qui leur est propre comme les dossiers de recherche biomédicale ou les données relatives aux transfusions sanguines.

159. **La conservation des documents de santé à des fins probatoires**. Un des enjeux principaux dans la conservation des documents de santé est de pouvoir les utiliser comme preuve. Pour cela, le système utilisé pour la conservation des documents doit respecter les conditions posées par le Code civil (section 1). Or s'agissant de données de santé, des spécificités du Droit spécial relatif à ces données doivent être envisagées, permettant parfois d'aider à respecter les conditions du Code civil, et parfois, d'être un frein à leur application comme la durée de conservation extrêmement longue des documents (section 2).

[419] *Ibid.*
[420] Olivier DUPUY, « La réforme des règles de durée de conservation des dossiers médiaux gérés par les établissements de santé », *RDS*, 2006, n°11, pp. 294-297.

Section 1 : Le maintien de l'intégrité pendant la conservation du document

160. **L'intégrité comme critère de conservation**. Qu'il s'agisse d'un document électronique natif ou copie, le Code civil prévoit un critère permettant de déterminer le niveau de fiabilité que l'on peut accorder à un document sur le long terme : l'intégrité.

En effet, l'article 1366 du Code civil relatif à l'écrit natif électronique prévoit que ce dernier bénéficiera de la même force probante que l'écrit papier « *sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* »[421].

Quant à la copie, le critère d'intégrité apparaît dans un premier temps comme davantage secondaire. En effet, le premier alinéa de l'article 1379 du Code civil prévoit que « *la copie a la même force probante que l'original. La fiabilité est laissée à l'appréciation du juge.* »[422]. Or, aucun critère à ce stade, ne permet de déterminer ce qui est entendu par ce critère de fiabilité. En revanche, le deuxième alinéa vient poser des critères à respecter afin que la copie soit présumée fiable, dont le critère d'intégrité ; « *est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'Etat* »[423]. Comme cela a été démontré lors du titre précédent (partie 1, titre 1, chapitre 2, section 1, §1), le critère de fiabilité doit être entendu comme la compilation des deux anciens critères de fidélité et de durabilité de la copie ; la fidélité renvoie à la notion de reproduction à l'identique de la forme et du contenu du document, tandis que la durabilité renvoie à la notion d'intégrité pendant la conservation de la copie. Aussi, que la copie soit ou non présumée fiable, il apparaît que l'intégrité du document doit être garantie afin que la copie puisse être fiable et bénéficier de la même force probante que l'original.

161. **La conservation dans un environnement commun.** Il apparaît donc que l'écrit natif électronique et la copie électronique ont un critère commun à respecter : la garantie de leur intégrité pendant toute la durée de leur conservation. Aussi, il est nécessaire d'envisager en même temps les conditions d'application de ce dernier (§1), d'autant plus que

[421] C. civ., art. 1366.
[422] C. civ., art. 1379.
[423] *Ibid.*

la conservation des documents natifs et copies électroniques sera réalisée dans le même environnement informatique (§2).

§1 La preuve de l'intégrité

162. **La garantie de l'intégrité**. La question qui se pose est comment garantir l'intégrité du document natif ou copie électronique pendant sa conservation, permettant de lui conférer la même valeur probante que l'écrit papier ou original ? Le Code civil ne donne que très peu d'informations quant à l'application de ce critère, laissant une grande latitude à son application. Or qui dit latitude d'application du critère, dit latitude d'appréciation du juge, laissant un flou quant à la valeur réelle qui sera accordée à ce document.

Afin de garantir au mieux l'intégrité du document pendant sa conservation et emporter de la manière la plus certaine possible la conviction du juge, il est nécessaire de s'attarder sur les quelques indications d'application de ce critère énoncées par le Droit (A) afin de déterminer ce qui, *in fine*¸ sera l'un des critères décisifs emportant la conviction du juge (B).

A) Les conditions d'application énoncées par le Droit

163. **La présomption de fiabilité**. Qu'il s'agisse de l'original électronique signé ou de la copie électronique, le Code civil prévoit plusieurs niveaux de fiabilité du document, notamment la fiabilité simple et la présomption de fiabilité. S'agissant de la fiabilité simple, aucune indication quant à l'application du critère de fiabilité n'est donnée ; en revanche s'agissant de la présomption de fiabilité, les textes donnent davantage d'éléments en imposant le respect de certaines conditions. Cela s'explique pour deux raisons : le respect des conditions permet, d'une part, de présumer de la fiabilité d'un document et donc de lui conférer une haute valeur juridique, équivalente à un écrit papier ou à un original, et d'autre part, de renverser la charge de la preuve en cas de contestation de la fiabilité du document produit. Ce renversement de la charge de la preuve n'est pas neutre[424] lors d'un contentieux, puisqu'il détermine la partie devant apporter la preuve de la fiabilité d'un document ou l'absence de fiabilité. Dans certains cas, cette fiabilité sera capitale pour déterminer la finalité d'un contentieux. Aussi, ce renversement de la charge de la preuve doit être encadré par des conditions suffisamment objectives impliquant des conditions définies par les textes, tant pour l'écrit natif électronique (1) que pour l'écrit copie électronique (2).

[424] Gwendoline LARDEUX, « Preuve : modes de preuves », *Répertoire de droit civil - Dalloz*, 2019.

1) L'intégrité de l'écrit natif électronique garantie par la signature électronique

164. **L'intégrité de l'écrit natif électronique signé**. L'écrit natif électronique ne bénéficie pas à lui seul d'une présomption de fiabilité. En revanche, il est prévu que la signature, réalisée par un procédé électronique conforme aux conditions fixées par le Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique, permet de présumer de la fiabilité du procédé « *jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie* ». Il apparaît que ce n'est donc pas l'écrit électronique qui bénéficie d'une présomption de fiabilité mais la signature électronique utilisée : la signature électronique qualifiée.

Bien qu'il ne soit pas fait explicitement mention d'une présomption de fiabilité d'un document natif électronique signé par ce genre de procédé, on peut tout de même supposer que la présomption de fiabilité du procédé de signature s'étend à la présomption de fiabilité du document lui-même. En effet, on constate que l'utilisation d'une signature présumée fiable, permet d'identifier la personne qui a apposé la signature et de garantir l'intégrité de l'acte, deux conditions permettant de garantir au document électronique, la même valeur que celle du document papier.

165. **La preuve de l'intégrité**. La signature électronique qualifiée[425], c'est-à-dire présumée fiable, va permettre de garantir l'intégrité du document[426], non pas en empêchant que le document signé ne puisse être modifié, mais en détectant toutes les modifications ultérieures éventuellement réalisées[427]. Il suffira, alors de comparer les données de signature au moment *t0* (à la signature) et *t+1* pour déterminer si une modification est survenue.

Or, si la signature électronique qualifiée est le moyen permettant de garantir l'intégrité d'un document natif électronique dans le temps du document, *quid* des documents natifs électroniques signés par une signature électronique inférieure à la signature qualifiée et des documents natifs électroniques non signés ?

i. Les documents signés par une signature autre que qualifiée : pour rappel, dans le domaine de la santé, la signature qualifiée n'est ni utilisée et ni utilisable pour le moment, impliquant par principe, qu'un document natif électronique signé ne pourra être présumé fiable et donc

[425] Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, JORF n°0229, 30 septembre 2017, texte n°8.
[426] Paul-Aymeric LLOAN, « La signature électronique : garantie des exigences légales d'identification », *op. cit.*
[427] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014, art. 26.

intègre. Or les autres niveaux de signature permettent tout de même d'assurer et de démontrer l'intégrité du document, notamment par l'utilisation d'une signature avancée. En effet, le Règlement eIDAS prévoit qu'une signature électronique avancée doit répondre à certaines exigences dont celle d' « *être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable* »[428], à l'instar de la signature électronique qualifiée[429]. Donc l'utilisation d'une signature avancée permettrait de prouver l'intégrité du document.

ii. Les documents non signés : le Code civil reste muet quant aux moyens devant être mis en place pour assurer la garantie de l'intégrité du document non-signé.

2) L'intégrité garantie pour la copie présumée fiable

166. **L'intégrité de la copie électronique.** Il est prévu que la copie fiable bénéficie de la même force probante que l'écrit original, dont l'appréciation de la fiabilité est laissée à l'appréciation du juge. A ce stade, aucun élément ne permet de déterminer ce qui est entendu par une « copie fiable », ni ce qu'il est nécessaire de mettre en œuvre pour qu'elle le soit.

En revanche, l'article 1379 alinéa 2 du Code civil prévoit une présomption de fiabilité en indiquant d'une part, ce qui est attendu d'une copie présumée fiable[430] et d'autre part en donnant les conditions à respecter et à mettre en œuvre[431] pour qu'elle le soit. Ces conditions peuvent être scindées en deux temporalités : au moment de la création de la copie[432] et pendant sa durée de conservation.

167. **Les conditions relatives à la conservation**. Sur les huit conditions énoncées par le Décret d'application relatif à la copie présumée fiable, quatre d'entre elles concernent la conservation[433]. La conservation va concerner soit les modalités de conservation de l'écrit en tant que tel, soit la conservation d'éléments ou de documents particuliers.

---

[428] *Ibid.*

[429] En effet, le Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique prévoit que la signature électronique qualifiée *« est une signature électronique […] avancée […] créée à l'aide d'un dispositif de création de signature électronique qualifié […], qui repose sur un certificat qualifié de signature électronique […]* ». Aussi, pour être qualifiée, la signature doit tout d'abord répondre aux exigences imposées pour la signature électronique avancée, notamment la détection de toute modification.

[430] C. civ., art. 1379. Il prévoit qu'une copie fiable est « *une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'État* ».

[431] Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61.

[432] Ce point a été traité dans le titre précédent (partie 1, titre 1, chapitre 2, section 1, §2, B).

[433] FNTC, « Copie fiable – Numérisation fidèle et archivage électronique », *FNTC,* 2019. *« Pour ce faire, il est recommandé de s'appuyer sur les normes NF Z 42-013 ou NF Z 42-020 ».*

Deux conditions concernent les modalités de conservation de l'écrit :

i. La copie électronique doit être conservée « *dans des conditions propres à éviter toute altération de sa forme ou de son contenu* »[434]. Cette condition renvoie directement à la définition même de la notion d'intégrité en son sens le plus large et commun : l'absence de modification. Le procédé de conservation utilisé par l'établissement de santé, devra empêcher l'altération du document, ou au moins permettre d'en détecter les modifications éventuelles.

Une exception est en revanche introduite par le Décret permettant de modifier le document tout en considérant que cette modification n'est pas une altération. En effet, *« les opérations requises pour assurer la lisibilité de la copie électronique dans le temps ne constituent pas une altération de son contenu ou de sa forme* »[435]. La lisibilité est la possibilité de pouvoir avoir accès au contenu du document et que ce contenu soit intelligible ; c'est une des conditions majeures permettant de garantir l'intégrité du document. Si ce document n'est ni lisible et ni intelligible dans le temps, c'est qu'il ne sera plus accessible en tout ou partie, ce qui entraînera une altération et donc une perte d'intégrité.

Or la lisibilité du document pendant toute la durée de sa conservation est difficilement possible sans réaliser des opérations sur celui-ci, au regard de l'évolution constante et rapide des technologies et des durées de conservation pouvant être très longues. Aussi, pour pouvoir être lisible pendant toute leur durée de conservation, les documents doivent subir des opérations, telles que des changements de supports.

En revanche, même si ces opérations ne constituent pas une altération, celles-ci doivent être tracées et donner lieu « *à la génération d'une nouvelle empreinte électronique de la copie* »[436].

ii. L'accès au(x) dispositif(s) de conservation doit faire « *l'objet de mesures de sécurité appropriées* »[437]. Mais de quel accès parle-t-on ? De l'accès de personnes au sein même de l'établissement ou de l'accès par des personnes extérieures ? Les deux sont à envisager. Le dispositif de conservation doit tout d'abord être protégé des accès extérieurs, afin d'éviter le vol de données ou de documents, ou encore leur altération. En effet, la conservation de documents de manière dématérialisée implique que l'ensemble des documents peut être

[434] Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 4.
[435] *Ibid.*
[436] *Ibid.*
[437] Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 6.

accessible à distance par des hackers exploitant les vulnérabilités des systèmes d'information. D'après le rapport du 22 février 2021 de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), les rançongiciels[438] sont la « *menace la plus immédiate à l'encontre des établissements de santé »*[439]. Ces rançongiciels impliquent le chiffrement des données d'un système d'information, tels les dossiers patients d'un établissement de santé. Or ce chiffrement implique une modification du document et donc son altération.

Les altérations, qu'elles soient volontaires ou non, peuvent également être faites par les personnes internes à l'établissement. Aussi, la limitation des accès aux documents aux seules personnes pour qui ils sont nécessaires, réduit les possibilités d'altération.

Cette restriction d'accès en interne se justifie, au-delà de l'intégrité des données : elle permet la confidentialité des données et le respect du secret professionnel. Le principe étant que seules les personnes habilitées et en ayant l'utilité, ont la possibilité d'accéder aux documents et aux données afin de préserver le secret des informations traitées.

iii. Doivent être conservées aussi longtemps que la copie elle-même, les traces et les empreintes générées lors de la reproduction du document et de sa conservation[440]. En effet, ces traces et ces empreintes correspondent aux éléments permettant de prouver l'absence d'altération des documents dans le temps ; en cas de perte de ces éléments, il sera impossible d'en prouver l'intégrité.

De plus, ces traces et empreintes doivent être conservées « *dans des conditions ne permettant par leur modification »*[441]. Il apparaît que le document n'est pas le seul à devoir être intègre, les traces et les empreintes doivent l'être également. Ces éléments étant décisifs pour prouver l'intégrité du contenu du document, il est primordial de pouvoir s'assurer qu'ils n'ont pas eux-mêmes subi d'altération.

Aussi, pour prouver qu'un document est conservé de manière intègre, il est nécessaire de produire des traces et empreintes, mais il sera également nécessaire de montrer l'intégrité de ces traces et empreintes en démontrant leur absence de modification. Il sera donc nécessaire

---

[438] Le rançongiciel est définie par l'ANSSI comme ceci : « *technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoie à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange d'un mot de passe de déchiffrement* ».

[439] ANSSI, *Rapport sur l'état de la menace cyber sur les établissements de santé,* 22 février 2021. Disponible à l'adresse : https://www.ssi.gouv.fr/ (consulté le 21/01/2022).

[440] Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 5.

[441] *Ibid.*

de pouvoir prouver, non seulement l'intégrité du document par des éléments de preuve, mais aussi l'intégrité de ces éléments.

iv. Pour finir, les dispositifs et mesures de sécurité mis en place et utilisés pour réaliser la copie et la conserver, ainsi que tous les éléments de preuves produits permettant de garantir l'intégrité de la copie, doivent faire l'objet d'une documentation écrite et conservée, aussi longtemps que la copie[442]. Cette documentation permettra d'expliquer et montrer ce qui a été mis en place pour garantir la non-altération du document et donc sa fiabilité.

168. **Les conditions de la copie présumée fiable comme conditions pour l'ensemble des documents électroniques.** Au regard des précédents développements, on se rend compte que le Droit ne nous donne que très peu d'éléments sur ce qui est attendu pour pouvoir attester de la fiabilité d'un document original ou copie électronique. Seule la copie présumée fiable donne une liste objective de conditions à respecter, bien que l'application de ces conditions reste très subjective. Ces conditions permettent de donner des éléments sur ce qui est attendu par le juge, pour attester de sa fiabilité, notamment concernant sa conservation. Il apparaît opportun de se baser sur ces conditions pour mettre en place la conservation des copies électroniques de manière générale. Nous pouvons aller plus loin en incluant également les documents originaux. En effet, que les documents soient des originaux et/ou des copies, ceux-ci seront, la plupart du temps, conservés dans le même environnement informatique. On peut donc légitimement se baser sur les conditions énoncées pour la copie présumée fiable afin de garantir l'intégrité d'un document lors de sa conservation, que celui-ci soit un original ou une copie.

B) L'importance de la constitution du dossier de preuve

169. **Emporter la conviction du juge**. La fiabilité d'un document ne doit pas être systématiquement démontrée, sauf lorsque celle-ci est contestée par la partie adverse. Dès lors, que la fiabilité soit à démontrer par la partie productrice du document ou que l'absence de fiabilité soit à démontrer par la partie qui la conteste, l'enjeu est d'emporter la conviction du juge[443]. Pour cela, la partie en question devra établir par tout moyen que ce qu'elle avance

[442] Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 7.

[443] Frédérique FERRAND, « Preuve », *op. cit. « Le code civil et le code de procédure civile français ne contiennent pas de règle précise définissant le degré de conviction que le juge doit atteindre pour accepter un fait comme prouvé. Parfois, la loi impose au juge de tenir un fait pour avéré (par le jeu des présomptions légales par exemple) ; certaines fictions légales interdisent même au juge de statuer selon la réalité des faits qu'il a pu percevoir ».*

(la fiabilité ou l'absence de fiabilité) est avéré par des éléments concrets qui constitueront son dossier de preuves.

170. **La traçabilité comme élément constitutif du dossier de preuve**. Ce qui nous intéresse ici est de pouvoir démontrer que le document conservé est bien intègre. Comme vu précédemment, pour qu'un document soit intègre, celui-ci doit être stable, c'est-à-dire ne pas avoir été altéré entre le moment de sa production et celui de sa restitution. Pour que ce document puisse être restitué, parfois de nombreuses années après sa production, ce dernier doit être lisible et intelligible, ce qui représente une condition majeure, à une époque où la technologie est en constante évolution. Les opérations réalisées pour permettre la lisibilité entraînent inévitablement une modification du document initial ; celle-ci n'est pourtant pas considérée comme une altération du document. Or, comment montrer au juge de manière concrète la stabilité et la lisibilité du document ? Par la traçabilité qui est une composante nécessaire à l'intégrité de ce document.

La traçabilité de manière large est définie comme la *« possibilité de suivre un produit aux différents stades de sa production, de sa transformation et sa commercialisation, notamment dans les filières alimentaires »*[444]. Transposée au monde informatique, la traçabilité d'un document électronique consiste à permettre de suivre les événements survenus sur un document. Monsieur Dimitri Mouton, Président de la société Demaeter[445] défini la traçabilité comme *« la capacité à suivre ou à reconstruire un historique fidèle des événements qui se sont déroulées au sein de ce système »*[446]. Les traces seront structurées de manière à conserver les informations suivantes : qui (utilisateur humain ou module technique) ; quoi (événement qui s'est déroulé et les éléments de contexte indispensables à l'interprétation ultérieure de la trace) ; quand (la date et l'heure de l'événement). Il est possible grâce aux traces de déterminer ce qui s'est passé durant tout le cycle de vie d'un document, et ainsi d'en raconter son histoire. La traçabilité est notamment une des conditions énoncées par le Décret relatif à la copie fiable, en imposant la conservation des empreintes et des traces produites lors de la reproduction de la copie, mais également pendant sa conservation. Grâce à la traçabilité, il serait possible de déterminer qui a modifié un document, quelle modification a été réalisée et quand cette dernière a eu lieu. Aussi *a contrario*, l'absence de trace de modification permettra

[444] Larousse, *V° « traçabilité »*, nom fém.
[445] DEMAETER, « présentation », disponible à l'adresse : https://www.demaeter.fr/ (consulté le 29/03/2021) : *« Demaeter est un cabinet de conseil spécialisé dans l'accompagnement des projets de dématérialisation, et doté d'une forte expertise dans le domaine de la sécurité »*
[446] Dimitri MOUTON, « Traçabilité et gestion de preuve », *Demaeter*. Disponible à l'adresse : https://www.demaeter.fr/ (consulté le 12/05/2021).

d'attester la non-altération du document et donc son intégrité. Comme l'a justement dit Alain Bensoussan, *« on sent bien que la fiabilité de la copie devient surtout une question de traçabilité »*[447].

171. **La traçabilité comme manifestation de la vérité.** La traçabilité apparaît comme un élément majeur de la manifestation de la vérité, *a contrario* son absence permettrait de la dissimuler. Prenons un arrêt de la Cour de cassation du 16 mai 2012 pour illustrer les propos[448] ; en l'espèce, un gynécologue obstétricien a réalisé un accouchement le 29 juillet 2000 à la suite duquel, l'enfant est né avec un handicap cérébral moteur important. Ce dernier a été poursuivi pour blessures involontaires. « *Lors des débats, le compte rendu d'accouchement présenté par la sage-femme a mis en évidence que le médecin avait ajouté des éléments sur celui-ci avant d'en remettre un exemplaire aux parents »*[449]. En effet, cette dernière avait envoyé une copie du compte-rendu à son assureur, montrant clairement que le document avait été modifié par la suite. « *La cour d'appel* [d'Aix-en Provence] *rappelle que* « *si des corrections d'un rapport médical qui doit être le fidèle reflet du déroulement de l'intervention ne sont pas interdites, les ajouts, rectifications ou précisions apportés ne peuvent être inclus dans le corps du document à peine de porter atteinte à sa sincérité mais à la suite pour en expliquer es motifs et les identifier ». Or les modifications apportées ont altéré la sincérité des faits »*[450]. Si la sage-femme n'avait pas transmis la copie de ce compte-rendu, les modifications effectuées par le gynécologue obstétricien seraient passées inaperçues entravant la manifestation de la vérité. L'informatique et plus exactement la traçabilité permet de pallier ces comportements, d'autant plus que « *la Cour de cassation souhaite que les comportements faisant obstacle à la manifestation de la vérité puissent être largement réprimés »*[451].

172. **La documentation primordiale**. La seule absence de trace permet-elle alors à elle seule de démontrer l'intégrité ? Ne pourrait-on pas penser que s'il n'y a pas de traces, c'est qu'elles n'ont pas été mises en œuvre ? Pour éviter cela, une documentation détaillée doit être réalisée.

La documentation est également une des conditions prévues par le Décret relatif à la copie présumée fiable. Elle permet de décrire concrètement ce qui a été mis en place pour garantir

[447] Polyanna BIGLE, « Quand la numérisation de document intègre le droit français », *op. cit.*
[448] Cass. Crim., 16 mai 2012, n°11-83.834, publié au bulletin.
[449] Marion GUIGUE, Anne PONSEILLE, « Condamnation de l'obstétricien pour altération d'un document concernant un délit pour faire obstacle à la vérité », *RDS*, 2012, n°49, pp. 612-614.
[450] *Ibid.*
[451] *Ibid.*

l'intégrité du document : le choix du dispositif de conservation, les mesures de sécurité mises en place afin de ne subir aucune attaque malveillante extérieure ou éviter l'altération de document par des personnes internes à l'établissement (restriction d'accès aux données, utilisation de support non modifiable), la traçabilité des actions menées sur le document (avec la liste des traces générées) etc.

La documentation est le résultat écrit des procédures mises en place au sein de l'établissement et permettra de démontrer que grâce aux solutions, actions, et dispositifs mis en place, le document produit à un instant *t+1* correspond au document produit à un instant *t.* Encore faut-il concrètement respecter ce qui est écrit dans la documentation.

173. **Le dossier de preuve comme élément déterminant ?** Bien que la traçabilité et la documentation ne soient pas les seuls éléments nécessaires pour attester de l'intégrité d'un document lors de la conservation, il s'agit d'éléments concrets et tangibles pouvant être présentés devant un juge, tant pour l'écrit copie électronique que pour l'écrit original électronique.

§2 La technologie comme critère du Droit

174. **L'écrit papier comme référence.** A la lecture des textes, il apparaît que même si le document papier et le document électronique peuvent bénéficier de la même valeur juridique, le papier reste le point de référence. En effet, l'article 1366 du Code civil établit la valeur juridique de l'écrit électronique, en se basant sur l'écrit papier. Or pour avoir la même valeur juridique que l'écrit papier, l'écrit électronique doit remplir certains critères qui sont induits pour l'écrit papier tels que la conservation du document de manière à préserver son intégrité pendant toute sa durée d'utilité administrative[452]. Aussi, l'enjeu de la conservation d'un document électronique *« consiste à apporter des garanties de sécurité afin de remplir les fonctions juridiques traditionnellement attachées au papier, mais dans un univers informatique ! »*[453] dans lequel par principe, les données « *peuvent être écrasées, […] sont volatiles et modifiables par nature »*[454]. C'est pour cela que le Droit impose pour l'écrit

[452] La durée d'utilité administrative est la durée pendant laquelle les documents doivent être conservés et doivent pouvoir être utilisés soit au regard de leur utilité pour celui qui les conserve, soit parce que le Droit impose une durée de conservation à respecter, ou encore au regard de leur utilité juridique. Cette durée d'utilité administrative comprend les deux premiers âges des archives (courant et intermédiaire).
[453] Eric A. CAPRIOLI, « Cadre jurxidique de l'archivage et régime juridique des tiers archiveurs », 2013. Disponible à l'adresse : https://www.caprioli-avocats.com/ (consulté le 01/05/2021).
[454] *Ibid.*

électronique (copie ou original) des conditions à respecter plus ou moins détaillées selon le niveau de fiabilité que l'on peut accorder au document.

175. **L'outil électronique comme gage d'intégrité**. Comme on a pu le voir, pour qu'une copie électronique soit présumée fiable, cette dernière doit être conservée dans des conditions permettant de garantir son intégrité (stabilité, lisibilité et traçabilité), grâce à la mise en place de contrôles d'accès (confidentialité) et d'une sécurité appropriée. Or tous les documents n'ont pas l'obligation de respecter ces conditions[455] pour bénéficier d'une valeur probante, ils doivent simplement être conservés de manière à préserver leur intégrité. Qu'il s'agisse d'un écrit électronique original ou copie, ce dernier devra être conservé dans un environnement électronique permettant de maintenir son intégrité. La technologie choisie par l'établissement pour conserver ces documents (A) déterminera la valeur probante qu'il souhaite pour chacun d'eux (B).

A) Les outils de conservation

176. **Quel outil choisir ?** Le Code civil impose que les documents électroniques originaux et copies doivent être conservées de nature à maintenir leur intégrité. Etant sur support électronique, les documents devront également être conservés de manière dématérialisée grâce à des outils technologiques permettant la conservation. Or, à l'ère du numérique, les technologies sont multiples et abondantes ; quel(s) outil(s) choisir pour permettre à ces documents de santé, de conserver leur valeur probante ? Le Droit français n'impose pas l'utilisation d'une technologie particulière laissant toute latitude aux professionnels quant aux choix des solutions à utiliser.

177. **La conservation et les notions voisines**. La notion de conservation est automatiquement associée aux notions de sauvegarde, de stockage ou d'archivage, qui sont considérées comme étant des synonymes de la conservation et donc des notions interchangeables. Bien que ces termes soient tous associés dans le langage courant, ils ne sont pas pour autant équivalents[456]. Pour déterminer ce qui les différencie mais également ce qui les relie, commençons par définir clairement la notion principale : la conservation.

[455] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61.
[456] Caroline ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit*, pp. 206-207.

L'idée même de conservation est de garder intact quelque chose, en l'espèce le document et son contenu, dès sa production, jusqu'à sa destruction éventuelle. Il y a donc deux éléments à prendre en compte : la durée (le temps que l'on souhaite pouvoir utiliser le document, peu importe son utilité (administrative, juridique, historique, recherche etc.) et l'absence d'altération (par sa modification ou sa destruction), renvoyant directement à l'intégrité. L'idée sous-jacente de la conservation introduite dans le Code civil est de lui conférer une dimension juridique, mais également un point de départ et de repère permettant de définir *a minima* ce que doit permettre l'outil utilisé.

L'archivage, le stockage ou encore la sauvegarde quant à eux, semblent davantage être des outils ayant comme finalité commune la conservation des documents. Pour autant, la conservation à elle seule ne suffit pas, puisque le Code civil n'a pas simplement évoqué l'obligation de conserver le document, mais que cette conservation devait être réalisée de manière à garantir son intégrité. Il s'agit donc les dispositifs de maintien de l'intégrité qui vont permettre de différencier et distinguer les outils de conservation ainsi que leur usage.

178. **L'archivage électronique à valeur probante**. Par principe, tous les documents produits au sein d'un établissement sont des archives au sens du Code du Patrimoine. En effet, une archive est définie comme étant « *l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité* »[457]. Aussi, dès lors que l'on parle de conservation d'une archive, on pense inévitablement à l'archivage au sein d'une salle des archives. Or l'archivage va bien au-delà du simple fait de conserver un document. L'archivage correspond à un ensemble d'actions réalisées permettant de gérer une archive pendant tout son cycle de vie, notamment son tri, son classement, son organisation, sa conservation ou encore sa sécurisation. Dès lors que le document est dématérialisé, son archivage l'est également et est défini comme « *l'ensemble des actions mises en œuvre pour réunir, identifier, sélectionner, classer et conserver des contenus numériques sur un support sécurisé, dans le but de les exploiter, de les rendre accessibles dans le temps, puis éventuellement les éliminer* »[458].

[457] C. patr., art. L. 211-1.
[458] Norme AFNOR NF Z 42-013 sur l'archivage électronique, 2020.

L'archivage électronique ne se limitant pas au seul fait de conserver un document mais mettant également en place des éléments garantissant l'intégrité du document comme la sécurité et son accessibilité dans le temps, tend à le placer comme outil de l'intégrité[459].

D'après la doctrine, l'archivage électronique *via* un Système d'Archivage Electronique certifié par l'AFNOR est effectivement l'outil suprême permettant de garantir l'intégrité d'un document dans le temps. Dès 1999, l'AFNOR a élaboré une norme NF Z42-013 relative à l'archivage électronique, donnant des recommandations aux professionnels sur « *la conception et l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes* »[460]. Dès lors, le principe était d'utiliser des systèmes d'information permettant de garantir l'intégrité du document pendant toute sa conservation. Au fil des années, cette norme a fait l'objet de plusieurs modifications[461] au regard des évolutions tant juridiques que technologiques, garantissant toujours plus la démonstration du maintien de l'intégrité du document (notamment en traitant les questions de traçabilité, de lisibilité, de documentation ou encore de sécurité qui sont des conditions à remplir pour présumer de la fiabilité de la copie) et a introduit le concept de SAE.

Cette norme est considérée comme faisant l'état de l'art en la matière mais n'est pas d'application obligatoire. Pour autant, « *la jurisprudence démontre que le recours à la norme volontaire ou la certification NF461 constitue un appui solide pour prouver la recevabilité du document en tant que preuve, en cas de litige ou de procédure juridique* »[462]. Cette norme a été complétée par une certification créée en 2012, « *laquelle garantit aux utilisateurs que des documents numériques soient capturés, archivés, restitués et communiqués en s'assurant que le document archivé garde la même valeur que le document d'origine pendant toute la durée de conservation* »[463]. Aussi peut-on considérer que l'utilisation d'un SAE certifié NF 461[464]

[459] En effet, avant même la réforme de 2016, l'archivage électronique était vu comme un moyen garantissant l'intégrité du document. *« Les archivistes peuvent d'ores et déjà valoriser l'utilité de l'archivage électronique pour constituer un faisceau de preuves à même d'emporter la conviction du juge dans les cas où le régime de la preuve est libre, notamment pour prouver la conservation de l'intégrité du document ».* (Antoine MEISSONNIER et Rémy ROQUES, « L'archiviste, les normes et le droit », *Gazette des archives*, 2015, n°240, pp. 135-151).

[460] Afnor, « NR Z42-013 - Archivage électronique – Recommandations et exigences », *Afnor éditions*, 2020.

[461] Création en juillet 1999, puis modifications en décembre 2001, mars 2009 et octobre 2020.

[462] Afnor, « FAQ Archivage électronique – qu'est ce que l'archivage à vocation probatoire ? En quoi cette norme peut-elle me permettre d'y accéder ? », disponible à l'adresse : https://www.afnor.org/numerique/faq/ (consulté le 23/08/2021). Et notamment l'arrêt CA Lyon, 6ème, 3 sept. 2015, n° 13/09407.

[463] Afnor, « FAQ Archivage électronique – pourquoi une norme sur l'archivage électronique ? », disponible à l'adresse : https://www.afnor.org/numerique/faq/ (consulté le 23/08/2021).

[464] La liste des établissements bénéficiant de la certification NF 461 est disponible à cette adresse : https://certificats-attestations.afnor.org/referentiel/NF461

permet de garantir la valeur probante d'un document à long terme et, est l'outil permettant de présumer de la fiabilité du document électronique[465].

179. **L'archivage électronique, qu'un moyen.** Or la question qui se pose est de savoir si l'archivage est « le » moyen permettant de conserver le document de manière intègre. L'archivage est un des moyens, mais n'est pas le seul moyen et ce, pour trois raisons :

i. Le Code civil ne fait pas mention de l'archivage. Si l'archivage était le seul moyen pour garantir l'intégrité dans le temps du document, le Code civil ou un des décrets d'application auraient fait la mention expresse de l'archivage, ce qui n'est pas le cas.

ii. Tous les documents étant des archives, cela laisse penser qu'une archive est obligatoirement conservée grâce à un système d'archivage, au regard de la racine commune des termes. Or ce n'est pas le cas. Un document peut être conservé en étant stocké sur un ordinateur, sans pour autant être archivé dans un système dédié. Le document sera simplement enregistré sans les autres composants de l'archivage comme le classement, ou la gestion des migrations de support, permettant la lisibilité du document. Ce stockage va bien permettre la conservation du document, mais va-t-il garantir son intégrité ? Peut-être, mais encore faut-il le prouver. Il sera plus compliqué de prouver l'intégrité du document par simple stockage, en l'absence d'éléments tels que la traçabilité, ou de mesures de sécurité appropriées, mais cela ne signifie pas pour autant que le document n'est pas resté intègre.

iii. Les textes n'imposant pas d'outil particulier, l'utilisation d'un système d'archivage électronique n'est, par principe, pas obligatoire. De plus, comme on a pu le voir, l'utilisation d'un SAE permettrait d'avoir le plus haut niveau de confiance quant à l'intégrité du document, or, tous les documents n'en ont pas besoin, car tous les documents n'ont pas la même importance.

B) Un outil pour un type de document

180. **Le niveau de fiabilité de l'écrit dépendant de l'outil technique.** Comme montré ci-dessus, la doctrine et la jurisprudence s'accordent à dire que l'utilisation d'un SAE conforme à la norme NF Z42-013 voire certifié NF 461 permet de garantir l'intégrité du document dans le temps conférant à l'écrit un haut niveau de fiabilité. Or d'autres outils tels que des outils de stockage, de sauvegarde, de gestion électronique de documents, ou même

[465] En effet, de nombreux arrêts montrent que le respect de la norme NF Z42-013 est un réel atout pour prouver la fiabilité du document électronique à long terme. CA, Douai, 2e ch. 2e sect., 19 décembre 2019, n°18/06253.

d'archivage, mais non conforme à la norme, vont bien permettre de conserver le document mais la garantie de son intégrité sera plus difficile à démontrer. C'est pourquoi en fonction du niveau de fiabilité que l'on souhaite accorder au document, certains outils seront plus adaptés que d'autres.

181. **Le référentiel force probante de l'ANS.** Au sein de son référentiel force probante[466] relatif aux documents contenant des données de santé, l'ANS décrit des niveaux de paliers à respecter en fonction du type de document, ainsi que les mesures de sécurité devant être mises en place lors de leur conservation.

Une distinction est réalisée selon qu'il s'agisse des documents électroniques originaux ou copies. Concernant la copie, les mesures de conservation sont les suivantes en fonction du type de document[467] :

	Palier 1	Palier 2	Palier 3
Type de document	Documents communiqués par la personne prise en charge (sans conséquence d'ordre médical sur la prise en charge)	Documents contenant des données de santé, mais ne faisant ni partie du palier 1, ni du palier 3	Document contenant l'expression de la volonté du patient
Niveau de fiabilité à accorder	Faible	Moyen	Fort
Mesures concernant la conservation de la copie	Confidentialité PGSSI-S	Archivage sécurisé mais non nécessairement certifié tel qu'un SAE (les exigences minimales portent sur la confidentialité, la sécurité, la disponibilité, le contrôle des accès, la traçabilité, l'intégrité)	SAE certifié conforme à la norme NF Z 42-013 dans sa dernière version

Aussi dès lors qu'une copie contiendrait des données de santé, elle devrait être conservée dans un système d'archivage, excluant les autres outils de conservation telle qu'une GED[468].

[466] Le référentiel force probante, faisant partie de la PGSSI-S.
[467] ANS, *Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation,* PGSSI-S, 2021.
[468] Une GED (gestion électronique de documents) est un outil permettant principalement de classer, de gérer (modification de documents, suppression etc.) et d'exploiter des documents en vue d'une utilisation courante. Par principe, une GED n'a pas vocation à conserver les documents sur le long terme, notamment les archives

Pour les documents natifs numériques, le choix des mesures de conservation dépendra davantage du niveau de signature utilisé, qui lui-même est dépendant du type de document (excluant par principe les documents natifs non signés)[469].

	Palier 1	Palier 2	*Palier 3*
Mesures concernant la conservation d'un document natif	Respect des exigences de disponibilité, d'intégrité et de confidentialité Sauvegarde Application de la PGSSI-S	Respect des exigences de disponibilité, d'intégrité et de confidentialité (l'espace de conservation n'est pas nécessairement un espace d'archivage mais peut être une GED) Sauvegarde ou redondance centralisée Contrôle d'accès	Archivage sécurisé mais non nécessairement certifié conforme à la norme NF Z 42-013

Il apparaît que pour l'ANS, le mode de conservation minimal à respecter sera tout d'abord dépendant de l'état du document, c'est-à-dire s'il est une copie ou un original. En effet, pour la copie, dès lors qu'un document contient des données de santé, la conservation doit être réalisée par un système d'archivage voire un SAE certifié ; tandis que pour l'original numérique, les modalités de conservation sont moins drastiques laissant la possibilité d'utiliser une GED (sous réserve que les documents ne puissent être modifiés ou supprimés avant la fin de la DUA) et n'imposant pour aucun document l'utilisation d'un SAE certifié.

On peut s'interroger sur les motifs de cette distinction. Est-ce une sécurité supplémentaire pour la copie, au regard de son statut ? En effet, même si la copie peut avoir la même force probante que l'original, son équivalence dépendra de sa fiabilité. Sachant également que la réalisation une copie respectant le palier 2 ou 3 du référentiel peut entraîner la destruction des originaux, l'exigence d'une sécurité maximale pourrait justifier l'usage systématique d'un archivage qui permettrait de garantir la conservation intègre du document et donc sa fiabilité.

---

dites intermédiaires. Or certains logiciels de GED vont au-delà d'une GED traditionnelle embarquant des briques supplémentaires telles que le stockage ou encore la possibilité de figer un document empêchant son altération (modification ou suppression).

[469] ANS, *Référentiel force probante des documents de santé – Annexe 3 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques,* PGSSI-S, 2021.

De plus, n'avons-nous pas vu précédemment que l'utilisation même d'une signature électronique permet de garantir l'intégrité du document ? Ce qui impliquerait la possibilité de mettre en œuvre des mesures de conservation plus souples.

182. **Une utilisation complexe.** Finalement, les modalités de conservation des documents dépendront de deux choses en santé, du type de données contenues dans le document et de la nature du document (copie ou original), complexifiant le choix des outils de conservation et leur mise en place, voire la multiplication des outils. Bien évidemment, les mesures énoncées par le référentiel sont des mesures minimales à appliquer, pouvant être dépassées selon les particularités de certains documents, et si le responsable de l'établissement le juge nécessaire.

Il apparaît tout de même que le SAE, qu'il soit certifié ou respectant simplement la norme NF Z42-013 est un gage réel de l'intégrité du document dans le temps et devient une composante essentielle du système d'information hospitalier. La difficulté persistante est davantage de déterminer quels sont les documents devant être archivés en son sein et lesquels ne le sont pas.

Section 2 : Les particularités du domaine de la santé

183. **Les documents de santé**. Dans le cadre de cette étude, un des enjeux est de déterminer la valeur juridique des documents dématérialisés contenant des données de santé (que l'on appellera documents de santé) et notamment leur valeur probante pour des besoins juridiques relatifs à la preuve. Le Code de la santé publique renvoie pour cela aux dispositions du Droit commun.

Pour autant, même si le Code civil définit les modalités permettant la reconnaissance de la valeur probante d'un document électronique, le contenu même de ce dernier, c'est-à-dire la nature des données, implique inévitablement et obligatoirement, l'application du Droit relatif aux données de santé, en plus du Droit civil, et tout particulièrement en ce qui concerne la conservation des documents de santé. En effet, les données de santé étant des données dites sensibles, des dispositions particulières doivent être mises en place afin de respecter les obligations légales applicables, tant au niveau national qu'européen.

Aussi les documents de santé sont régis par plusieurs Droits ayant des finalités différentes : l'un permet de garantir la valeur probante du document en tant que tel, indépendamment de la nature des données, tandis que l'autre s'attache à la protection devant être mise en place spécifiquement pour les données de santé. Pour autant, bien que poursuivant un but différent, certaines mesures devant être appliquées pour la protection des données de santé pourront servir à prouver la valeur juridique du document.

184. **Les spécificités relatives aux documents de santé**. Le choix de l'outil permettant la conservation des données de manière intègre devra donc dépendre du niveau de fiabilité que l'on souhaite accorder au document (dans un but probatoire) mais également prendre en compte et respecter les Droits annexes applicables aux données de santé (§1). Ces spécificités en santé pourront aider à prouver l'intégrité du document, mais pourront également être un frein à la dématérialisation totale des documents de santé (§2).

§1 Le respect des Droits annexes

185. **La donnée de santé**. La nature même de la donnée, de santé ou médicale, lui confère un statut particulier nécessitant la mise en place d'une protection accrue. Mais qu'entend-on exactement par donnée de santé ? *« Le législateur français n'a pas jugé utile de*

définir – de façon explicite- ce que sont ces données »[470] pendant de nombreuses années. « *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* »[471]. C'est finalement le Règlement Général sur la Protection des Données (RGPD) qui a donné une définition des données de santé commune aux états de l'union européenne : les données de santé sont les « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* »[472]. Comme on peut le constater, cette définition de la donnée de santé est particulièrement large permettant ainsi d'englober véritablement l'ensemble des données relatives à la santé d'une personne sans en exclure par mégarde. Or, qui dit définition large implique « *le champ libre à l'interprétation, à la casuistique* »[473] mais également la possibilité de faire entrer dans cette définition de très nombreuses données, qui n'étaient pas nécessairement visées. Le RGPD donne quelques exemples de ce qui entendu par une donnée de santé : les données concernent « *l'état de santé physique ou mentale passé, présent ou futur de la personne concernée* »[474], ou encore « *toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source* »[475]. Cette définition pousse certains auteurs à considérer que *« les données de santé ne sont pas uniquement des données issues de la relation de soin »*[476] mais s'étend également aux données obtenues dans le cadre des soins de manière générale ; les données sur une personne en vue d'une inscription pour une prise en charge sanitaire, et plus généralement toutes les données administratives, les informations concernant le remboursement des frais. *« Aussi, les données de santé, qu'elles proviennent ou*

[470] Isabelle DE LAMBERTRIE, « Qu'est-ce qu'une donnée de santé ? », *RGDM, num. spé. « Le droit des données de santé »*, LEH, 2004, p.18.
[471] Agathe VOILLEMET, *L'usage de la donnée médicale – Contribution à l'étude du droit des données,* Thèse dactylographiée, Lille, 2022, p.20.
[472] 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/C, JOUE, L 119, 04 mai 2016, art.4.
[473] Manon BLANCHARD, « Données de santé : une définition, trois critères », *Desmarais avocats*, 2018.
[474] 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/C, JOUE, L 119, 04 mai 2016, considérant 35.
[475] *Ibid.*
[476] Valérie OLECH, *Le secret médical et les technologies de l'information et de la communication*, *op. cit.*, p.178.

non d'une prise en charge sanitaire, et qu'elles soient ou non couvertes par le secret professionnel, répondent-elles, en principe au même régime »[477].

186. **Une notion précisée par la Cnil**[478]. La Cnil est venue compléter la notion de donnée de santé, expliquant que cette notion devait être « *à apprécier, au cas par cas, compte tenu de la nature des données recueillies »*[479] et a scindé les données de santé en trois catégories, aidant les professionnels à déterminer si une donnée est une donnée de santé ou non. Les trois catégories de données sont les suivantes :

i. Les données de santé par nature : il s'agit des données directement relatives à la santé telles que les antécédents médicaux, ou encore les résultats d'examens.

ii. Les données devenues des données de santé par croisement : certaines données à elles seules ne sont pas forcément des données de santé. Or dès lors que certaines données sont associées entres elles, elles deviennent des données de santé dès lors que l'on peut « *tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques…), croisement de la tension avec la mesure de l'effort, etc.* »[480].

iii. Les données de santé au regard de leur utilisation : il s'agit des données devenant des données de santé *« en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical* »[481].

Dès lors qu'une donnée ne fait pas partie d'une de ces catégories, elle n'est pas considérée comme une donnée de santé. A ce titre « *une application collectant un nombre de pas au cours d'une promenade sans croisement de ces données avec d'autres »*[482], n'est pas une donnée de santé.

---

[477] *Ibid.*
[478] Cnil, « Besoin d'aide – la Cnil, c'est quoi ? », disponible à l'adresse : https://www.cnil.fr/ : « *La Commission Nationale de l'Informatique et des Libertés (CNIL) a été créée par la loi Informatique et Libertés du 6 janvier 1978. Elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés. Ainsi, elle est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. […] Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction* ». A ce titre, la Cnil élabore des recommandations, des guides ou encore des référentiels notamment à destination des professionnels afin de les aider dans la compréhension du RGPD et de la Loi informatique et liberté et dans leur application.
[479] Cnil, « Qu'est-ce qu'une donnée de santé ? », disponible à l'adresse : https://www.cnil.fr/
[480] *Ibid.*
[481] *Ibid.*
[482] *Ibid.*

187. **Le régime juridique particulier de la donnée de santé**. Dès qu'une donnée est qualifiée de donnée de santé, un régime juridique particulier s'applique au regard de la sensibilité de la donnée nécessitant sa protection (A), et tout particulièrement lorsque la donnée sera conservée par un tiers (B).

A) La protection des données de santé

188. **Une protection ancienne**. Dès le IVème siècle avant J. C. les données de santé ont fait l'objet d'une protection particulière avec le serment d'Hippocrate[483], introduisant le devoir de garder le secret sur ce qui aura été confié et instituant ainsi le devoir de secret professionnel en santé. Ce devoir de secret professionnel apparaît autant utile que nécessaire au regard des données que le professionnel sera amené à manipuler, qui sont directement liées à l'intimité même de la personne. Or comme le dit l'adage de Louis Portes, « *il n'y a pas de médecine sans confiance, de confiance sans confidence, de confidence sans secret* »[484]. En effet, le patient doit pouvoir communiquer au professionnel ses plus intimes secrets sur son état afin de pouvoir bénéficier des meilleurs soins possibles. Mais sans garantie d'une stricte confidentialité, le patient sera réticent à se dévoiler engendrant une rétention d'informations. La confiance du patient envers le professionnel, et la confidentialité de ce dernier est le ciment même d'une relation de confiance et ainsi, d'une bonne prise en charge.

Encore aujourd'hui, le secret professionnel fait partie intégrante des obligations du professionnel de santé, et est consacré comme un droit pour le patient[485]. L'article L. 1110-4[486] du Code de la santé publique l'illustre parfaitement en rappelant au premier alinéa, le

---

[483] Valérie OLECH, *Le secret médical et les technologies de l'information et de la communication*, *op. cit. « Il n'est pas un ouvrage sur le « secret médical » qui ne fasse une place introductive au serment d'Hippocrate. Cette démarche a généralement vocation à souligner l'ancienneté de ce devoir qui fonde l'éthique médicale depuis plus de deux millénaires. Bien que le texte ait fait l'objet de multiples traductions qui sont encore l'objet de discussions, la formule relative au devoir de secret qui incombe a médecin contient toujours le même verbe : « taire ». Le médecin doit taire ce qu'il voit ou entend ».*

[484] Portes L. « Du secret médical », Communication à l'Académie des Sciences Morales et Politiques, 5 juin 1950, publiée dans son ouvrage posthume : *À la recherche d'une éthique médicale,* Masson, 1964, p. 153.

[485] En effet, un arrêt de la Cour de cassation (Cass. crim., 25 octobre 2011, pourvoi n°10-87.179) confirme que le patient est l'unique bénéficiaire du secret professionnel. C'est un droit pour lui et seulement pour lui. Un professionnel de santé ne peut pas l'invoquer. Pierre-Laurent VIDAL, « Le patient : unique bénéficiaire du secret médical », *RDS*, 2012, n°46, pp. 288-289. *« La question posée à la chambre criminelle était donc celle de savoir si le secret professionnel, institué originairement dans l'intérêt du patient, pouvait s'étendre aux informations données par des médecins visant leur confrère. La Cour de cassation répond par la négative en retenant que le secret professionnel visé par l'article R. 4127-4 du Code de la santé publique ne concerne nullement les rapports des médecins entre eux ou avec les directions des établissements médicaux au sein desquels ils sont amenés à traiter des patients mais est seulement établi dans l'intérêt des patients ».*

[486] C. santé publ., art. L. 1110-4 : « *Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code, le service de santé des armées, un*

droit pour le patient « *au respect de sa vie privée et du secret des informations la concernant* »[487], et à l'alinéa 2 le devoir pour tout professionnel intervenant dans le système de santé, de respecter le secret sur l'ensemble des informations concernant la personne prise en charge, venues à sa connaissance. On constate que le secret couvre bien plus que les seules données de santé en ne limitant pas le secret aux informations de santé mais en incluant l'ensemble des informations venues à sa connaissance, laissant libre la parole du patient.

De plus, on se rend compte que le champ du secret professionnel en matière médicale est plus large que celui strictement envisagé dans le code pénal ; il ne se limite pas à la divulgation d'une information devant être tenue secrète. L'article L. 1110-4 du Code de la santé publique « *précise qu'une personne ayant « obtenu » ou simplement « tenté d'obtenir » la communication d'informations soumises au secret médical est également susceptible d'être sanctionnée d'un an d'emprisonnement ou de 15000 euros d'amende. Ainsi la violation du secret médical ne serait pas uniquement entendue comme la « révélation » d'informations de la part du détenteur du secret mais également comme l'« accès » à ces informations par des tiers non autorisés »*[488]. Cette extension de l'obligation du secret professionnel permet de pouvoir sanctionner tout individu dont la volonté est de subtiliser des données à caractère secret. Cette approche est fort souhaitable avec l'utilisation des nouvelles technologies en santé.

189. **Le secret professionnel et l'émergence des nouvelles technologies**. L'émergence des technologies de l'information et de la communication a conduit à la dématérialisation des données de santé avec la création, de dossiers patients informatisés[489] ou encore d'outils permettant une prise en charge à distance. Or qui dit dématérialisation, dit création de nouveaux risques et dérives, tels que les cyberattaques, le traitement à grande échelle des données, mais également l'accès indu aux données (car facilité par le rassemblement de l'ensemble des données), mettant à mal le secret des informations

---

professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations la concernant.
Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé ».

[487] C. santé publ., art. L. 1110-4.

[488] Vincent BONNIOL, Madeline GANNE, « Protéger le secret du dossier médical hospitalier : une utopie ? », *RDS*, 2016, n°71, pp.336-347.

[489] Patrick MISTRETTA, « La loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Réflexions critiques sur un droit en pleine mutation », *JCPG*, 2002, doctr. 141. *« L'utilisation du support informatique est intrinsèquement porteuse d'insécurités pour le dossier médical (vols, copies de fichiers…) que multiplient les possibilités récentes de connexion à distance (internet, intranet…) ».*

concernant le patient[490]. « *Les menaces pour le secret médical*[491] *n'auront jamais été aussi grandes qu'avec la généralisation des transmissions informatisées de données, la constitution de dossiers médicaux dématérialisés et la multiplication des professionnels habilités à y accéder »*[492]. On pourrait même aller jusqu'à *« craindre une disparition totale du secret professionnel. Il n'en est rien. L'exemple du casier judiciaire prenant la forme d'un système automatisé centralisé depuis 1978 est éclairant. L'accès illicite au casier judiciaire par un magistrat utilisant ses codes d'accès pour des raisons non professionnelles est une violation du secret professionnel. Un magistrat de Nice a ainsi été mis à la retraite d'office en 2004 pour avoir utilisé son login de magistrat et son mot de passe en dehors d'une finalité judiciaire*[493]*. La tentation de « fouiller » dans les fichiers et autres dossiers numériques est un délit. Les curieux doivent savoir que les accès informatiques sont traçables et facilitent la preuve d'une violation du secret professionnel. »*[494] Le parallèle est donc possible en santé ; il

---

[490] Rodolphe BIGOT, « Le secret médical à l'épreuve du numérique », *BJDA*, 2021, n°75. Rodolphe BIGOT, va jusqu'à parler « d'effondrement » du secret « médical ». En effet, il fait énonce que de nouveaux risques sont apparus engendrant un effondrement possible à terme du secret qu'il qualifie de médical. Ces risques sont *: « le tsunami des cyberattaques de masse »*, le développement des technologies comme la blockchain ou encore l'intelligence artificielle, technologies présentant des risques pour le secret professionnel, ainsi que *« qu'un rempart normatif insuffisant »* comportant des sanctions inadaptées et peu appliquées.

[491] *« 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 »* (Bruno PY, « Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *RDS*, 2013, n°50 hors-série, p. 165). On préfèrera le terme « secret professionnel » au terme « secret médical » lors des développements suivants. *« Comme l'écrit avec juste raison le professeur Patrick Mistretta* (Patrick Mistretta, *Droit pénal médical*, LGDJ, 2013, § 3, p. 294-312), *il est une croyance erronée communément admise par quelques juristes et l'ensemble des professionnels de santé, au premier chef desquels se trouvent les médecins, qui consiste à affirmer l'existence d'un secret médical qui serait le propre du corps médical, d'autant plus que l'article 226-13 du Code pénal ne cite pas nommément les médecins, ni les autres professions de santé d'ailleurs.* (Alain MACRON, « Loi de modernisation de notre système de santé et partage d'informations de données de santé : consécration du secret partagé tous azimuts », *RDS*, 2016, n°74, p. 922). En effet, le secret médical au regard du sens de ces mots ne permet pas, de manière terminologique, de protéger toutes les données devant l'être, et suppose, à défaut, qu'il ne concerne que les professionnels de santé, voire des médecins. Or le champ du secret est vaste et ne concerne pas seulement les professionnels de santé, notamment au regard de l'évolution du droit en la matière (voir partie 2 de la thèse). Ainsi, *« lorsqu'ils emploient l'expression de secret « médical », les médecins commettent trois erreurs. La première est de croire qu'ils sont soumis à un secret propre aux médecins. La deuxième consiste à penser que le secret est limité aux données médicales. La troisième repose sur l'idée qu'il n'y aurait pas de secret d'un médecin à l'égard d'un autre médecin. Ce qui peut être résumé par une allusion aux officiants celtes. Le secret des druides, portant sur le culte, n'est communicable que de bouche de druide à oreille de druide... Cette conception est fausse et surtout juridiquement dangereuse »* (Bruno PY, « Le secret professionnel est-il un droit du patient ? », *RDSS*, 2022, n°02, pp. 225-234). En revanche, *« la notion de secret professionnel désigne à la fois des faits qui ne doivent pas être révélés et le voile que le professionnel doit conserver pour que les informations qu'il détient ne soient pas connues des tiers »*. (Frison-Roche (Marie-Anne), Secrets professionnels, Autrement, 1999, p. 18). Le terme secret médical est trop restreint, dans le cadre de nos développements, on préfèrera donc le terme secret professionnel davantage opportun, d'autant plus que certains textes de droit applicables utilisent ce terme plus que celui de secret médical.

[492] Didier TABUTEAU, « e-santé et nouvelles technologies », *op. cit.*, pp-3-5.

[493] CSM, 29 octobre 2004, pourvoi rejet par le CE 15 mars 2006, n°276042.

[494] Bruno PY, « Le secret professionnel est-il un droit du patient ? », *RDSS*, 2022, n°02.

est plus aisé de contrôler les accès[495] des dossiers patients informatisés grâce à la traçabilité[496], permettant, en cas d'accès indu, de sanctionner le professionnel fautif pour violation du secret professionnel[497].

On peut penser également, *« au risque d'effraction d'un dossier médical individuel lors d'un cambriolage chez un médecin* [qui] *pourrait succéder* [à] *la menace de consultations discrètes et systématiques de milliers de dossiers médicaux ou au contraire de mise en ligne d'informations médicales personnelles. De même, les NTI comportent, sur le champ de la santé, le risque évident d'un dévoiement à des fins commerciales mais aussi idéologiques ou sectaires* »[498] venant troubler le droit, pour le patient, de garder ses informations secrètes.

A titre d'exemple, la santé numérique est aujourd'hui un véritable marché économique tant pour les industriels avec la création de systèmes d'information dédiés que pour les hackers qui prennent pour cible les établissements de santé. L'ANSSI a publié le 22 février 2021 un rapport sur *« l'état de la menace cyber sur les établissements de santé » et notamment sur les cyberattaques par des rançongiciels[499] qui est à ce jour la « menace la plus immédiate à l'encontre des établissements de santé »*[500] surtout depuis 2019. Plusieurs centres hospitaliers français ont été victimes de ces rançongiciels tels que le CHU de Rouen ou encore le CH de Marmande-Tonneins impactant le fonctionnement de l'établissement. Très récemment, ce sont les hôpitaux de Vivalia, dont celui de Arlon qui ont fait les frais d'une cyberattaque en

[495] En juin 2015, une enquête de terrain a été réalisée par Vincent BONNIOL et Madeline GANNE pour connaître les pratiques des établissements de santé afin de déterminer les mesures mises en place pour garantir le secret professionnel du dossier patient. Cette étude a révélé, s'agissant des contrôles d'accès, qu'il s'agit d'une pratique difficile à mettre en place : (Vincent BONNIOL, Madeline GANNE, « Protéger le secret du dossier médical hospitalier : une utopie ? », *RDS*, 2016, n°71, pp. 336-347) *« Bien que la plupart d'entre eux [les professionnels] reconnaissent ne pas avoir la possibilité technique ni le temps d'effectuer cette vérification, certains sont toutefois parvenus à contrôler les droits d'accès. Reste souvent à déterminer s'il s'agit d'un accès mal intentionné, d'une erreur de manipulation de la part d'un membre du personnel ou d'un accès « bris de glace » légitimé par le seul intérêt du patient ».*

[496] Caroline ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé partagées*, *op.cit.*, p. 19. *« S'il est vrai que l'informatique multiplie les possibilités de transmission, parfois indue, de l'information, chaque consultation de données est tracée, ce qui est une garantie considérable pour peu que la personne concernée puisse en avoir connaissance. Le système informatique date et identifie toutes les personnes qui y ont accès. Le système peut également bloquer l'accès à certaines données tout en mémorisant la tentative, ce qui n'est absolument pas envisageable à l'ère des dossiers papier empilés sur les chariots des services hospitaliers ».*

[497] *« En novembre 2020, une infirmière de l'hôpital Nord Franche-Comté a été condamnée à une peine d'amende pour violation du secret professionnel pour avoir consulté à plusieurs reprises le dossier médical informatisé d'une patiente qui ne se trouvait pas dans son service, mais était sa locataire à titre extra-professionnel ».* (Bruno PY, « Le secret professionnel est-il un droit du patient ? », *RDSS*, 2022, n°02.).

[498] Didier TABUTEAU, « e-santé et nouvelles technologies », *op. cit.*, pp-3-5.

[499] L'ANSSI définit le rançongiciel de la manière suivante : « *technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement ».*

[500] ANSSI, *Rapport sur l'état de la menace cyber sur les établissements de santé, op. cit.*

mai 2022. *« Au total [...] près de 200 serveurs informatiques et 1 500 ordinateurs »*[501] ont été infectés par le virus, obligeant les établissements à passer en mode dégradé ; presque la totalité des opérations non urgentes et des consultations ont été annulés à la suite de cette attaque. En dehors du rançongiciel lui-même, une des menaces est bien évidemment la divulgation de données de santé. En effet, l'ANSSI précise que « *la nature particulièrement sensible de ces données peut en faire des cibles d'intérêt pour des attaquants poursuivant des objectifs lucratifs ou d'espionnage* ».[502] Or le paiement de la rançon ne permet pas de garantir la restitution des données qui peuvent être supprimées, vendues ou encore divulguées.

Pour autant, même si l'introduction de l'outil informatique implique des bouleversements quant au respect du secret professionnel, *« la relation du patient au professionnel de santé est originairement une relation de confiance qui n'est pas mise en cause par les procédures qu'introduit l'informatisation. Mais dans la mesure où celle-ci a été perçue par des partenaires avertis comme un risque certain, une vigilance particulière est imposée au professionnel de santé. Certes, l'informatisation des données médicales nominatives ne veut pas dire levée du secret médical, mais sans aucun doute modification de sa protection »*[503].

190. **La protection des données à caractère personnel**. La protection des données de santé *via* la sécurité des SI, comme le DPI est un enjeu primordial pour les établissements de santé autant pour les protéger des menaces externes (cyberattaque) qu'internes (détournement de finalité, accès aux données) à l'établissement.

Ces données, avant d'être des données de santé, sont des données à caractère personnel[504] protégées par le RGPD[505]. L'objectif du RGPD est d'établir « *des règles à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données* [tout en protégeant] *les libertés et droits*

[501] Simon MARTIN, « Une rançon a été réclamée à l'intercommunale belge gérant notamment l'hôpital d'Arlon ou encore celui de Bastogne, situés tout proche de la frontière luxembourgeoise », *Luxemburger Wort*, 2022.
[502] *Ibid.*
[503] Jean-Claude CHOCQUE, « Impacts et enjeux de l'informatisation dans le système de santé », *La Gazette du Palais*, 2000, n°295, p. 15.
[504] 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/C, JOUE, L 119, 04 mai 2016, art.4. Les données à caractère personnel sont définies de la manière suivante : *« toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».*
[505] 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/C, JOUE, L 119, 04 mai 2016.

fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel »[506]. Le RGPD souhaite notamment encadrer le traitement[507] de données à caractère personnel afin de les protéger et responsabiliser les personnes morales ou physiques mettant en place ces traitements.

A ce titre, un ensemble de dispositions sont décrites permettant la protection des données, dont certaines sont à appliquer en fonction de la nature des données traitées, du contexte et des finalités du traitement ou encore des risques potentiels.

Par principe, les données de santé étant des données dites sensibles, leur traitement est donc interdit, sauf cas particuliers[508] tels que le consentement de la personne, ou encore la nécessité de les traiter pour la prise en charge du patient. Le niveau de protection à leur accorder est donc naturellement élevé impliquant par exemple, la réalisation de mesures de protection supplémentaires par rapport à d'autres données à caractère personnel, comme une analyse d'impact[509]. Cette analyse d'impact permettra notamment de déterminer les mesures de sécurité techniques et organisationnelles appropriées et adaptées aux risques encourus telles que : « *la pseudonymisation et le chiffrement des données à caractère personnel ; des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; une procédure visant à tester, à analyser et à évaluer*

[506] 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/C, JOUE, L 119, 04 mai 2016, art. 1.

[507] 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/C, JOUE, L 119, 04 mai 2016, art. 4. Le traitement est défini de la manière suivante : « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

[508] 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/C, JOUE, L 119, 04 mai 2016, art. 9.

[509] Cnil, « Analyse d'impact », disponible à l'adresse : https://www.cnil.fr/ : *« Une analyse d'impact sur la protection des données est une étude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.*
L'AIPD se décompose en trois parties : une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels ; l'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ; l'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données ».

régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement »[510].

191. **Un Droit adapté**. Cette obligation de protection et notamment de sécurité de la donnée de santé est réaffirmée au sein du Code de la santé publique missionnant l'ANS pour l'élaboration de deux référentiels, d'interopérabilité et de sécurité, devant être respectés par les services numériques en santé « *afin de garantir l'échange, le partage, la sécurité et la confidentialité des données de santé à caractère personnel* »[511]. Le référentiel d'interopérabilité (CI-SIS), *« vise à rendre la communication compréhensible et indépendante des filières technologiques grâce à un ensemble de conventions techniques entre les parties qui peuvent prendre la forme de convention d'usage comme le langage de programmation JAVA, ou de normes nationales ou internationales. Concrètement, les conventions interopérabilité conduisent à des spécifications techniques détaillées appelées spécifications d'interface, ou protocoles, que chaque concepteur se doit de respecter »*[512]. Quant au référentiel de sécurité, il correspond à la PGSSI-S[513] qui « *rassemble des référentiels d'exigences, des guides de bonnes pratiques et propose un cadre commun de niveau de sécurité des SI du secteur de la santé* »[514] et donc, permet de « *faire face aux risques menaçant les systèmes d'information de santé »*[515].

Les spécificités du domaine de la santé ainsi que le caractère sensible des données entraînent la nécessité de mettre en place des mesures de sécurité particulièrement élaborées et minutieuses. Ces mesures vont, au-delà la protection de la donnée, servir à prouver la valeur probante des documents. En effet, la PGSSI-S contient plusieurs référentiels permettant de répondre aux obligations posées par le Code civil. Le référentiel d'imputabilité va par exemple détailler les traces devant être mise en place au sein d'un SI afin de pouvoir « *attribuer à chaque utilisateur ou à chaque machine l'intégralité des actions qu'il a effectuées sur le système [*et*] s'assurer que chaque action est attribuée de façon univoque à*

[510] 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, JOUE, L 119, 04 mai 2016, art. 32.
[511] C. santé publ., art. L. 1470-5.
[512] Caroline ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé partagées, op. cit.,* p. 217.
[513] La PGSSI-S est composée de référentiels (sur identification des acteurs sanitaires, l'imputabilité, force probante etc.) et de guides pratiques (la mise en place d'un accès Wifi) disponibles à cette adresse : https://esante.gouv.fr/securite/pgssi-s/espace-de-publication
[514] ANS, « PGSSI-S ». Disponible à l'adresse : https://esante.gouv.fr/ (consulté le 16/07/2021).
[515] *Ibid.*

l'utilisateur ou la machine l'ayant effectuée »[516]. La traçabilité ou même l'absence de traces, permettra de démontrer l'intégrité du document et donc de prouver l'absence de modifications.

B) La conservation impliquant l'hébergement des données de santé

192. **L'hébergement de données**. Comme nous venons de le voir, les données de santé doivent bénéficier d'une protection particulière au regard de leur criticité. Cela est notamment réaffirmé par l'obligation de respecter la règlementation relative à l'hébergement des données de santé[517], dès lors que celles-ci font l'objet d'une conservation. Caroline ZORN-MACREZ définit l'hébergement comme étant une *« activité de commerce électronique proposant l'externalisation de la conservation de données électroniques, ainsi que des solutions associées, notamment d'archivage ou de stockage des données »*[518].

Cette règlementation « *définit les modalités et les conditions attendues »*[519] sur la sécurité à mettre en place lors de l'hébergement. « *Par cet encadrement, le législateur souhaite garantir la confiance dans les tiers auxquels des structures et des professionnels des secteurs sanitaire, social et médico-social confient les données de santé qu'ils produisent ou recueillent, notamment en mesurant l'impact de l'activité du prestataire sur la protection des données, au travers des critères de sécurité à l'état de l'art « disponibilité, intégrité, confidentialité et auditabilité (DICA) » notamment visés par l'ANSSI et les normes ISO* »[520].

193. **L'application de la règlementation**. Sont concernés par cette règlementation, les personnes réalisant l'hébergement de données de santé, « *pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même* »[521]. En sont donc exclues, les personnes physiques ou morales hébergeant par leurs propres moyens leurs données, c'est-à-dire, dès lors que la prestation d'hébergement n'est pas sous-traitée.

En effet, *« les centres médicaux n'ont pas pour vocation première d'héberger les serveurs informatiques nécessaires au stockage de leurs données de santé. L'option d'externalisation*

---

[516] ANS, *Référentiel d'imputabilité*, PGSSI-S, 2014.
[517] Cyrille CHARBONNEAU et Frédéric-Jérôme, « La dématérialisation des données médicales et les enjeux de leur hébergement », *La gazette du Palais*, 2002, n°351, p.23.
[518] Caroline ZORN-MACREZ, « CHRONIQUE MARTIENNE », DES DONNEES DE SANTE NUMERISEES. Brèves observations sur une réglementation surréaliste », *RDS*, 2010, n°36, p.339.
[519] ANS, *HDS – certification Hébergeur de Données de Santé*, disponible à : http://esante.gouv.fr/
[520] DSSIS, Ministère de la Santé, « Explication du champ d'application du cadre juridique de l'hébergement de données de santé », 2019.
[521] C. santé publ., art. L. 1111-8.

est alors un compromis acceptable, car en échange du coût financier du forfait, le prestataire se retrouve en charge de l'infrastructure informatique »[522]. Pour cela, le tiers hébergeur doit faire l'objet d'une certification[523] de conformité à la règlementation pour pouvoir héberger des données de santé[524] qui est divisée en deux types d'hébergement différents : l'infogérance[525] et la gestion de structures physiques. Dès lors que l'hébergeur propose ces deux prestations, il doit être certifié sur les deux périmètres. Cette certification est le gage de la protection adéquate des données de santé pour une durée de trois ans, faisant l'objet chaque année, d'un audit de contrôle et de surveillance.

194. **L'obtention de la certification.** L'obtention de la certification HDS repose sur la conformité au référentiel de certification élaboré par l'ANS[526] dont l'appréciation est réalisée par un organisme certificateur accrédité par le Cofrac. L'audit réalisé en deux étapes (documentaire et sur site) vérifie le respect de plusieurs normes ISO (en tout ou partie) sur la sécurité des SI[527], la gestion des service[528] et la protection des informations personnelles[529] ainsi que des exigences spécifiques à l'hébergement de données de santé et notamment le respect de la PGSSI-S. Aussi, la conservation externalisée implique de passer par un prestataire certifié HDS, qui, pour bénéficier de cette certification, doit mettre en place un SMSI (système de management de la sécurité de l'information) respectant de nombreuses conditions sur la sécurité de son SI relatives à l'authentification pour accéder aux données, la

[522] Sébastien CIPERE, *Un système de médiation distribué pour l'e-santé et l'épidémiologie*, Thèse dactylographiée, Clermont-Ferrand, 2016, p. 34.

[523] La liste des hébergeurs certifiés est disponible à cette adresse : https://esante.gouv.fr/labels-certifications/hds/liste-des-herbergeurs-certifies
Éric CAPRIOLI et Isabelle CANTERO, « Traitement et hébergement de données de santé : entre protection et risques », *Revue pratique de la prospective et de l'innovation,* 2021, n°2. En effet, l'hébergeur de données tiers doit obligatoirement être certifié. En cas d'absence de certification, il peut être mis fin d'office à l'hébergement. Dans un jugement récent, le tribunal judiciaire de Paris a ordonné la fermeture immédiate de deux sites internet permettant la prise de rendez-vous en ligne et traitant des données à caractère personnel. Un des motifs de sa décision est l'absence de certification de l'hébergeur, alors même que des données de santé été traitées. TJ Paris, 6 nov. 2020, n°20/54799.

[524] Avant la loi de modernisation de notre système de santé (n°216-41 du 26 janvier 2016), les hébergeurs tiers devaient faire l'objet d'un agrément dans les conditions définies par le décret n°2006-6 du 4 janvier 2006. Cet agrément a laissé la place à la certification HDS renforçant les garanties sur la sécurisation des données de santé.

[525] C. santé publ., art. R. 1111-9.

[526] C. santé publ., art. R. 1111-10. Une nouvelle version du référentiel HDS a été mis par l'ANS en concertation en 2020 pour laquelle la synthèse n'est pas encore disponible.

[527] Norme ISO 27 001 : Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information – Exigences.

[528] Norme ISO 2000-1 : Technologies de l'information - Gestion des services - Partie 1 : exigences du système de management des services - Technologies de l'information - Gestion des services - Partie 1: Exigences du système de management des services.

[529] Norme ISO 27018 : Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.

traçabilité des actions réalisées, les mesures de sauvegarde mises en place, ou encore la sécurité contre les intrusions.

195. **Une particularité française**. L'obtention de cette certification pour l'hébergement des données de santé par un tiers est une spécificité purement française. Cette contrainte juridique supplémentaire implique que les acteurs internationaux souhaitant héberger des données de santé françaises, se heurtent à des exigences vis-à-vis desquelles ils ne sont pas habitués. Le changement de règlementation intervenu en 2017 est venu assouplir ou tout du moins faciliter le respect des exigences devant être mises en place pour héberger les données de santé. Cette certification « *s'inscrit dans une approche plus internationale, facilitant l'obtention de l'autorisation à des acteurs peu familiers des spécificités françaises* »[530]. A titre d'exemple, « *cette procédure de certification s'inspire désormais largement de la procédure d'accréditation des dispositifs médicaux pouvant faire l'objet d'un certificat CE avant leur mise sur le marché, […] [et s'appuie sur] des normes internationales dans le cadre de l'évaluation du candidat à la certification (norme ISO 27001 et ISO/IEC 20000)* »[531] permettant un accès plus aisé à la certification pour les acteurs internationaux puisqu'ils sont davantage familiarisés avec ces exigences internationales.

196. **La particularité de l'archivage électronique externalisé**. Avant 2009, le recours à un archivage externalisé des archives publiques n'était pas possible. Depuis l'externalisation de l'archivage, celui-ci, notamment électronique, est possible sous réserve de l'obtention, par le tiers archiveur, d'un agrément délivré après l'obtention d'une « *certification correspondant aux normes relatives à l'archivage électronique* »[532]. En l'espèce, la certification visée est la NF 461 relative au système d'archivage électronique.

Cet agrément dispense *ipso facto* le prestataire de devoir passer la certification HDS, dès lors que l'archivage est réalisé sur support papier. En revanche, en cas d'archivage électronique, la certification HDS reste toujours obligatoire.

On constate qu'en matière de conservation électronique, l'utilisation d'un SAE certifié NF 461 bénéficie du plus haut niveau de fiabilité à ce jour.

197. **La conservation de la donnée de santé.** Au regard de la nature même de la donnée de santé et de sa qualification « sensible », un ensemble de dispositions lui sont

[530] Stéphanie ABDESSELAM, Laetitia GAILLARD, Daniel KADAR, « Données de santé : un vecteur d'innovation sous trop haute surveillance ? », *RJSP*, juin 2021, n°21, p. 42.
[531] *Ibid.*
[532] C. patr., art. R. 212-23.

applicables afin d'en assurer la protection, dispositions accrues dès lors que cette donnée est dématérialisée.

Cette protection juridique définie par les textes se matérialise par la mise en place d'une protection technique. Ce renforcement de la protection de la donnée de santé et ces mesures techniques vont également permettre de pouvoir prouver l'intégrité du document, grâce à la traçabilité et aux mesures de confidentialité et de sécurité mises en place. En effet, dès lors que les mesures de sécurité mises en place sont suffisantes pour protéger les données de santé (conformément à la certification HDS par exemple), elles le sont également pour prouver l'intégrité du document et sa fiabilité.

§2 Vers une dématérialisation totale en santé

198. **Le papier et la santé**. La valeur probante des documents sur support électronique est de manière générale régie par les articles 1366, 1367 et 1379 du Code civil ainsi que leurs Décrets d'application. Ces articles portent respectivement sur la valeur probante de l'écrit original sur support électronique ainsi que sur la copie (papier ou électronique). Cette avancée juridique permet de prendre en compte l'évolution de la société actuelle et de ses pratiques, notamment avec l'utilisation de plus en plus fréquente des technologies de l'information et de la communication. Or, bien que la dématérialisation fait partie aujourd'hui de notre quotidien, le papier reste tout de même un support utilisé notamment en santé (A) ce qui peut entraîner la (re)-matérialisation de documents, dont la valeur juridique n'est pas textuellement envisagée par le Code civil (B).

A) Les limites de la dématérialisation en santé

199. **Le document papier : toujours une utilité**. L'utilisation de documents sur support papier reste aujourd'hui encore une pratique répandue tant dans la vie personnelle que professionnelle et semble même nécessaire dans certains cas.

Dans le domaine de la santé, certains documents doivent être produits sur support papier, tels que les documents à fournir aux patients. Prenons l'exemple du certificat sportif. Jusqu'en mars 2022, dès lors qu'une personne souhaitait pratiquer un sport au sein d'un club affilié à une fédération sportive, la production d'un certificat médical attestant l'absence de contre-indication était obligatoire pour obtenir une licence[533]. Depuis, ce certificat n'est obligatoire

[533] C. sport, art. L. 231-2.

que dans des particuliers. Ce certificat réalisé par le médecin traitant était confié au patient sur support papier afin qu'il puisse le transmettre à son club. Serait-il envisageable, pour les cas nécessitant encore la production du certificat, de confier ce document par voie électronique ? Envisageable oui, praticable aujourd'hui non, mais bientôt peut-être.

200. **Vers le 100% dématérialisé ?** Envisageons plusieurs scénarios :

i. L'envoi du certificat directement au club sportif : le médecin est soumis au secret professionnel[534]. Ainsi, toutes les informations venues à la connaissance du médecin doivent rester secrètes et ne doivent pas être divulguées sous peine de sanctions[535], sauf dans les cas très restreints prévus par la Loi tels que l'échange et/ou le partage d'informations[536] entre acteurs de santé[537]. Le médecin n'a donc pas la possibilité d'envoyer le certificat directement au club, même si le patient lui donne son accord. En effet, le professionnel « *ne peut être délié du secret* »[538], seule la loi peut l'autoriser.

ii. L'envoi du certificat au patient de manière dématérialisée : Les données de santé sont des données sensibles et doivent être protégées. Leur traitement et leur hébergement, surtout par voie électronique doit faire l'objet de mesures de sécurité renforcées impliquant l'utilisation d'outils adaptés au domaine.

A titre d'exemple, l'envoi par messagerie électronique de documents contenant des données de santé doit être réalisé par une messagerie sécurisée. Or à ce jour, seuls les professionnels de santé peuvent bénéficier de cette messagerie sécurisée, ainsi que les acteurs du médico-social sous certaines conditions. Aussi, le patient est exclu des personnes pouvant en bénéficier ne permettant pas l'échange de données entre un professionnel de santé et un patient, *via* une messagerie électronique sécurisée.

La Loi du 24 juillet 2019[539], appelée « Ma Santé 2022 » vient modifier cela en prévoyant l'ouverture automatique (sauf opposition) et gratuite, pour chaque personne d'un espace

[534] C. santé publ., art. R. 4127-4.
[535] A titre d'exemple, en cas de divulgation d'une information médicale en dehors des cas prévus par la Loi est puni jusqu'à un an d'emprisonnement et 15 000 euros d'amende. C. pén., art. 226-13.
[536] C. santé publ., art. L. 1110-4 et ses Décrets d'application.
[537] La liste des acteurs de santé pouvant échanger et/ou partager des données de santé sur un patient est prévue à l'article R. 1110-2 du Code de la santé publique. On y trouve notamment les professionnels de santé (médecin, infirmière etc.), et les non-professionnels de santé tels que les assistants de service social, les ostéopathes ou encore les mandataires judiciaires.
[538] Caroline ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit.*, p-9.
[539] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1), JORF n°0172, 26 juillet 2019, texte n°3.

numérique de santé (ENS)[540] accessible en ligne à partir du 1er janvier 2022. Cet ENS permet pour chaque personne identifiée et authentifiée de bénéficier d'un seul espace regroupant tous les éléments nécessaires à la gestion de sa santé tels que l'accès à son dossier médical partagé (DMP), ou l'accès à *« une messagerie de santé sécurisée permettant à son titulaire d'échanger avec les professionnels et établissements de santé »*[541]. Cet ENS est véritablement vu comme un « *nouveau levier au service de la maîtrise des données personnelles de santé »*[542], de manière sécurisée.

Il serait donc envisageable pour le médecin traitant de mettre le certificat sportif au sein de l'ENS ou de l'envoyer par messagerie sécurisée au patient. En revanche, comment le patient transfèrera-t-il ce certificat au club sportif ? Sans transfert sécurisé, la chaîne de dématérialisation du certificat s'arrête là, obligeant la production d'une version papier du certificat.

201. **Les obstacles à la dématérialisation totale.** Malgré les évolutions technologiques et la favorisation de la dématérialisation des documents contenant des données santé, il apparaît tout de même que certains obstacles persistent ne permettant pas de dématérialiser à 100% tous les documents, parmi lesquels on peut retrouver :

i. L'impossibilité pour le professionnel de santé de transmettre les documents de santé d'un patient, à un non-professionnel du système de soins.

ii. L'utilisation par les professionnels de santé comme par le patient des outils mis à disposition permettant l'accès, l'échange et le partage d'informations de manière sécurisée. Avec la création de l'ENS, les échanges semblent propices, permettant peut-être de diminuer les documents produits en version papier. En revanche, cela sera conditionné par l'utilisation qui en sera faite, autant par les professionnels que par le patient.

iii. L'attachement par le patient au papier et à ses habitudes.

On constate que le document papier, notamment en santé a encore de beaux jours devant lui.

---

[540] Annelore COURY, Dominique PON, « Accélérer le virage numérique – rapport final », *Stratégie de transformation du système de santé*, 2018. L'ENS est « *un compte personnel unique, créé dès la naissance pour chaque citoyen, donnant accès à un portail personnalisé de services ainsi qu'à des applications de santé référencées. Il sera accessible sur tous supports (smartphone, ordinateur, tablette, borne interactive, ...) et permettra à chaque usager de gérer l'ensemble de ses données personnelles de santé ainsi que tous ses services numériques de santé* ». Rapport final – accélérer le virage du numérique.

[541] C. santé publ., art. L. 1111-13-1.

[542] Florence EON, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS*, 2019, hors-série, p. 55.

B) La valeur probante des documents (re)-matérialisés

202. **Les beaux jours du document papier.** Le document papier reste un support essentiel dans notre système de santé, surtout dès lors que le document est donné au patient. Cela implique qu'un document dématérialisé (nativement ou en tant que copie) pourra être matérialisé ou re-matérialisé sur support papier. Quelle est la valeur juridique de ces documents ? Le Code civil ne prévoit pas textuellement ce cas de figure ; reste à savoir si les dispositions actuelles peuvent suffire ou s'il faut des dispositions particulières.

203. **Les dispositions du Code civil suffisantes**. Repartons des textes du Code civil. Si l'on parle de matérialisation ou de re-matérialisation deux cas de figures se posent :

i. Soit le document est créé de manière numérique, dans le but de le matérialiser immédiatement si bien que le document validé est celui en version papier ; il s'agira par exemple d'un contrat rédigé de manière informatique, mais qui sera imprimé et signé de manière manuscrite. Même si le document est rédigé grâce aux TIC, sa validation étant réalisé sur le document papier, l'original sera donc le document papier. Dans ce cas, la matérialisation ne pose pas de difficulté puisque les règles concernant l'écrit original papier s'appliquent.

ii. Soit le document est créé et validé de manière électronique (donc est un document natif) puis est ensuite matérialisé. Il s'agirait ici de la production d'une copie, qui est prévue par le Code civil. Or, si l'on regarde le Décret permettant de bénéficier d'une copie fiable, la matérialisation ne semble pas être envisagée. Pour autant, même s'il n'y a pas de présomption de fiabilité possible pour cette copie, cela ne signifie pas qu'elle ne peut pas bénéficier d'une valeur juridique, puisque par principe, « *la copie fiable a la même force probante que l'original* »[543].

iii. Soit le document a été créé et validé sur support papier, puis dématérialisé, créant une copie électronique puis re-matérialisé, créant la copie papier, d'une copie électronique. Si l'on repart de l'article 1379, il est prévu une équivalence de valeur probante entre une copie et un document original. L'utilisation du mot « original » laisse à penser que la valeur probante de la copie de la copie ne semble pas du tout envisagée. Pourtant, le second alinéa prévoit qu' « *est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte* »[544]. Il n'est plus fait référence

[543] C. civ., art. 1379.
[544] *Ibid.*

à l'original mais simplement à l'acte. Or nous venons de dire que ce second alinéa ne prend pas en compte la copie matérialisée d'un original électronique.

La terminologie utilisée laisse planer un doute sur la valeur probante de la copie de la copie. En effet, pourquoi la copie de la copie ne pourrait-elle pas bénéficier d'une valeur équivalente à l'original dès lors qu'elle est fiable par rapport à la première copie, qui elle-même est fiable par rapport à l'original ?

Pourrait-on envisager que la copie de la copie puisse avoir la même force probante que le document original ? Si une copie fiable bénéficie de la même valeur que l'original, on peut légitimement penser que la copie fiable, d'une copie elle-même fiable, pourrait bénéficier de la même valeur que l'original et donc bénéficierai d'une valeur juridique propre.

204. **Les éléments de réponse apportés par la règlementation en santé**. Le Droit de la santé permet de donner quelques éléments de réponses sur la valeur probante des documents de santé matérialisés.

Le Code de la santé publique prévoit la possibilité pour un professionnel de santé[545] de matérialiser un document électronique à la demande du patient[546], « *pour répondre à un besoin lié à la prise en charge des personnes, qu'il s'agisse de leur permettre de faire valoir leurs droits (entente préalable, certificat d'arrêt de travail, pour ne citer que ces exemples) ou de contribuer à la prise en charge de la personne concernée* »[547]. Ce document matérialisé peut résulter d'une compilation d'un ou plusieurs documents existants, dès lors que leur sens et leur contenu n'est pas modifié. Cet article permet de créer un nouveau document à partir de données présentes au sein d'un SI, afin que ce document puisse être envoyé par voie électronique ou imprimé sur support papier. A titre d'exemple, « *les documents matérialisés dans le cadre de la solution e-prescription définie par le Ministère des solidarités et de la santé sont réputés conformes au référentiel »*[548].

205. **La notion de matérialisation.** La notion de matérialisation au sein de l'article L. 1111-19 du Code de la santé publique semble bénéficier d'un double sens : d'une part, elle est envisagée comme le résultat de la formalisation d'un document provenant d'un ou

[545] Un professionnel de santé ou établissement mentionné à l'article L. 1111-25 du Code de la santé publique.
[546] Ou de tout autre personne devant obtenir des documents, comme les titulaires de l'autorité parentale ou encore les ayants-droits.
[547] Rapport au Président de la République relatif à l'ordonnance n° 2017-29 du 12 janvier 2017 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique.
[548] ANS, *Référentiel force probante des documents de santé – Annexe 4 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la matérialisation des documents de santé numériques,* PGSSI-S, 2021.

plusieurs documents numériques (dont le résultat peut être en format électronique ou papier), et d'autre part, comme la manifestation tangible du document par sa matérialisation sur support papier.

Le document matérialisé envisagé par le Code de la santé publique ne serait donc pas une copie mais la création d'un nouveau document grâce à la compilation de document existants.

206. **La valeur probante du document matérialisé**. La valeur probante du document ainsi matérialisé est présumée équivalente à l'écrit numérique d'origine *« lorsqu'a été utilisé un procédé de production permettant d'insérer les métadonnées nécessaires à la garantie de l'identification de l'émetteur et de l'intégrité des données ainsi matérialisées »*[549]. Les métadonnées vont jouer un rôle très important pour prouver l'identité du signataire ou encore l'intégrité. Prenons l'exemple d'un document natif numérique signé électroniquement : en principe, la signature électronique n'a pas de représentation graphique visible sur le document, ce qui est *« l'un des principaux reproches […] fait à l'égard de la signature électronique »*[550], ou il peut parfois y avoir un cartouche de signature avec la mention « signé électroniquement par Nom Prénom », ce qui en soit ne permet pas de garantir réellement la signature, puisque c'est le contrôle informatique de la signature qui permet de déterminer sa validité. Aussi, pour garantir la validité de la signature, il sera nécessaire d'imprimer les métadonnées relatives à la signature attestant sa validité.

« La matérialisation des documents de santé numériques expose les acteurs du secteur santé-social principalement aux risques de falsification et d'usage de faux. Ainsi, les principaux enjeux auxquels le processus de matérialisation doit répondre sont : l'authentification des documents matérialisés ; la garantie de la force probante »[551]. Aussi, le document matérialisé doit d'une part permettre d'identifier la personne auteure du document, et garantir son intégrité dans le temps, notamment au moment de sa matérialisation, c'est-à-dire son contexte.

A l'instar du document natif numérique ou de la copie, les modalités à mettre en place pour garantir la valeur probante du document matérialisé dépendra de la valeur que l'on souhaite lui accorder, en fonction du « *cadre légal associé au document concerné, les enjeux et les*

[549] C. santé publ., art. L. 1111-29.
[550] CASSAR Bertrand, *La transformation numérique du monde du droit*, Thèse dactylographiée, Strasbourg, 2020, p. 74. En effet dans la pratique quotidienne, un document ne présentant pas de signature « graphique » semble non signé, alors même qu'une signature électronique est présente. Dans l'esprit de tout un chacun, ce graphisme est encore indispensable, ce qui peut parfois poser difficulté. Certaines personnes veulent impérativement voir une image de signature apposée, en plus de la signature électronique avec les métadonnées. Il n'est pas rare de voir les fournisseurs de signatures électroniques, proposer l'ajout d'une signature simplement graphique en plus des données informatiques et ce, dans le seul but de rassurer de manière visuelle.
[551] ANS, *Référentiel force probante des documents de santé – Document introductif*, PGSSI-S, 2021.

risques induits »[552]. Dans le cadre du référentiel force probante de la PGSSI-S, l'ANS a détaillé trois paliers détaillant les niveaux de sécurité à mettre en place en fonction de la criticité du document, allant de la simple impression pour le palier 1 (avec une sécurité minimale garantissant l'identitovigilance, le secret professionnel et la confidentialité des données devant être appliqués pour tous les documents, peu importe le palier) ; l'impression du/des document(s) avec en plus un cartouche contenant des métadonnées démontrant l'identification de la personne, et l'intégrité du document pour le palier 2. La production et la conservation de traces attestant la matérialisation du document permettront de démontrer également son intégrité ; et pour le dernier et plus haut palier, mêmes conditions que pour le palier 2, avec en plus, la conservation du document natif numérique ayant fait l'objet de la matérialisation, afin de pouvoir comparer au besoin les deux documents[553].

207. **La copie matérialisée.** Il semblerait que cet article puisse également encadrer la valeur probante des documents natifs numériques matérialisés en format papier sans pour autant être le résultat d'une mise en forme particulière. En effet, le Code de la santé publique prévoit que le document matérialisé peut être le résultat de la mise en forme d'un ou plusieurs documents impliquant deux choses : d'une part, la matérialisation peut être le résultat d'un seul et unique document et d'autre part, le document peut faire l'objet d'une mise en forme, dès lors que le sens du document et son contenu ne sont pas modifiés. Aussi, la mise en forme peut ne pas avoir été modifiée.

[552] ANS, *Référentiel force probante des documents de santé – Annexe 4 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la matérialisation des documents de santé numériques*, PGSSI-S, 2021.
[553] *Ibid.*

Conclusion du chapitre. Comme on a pu le voir, la conservation du document et notamment les outils utilisés pour cette conservation électronique, permettront de démontrer l'intégrité du document dans le temps. Les spécificités du domaine de la santé et notamment le caractère sensible des données traitées permettent de contribuer à apporter la preuve de l'intégrité de la donnée au regard des mesures indispensables à mettre en place en termes de sécurité ou encore de traçabilité. Pourtant, il arrive également que la santé soit un frein pour la mise en place d'une dématérialisation totale au sein des établissements de santé, au regard de la nécessité de continuer à produire des documents papiers soit par la matérialisation de copies sur support papier de documents dématérialisés (qu'ils soient natifs électroniques ou copies), soit par la création d'un nouveau document provenant de plusieurs autres documents. La valeur probante de ce dernier sera notamment démontrée grâce à la conservation d'éléments de preuves tels que la traçabilité (information portant sur la création et éventuellement son impression) et/ou de la conservation du document créé au sein du SI de l'établissement afin de pouvoir le comparer au document papier produit, le cas échéant.

En revanche, même si l'établissement met en place le plus haut niveau de garantie pour conserver ses documents dématérialisés afin de leur conférer une présomption de fiabilité, il apparaît que d'autres facteurs entrent en jeu et peuvent risquer de diminuer la valeur probante du document. En effet, la plupart des établissements de santé font appel à un prestataire tiers pour conserver les documents de santé, or c'est bien l'outil choisi qui permettra d'attester l'intégrité du document dans le temps. Aussi, l'établissement doit être particulièrement vigilant dans le choix de son moyen de conservation (qui doit être en conformité avec ses attentes et ses besoins, à la suite d'une étude réalisée) et dans la contractualisation mise en place.

Que le contrat soit réalisé de gré à gré ou *via* une procédure de commande publique, l'objet même du contrat et son périmètre doivent être définis. Le contrat doit notamment contenir une partie technique et une partie administrative :

i. Au sein de la partie technique, on doit pouvoir retrouver toutes les exigences de sécurité minimales devant être mises en place en conformité avec la règlementation en vigueur (la fourniture d'un plan d'assurance sécurité adapté au contexte, un plan de continuité d'activité, les moyens d'authentification, la traçabilité, la réalisation d'audit de sécurité etc.), les modalités de support technique et la maintenance de l'outil, les fonctionnalités attendues par ce dernier et notamment la mise en place d'un plan de réversibilité devant être régulièrement mis à jour.

ii. Au sein de la partie administrative, outre les clauses standards d'un contrat (prix, facturation, durée du contrat et renouvellement, les modalités d'exécution des prestations, modification etc.), doivent être ajoutées les clauses relatives au RGPD (définition du responsable de traitement, lieu d'hébergement des données), les standards et normes à respecter ainsi que les certificats ou agréments à fournir (par exemple si l'outil envisagé est un SAE, il est possible d'exiger la certification NF 461 ainsi que la certification HDS), les modalités relatives à la vérification des prestations réalisées. Pour finir, deux clauses importantes, trop souvent négligées, les pénalités et la rupture du contrat. En effet, la mise en place d'un outil de conservation nécessite de gros investissements en termes financier et de temps. L'établissement doit pouvoir se fier à son outil et être certain qu'il respectera les obligations légales, et répondre à ses attentes tant techniques qu'administratives. En cas de non-respect, l'établissement doit pouvoir inciter son prestataire à respecter ses obligations, notamment grâce aux pénalités envisagées. En dernier recours, l'établissement doit pouvoir se désengager de son contrat grâce à la clause de rupture, notamment en cas de perte d'une certification obligatoire.

Chapitre 2 : L'impact de la dématérialisation sur le Droit

208. **L'évolution des pratiques**. Les nouvelles technologies ont permis d'ouvrir les portes à de nombreuses perspectives entraînant l'évolution et/ou le développement des pratiques dans tous les domaines, tant pour les professionnels que pour les particuliers.

Le commerce est notamment l'un des secteurs fortement impacté grâce au développement du commerce électronique (ou du e-commerce). La FEVAD[554] a publié les chiffres clés du e-commerce en 2020 montrant un chiffre d'affaires atteignant les 112 milliards d'euros correspondant à une hausse de 8,5% en une année. Par rapport à l'an dernier, on compte la création de 17 400 nouveaux sites de vente en ligne[555]. La dématérialisation du commerce est un réel marché concurrentiel obligeant les professionnels à faire évoluer leurs pratiques et à proposer la vente de leurs produits et services en ligne, y compris lorsqu'ils possèdent un site physique.

Ce développement a notamment entraîné le changement des habitudes des consommateurs leur laissant la possibilité de réaliser l'intégralité de leurs achats en ligne (les courses alimentaires, la livraison de repas, l'achat de biens ou de services etc.).

209. **La dématérialisation et le Droit.** Les évolutions permises par les nouvelles technologies ont entraîné inévitablement l'évolution et/ou la création de règles de Droit afin d'encadrer juridiquement ces nouvelles pratiques. Ces changements ont pu être effectués de deux manières différentes :

i. Soit pour encadrer en amont de nouveaux usages possibles grâce aux nouvelles technologies : à titre d'exemple, l'obligation pour tout contribuable (sauf en cas d'impossibilité) de procéder à sa déclaration de revenus par voie électronique[556].

ii. Soit pour pallier une pratique déjà en cours : dans notre cas d'espèce, la Loi adaptant le droit de la preuve aux technologies de l'information[557] est venue acter la reconnaissance de l'écrit électronique comme preuve, ce qui avait déjà été admis par les juges[558].

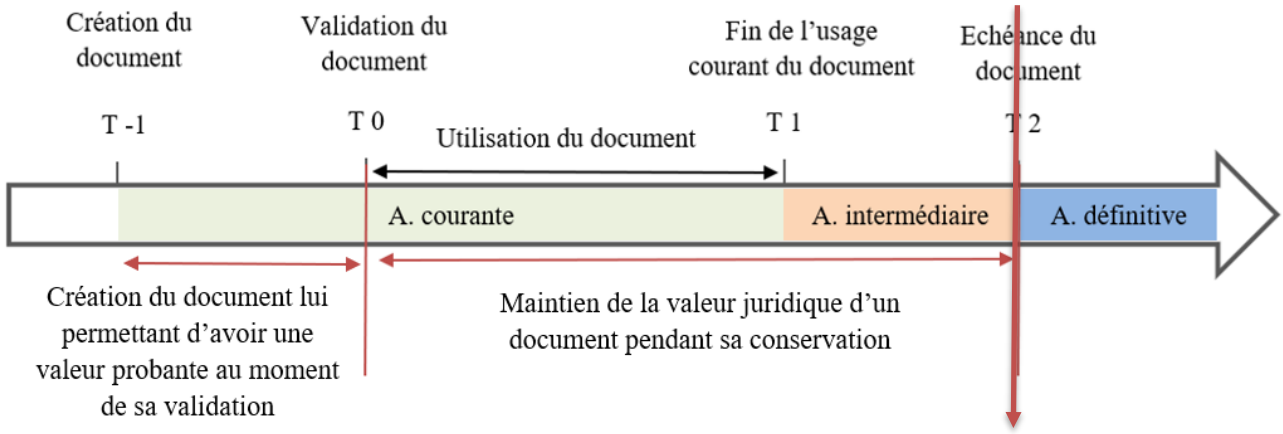
---

[554] Fédération e-commerce et vente à distance.
[555] Fevad, « Communiqué de presse – bilan du e-commerce en 2020 : les ventes sur internet atteignent 112 milliards d'euros grâce à la digitalisation accélérée du commerce de détail », 2021.
[556] C. gén. impôts, art. 1649 quater B.
[557] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62, 14 mars 2000, texte n°1.
[558] Cass, Com, 2 décembre 1997, 95-14.251, Publié au bulletin.

Cette reconnaissance de la valeur probante de l'écrit électronique (original et copie), a conduit les professionnels à vouloir atteindre le « zéro papier » en détruisant les documents originaux papier une fois dématérialisés (section 1). Or, même si le Droit a évolué à l'instar de la technologie, certaines zones d'ombres persistent quant à l'application concrète et le poids du Droit face à la dématérialisation (section 2).

Section 1 : La destruction des documents contenant des données de santé

210. **La destruction.** En principe, la destruction du document intervient dès la fin de sa période de conservation ; il s'agit de la dernière étape du cycle de vie d'un document (sauf en cas de versement en tant qu'archive définitive).



Comme on a pu le voir précédemment, le devoir et le temps de conservation d'un document seront déterminés selon plusieurs facteurs : par une obligation légale ou réglementaire (temps de conservation défini par les textes), pour des besoins juridiques (le document est nécessaire en tant que preuve), pour son utilité (nécessaire pour une finalité déterminée).

Dans les deux premiers cas, une destruction anticipée du document (c'est-à-dire avant la fin de sa durée de conservation) et donc la perte du document, peut entraîner un risque juridique pour la personne morale ou physique et notamment des sanctions. Aussi et par principe, la destruction anticipée d'un document est impossible.

211. **L'objectif du « zéro papier ».** Et pourtant, dans le cadre de la dématérialisation, la reconnaissance de la valeur probante d'un document natif numérique au même titre qu'un document papier et d'une copie électronique au même titre qu'un document original, amène les professionnels à vouloir atteindre le « zéro papier »[559]. Cela signifie notamment, pouvoir détruire les documents originaux papier, avant la fin de la durée de conservation définie (§1), selon les règles de Droit applicables (§2).

[559] Le principe du « zéro papier » est de remplacer au sein d'une entité (entreprise, structure, établissement, cabinet) tous les documents en version papier, en documents électronique. Cela implique également que l'ensemble des traitements effectués sur les documents seront dématérialisés (conservation, échanges etc.).

§1 Une destruction des documents originaux papier anticipée

212. **La double conservation**. L'objectif suprême de la dématérialisation des originaux papier est donc de pouvoir *in fine* les détruire de manière anticipée et ne conserver que les copies dématérialisées afin d'éviter la double conservation de ces mêmes documents. En effet, cette double conservation pour un établissement engendre plusieurs inconvénients tels que :

i. La perte financière : la conservation de documents génère la mise en place d'un système de conservation adapté au type de document, au type de données conservées et à leur format. Aussi, une conservation papier impliquera l'acquisition de locaux pouvant contenir une multitude de documents, accessibles rapidement en cas de besoin, et notamment présentant des mesures de sécurité empêchant les intrusions, ou encore la destruction des archives. Des mesures similaires mais adaptées aux SI devront être mises en place pour les documents conservés de manière informatique.

Dès lors qu'un document papier est dématérialisé, celui-ci sera conservé à la fois en version papier et en version informatique engendrant une redondance des coûts de conservation pour un même document.

ii. La prise de risque : à première vue, la redondance de documents parait permettre d'avoir plus facilement accès à la donnée, puisque plus aisée à retrouver. Or cela signifie également qu'en cas de modification d'un document/dossier conservé à un endroit, les mêmes modifications doivent avoir lieu dans tous les autres endroits de conservation, afin de toujours avoir des documents à jour et complets. Ce qui en pratique n'est pas le cas, impliquant des erreurs potentielles.

213. **La destruction anticipée**. Pour pouvoir éviter la redondance de conservation et se rapprocher davantage de l'objectif « zéro papier », il conviendrait de pouvoir détruire les document originaux papier. Pour cela, il est nécessaire de déterminer si cette destruction est autorisée juridiquement, notamment pour les documents de santé (A) et si oui, d'en mesurer les risques éventuels pour l'établissement de santé (B).

A) Une anticipation expressément autorisée pour les documents de santé

214. **L'objet de la conservation**. Par principe, la destruction, c'est-à-dire la disparition pure et simple de documents est interdite (en cas d'obligation de conservation par le Droit) ou déconseillée (en cas d'utilité ultérieure pour l'établissement). Pour autant, quel est

le véritable objet devant être conservé et ne pouvant être détruit ? Est-ce le contenu informationnel contenu dans le document en lui-même ou le caractère « original » du document c'est-à-dire sa forme initiale ? La réponse à cette question permettra de déterminer si un document original peut être détruit afin de ne conserver que sa copie dématérialisée.

215. **Le contenu informationnel**. Le but même de conserver des documents écrits est de pouvoir se servir de leur contenu informationnel. C'est l'absence de ce contenu qui engendrera des conséquences juridiques directes ou indirectes, pour la personne morale ou physique en charge de conserver le/les documents. Ces conséquences seront directes dès lors qu'une sanction est textuellement prévue pour l'absence de conservation d'un document, ou, indirectes, quand cette absence a pour conséquence des sanctions connexes. A titre d'exemple, la création et la conservation d'un dossier patient est une obligation légale. Pourtant, aucune sanction ne permet de sanctionner l'absence de conservation d'un dossier médical. En revanche, la jurisprudence semble considérer que l'absence de dossier médical dans le cadre d'un recours en matière de responsabilité médicale, constitue « *une perte de chance pour le patient de gagner son procès* »[560] impliquant un renversement de la charge de la preuve. C'est « *à l'établissement de santé de démontrer que les soins prodigues ont été appropriés* »[561] et non plus au patient de prouver la faute.

Le contenu informationnel est donc déjà un élément déterminant devant être conservé. Reste à savoir si le critère « original » du document est lui aussi déterminant.

216. **Le caractère original et la preuve**. Comme vu précédemment, jusqu'en 2016[562], le droit français ne reconnaissait « *qu'une valeur subsidiaire aux copies d'actes sous seing privé* »[563] impliquant la nécessité de conserver au maximum le document original.

Depuis l'Ordonnance de 2016, la valeur probante de la copie s'est vue mise au même niveau que le document original, sous réserve d'être fiable, indépendamment de la subsistance ou non de l'original qui « *ne conditionne plus la valeur probatoire de la copie* »[564]. La copie apparaît désormais comme un mode de preuve à part entière ayant une valeur juridique propre et équivalente au document original.

---

[560] Isabelle BRIENT, « Dossier médical perdu ou incomplet : renversement de la charge de la preuve », *village-justice*, 2018.
[561] Cass. Civ., 1ère, 26 septembre 2018, 17-20.143, publié au bulletin.
[562] Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035, 11 février 2016, texte n°26.
[563] Inconnu, « La copie ou l'original », *Le Monde*, 1980. Disponible à l'adresse : https://www.lemonde.fr/ (consulté le 23/10/2021).
[564] Rapport au Président de la République relatif à l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

Pour autant, même si l'original et la copie se retrouvent sur le même pied d'égalité, cela ne signifie pas la disparition de la notion d' « original » et de son utilité. En effet, la copie bénéficie d'une règlementation qui lui est propre, pour pouvoir justement l'élever au rang de l'original en prouvant sa fiabilité. De plus, le Code civil prévoit également que le juge peut toujours demander la production de l'original, s'il existe encore, non pas pour valider la copie, mais davantage comme élément de comparaison de la fiabilité entre original et copie.

La valeur probante de l'original et de la copie pouvant être équivalente, on peut légitimement penser qu'une copie peut suffire comme preuve dès lors qu'elle est fiable, et que l'original peut ainsi être détruit. La doctrine est en désaccord sur ce sujet : certains prônent la possibilité de détruire l'original, tandis que d'autres pensent que l'article 1379 du Code civil *« ne valide pas la suppression pure et simple du papier puisqu'il précise que sa production « pourra toujours être ordonnée par le juge ». Il ne faut donc pas faire dire à l'article 1379 du code civil ce qu'il ne dit pas. Certes, la valeur probante du document numérisé est la même que celle de l'original. Mais il ne s'agit pas d'un blanc-seing pour la destruction des archives »*[565]. Cette analyse semble partagée : « *on ne peut pas détruire volontairement un original papier ou numérique pendant sa durée légale de conservation »*[566]. Et pourtant, le Code civil ne l'interdit pas non plus. Pourquoi ne pourrait-on donc pas détruire l'original, dès lors que la copie est fiable sachant que sa valeur sera équivalente au document original et que l'obligation de conservation du document est respectée ? La notion d'original ici n'a plus d'intérêt.

La norme NF Z42-026 permettant la numérisation des documents de manière fiable envisage la destruction des documents originaux papiers dès lors que la copie est fiable validant davantage la thèse selon laquelle, la destruction anticipée des documents originaux est possible avant la fin de la durée de conservation[567].

217. **Une destruction possible des documents contenant des données de santé.** Le doute est levé concernant les documents contenant des données de santé. En effet, l'article L. 1111-26 du Code de la santé publique prévoit expressément la possibilité de détruire un

[565] Isabelle RENARD, « Droit de la preuve », *LegalTech*, 2016.
[566] Polyanna BIGLE, « Quand la numérisation de document intègre le droit français », *op. cit.*
[567] En effet, déjà en 2015 avant même la réforme du droit de la preuve, l'arrêt de la Cour d'Appel de Lyon (CA, Lyon, 6e chambre, 3 septembre 2015 – n° 13/09407) avait validé la destruction des documents originaux pour ne conserver que la copie. Cet arrêt « *nous confirme que la destruction d'un fond d'archives papier pour le remplacer par une gestion numérisée est un véritable projet, qui doit être documenté de façon complète aux fins de convaincre le juge de la fiabilité du dispositif et, partant, de la force probante de la copie numérisée* » (Isabelle RENARD, « valeur juridique d'une copie numérisée ? Peut-on ou non détruire l'original papier ? », *Legaltech*, 2016).

document original contenant des données de santé avant sa durée légale de conservation (ou déterminée par le responsable de traitement), dès lors qu'une *« copie numérique fiable a été réalisée »*[568]. La destruction volontaire est ici clairement autorisée par les textes.

B) Un risque juridique pour l'établissement ?

218. **La simplification du système**. Le Code de la santé publique autorise la destruction des documents originaux contenant des données de santé, sous réserve de la réalisation d'une copie numérique fiable, donc équivalente au document original. Bien que cette destruction ne soit qu'une possibilité pour l'établissement de santé, elle fait partie d'une des mesures visant à améliorer et simplifier le système de santé notamment sur le traitement des données de santé à caractère personnel[569].

219. **La copie fiable**. Pour pouvoir détruire le document original, la réalisation d'une copie fiable au sens du Code civil est primordiale. En effet, le risque encouru en cas de copie non fiable, est de voir sa valeur probante diminuée nécessitant la production d'autres preuves pour corroborer le contenu de la copie ou la production du document original, ce qui ne sera pas possible en cas de destruction anticipée. Aussi la réalisation de copies fiables est déterminante pour pouvoir détruire les documents originaux.

Comme on a pu le voir, l'article 1379 laisse une grande latitude quant à l'application du critère de fiabilité, ne déterminant que pour la copie présumée fiable, des conditions à respecter[570]. Dès lors que la copie est présumée fiable, l'établissement pourra détruire le document original en toute sécurité. En revanche, bien que les critères soient énoncés clairement, leur interprétation et leur mise en œuvre sont davantage subjectives, laissant une grande marge d'appréciation. Aussi, autant pour la copie simplement fiable que pour celle présumée fiable, la certitude *a priori* d'une reconnaissance de la valeur probante de la copie n'est par principe, pas nécessairement garantie.

220. **Le niveau de fiabilité**. Bien que la fiabilité des copies ne puisse être garantie à 100%, il est tout de même possible de détruire les documents originaux contenant des données de santé. L'ANS prévoit au sein de son référentiel force probante, que les copies réalisées et conservées selon les conditions énoncées pour les paliers 2 (copie numérique « sécurisée ») et

[568] C. santé publ., L. 1111-26.
[569] Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé (1), JORF n°0022, 27 janvier 2016, texte n°1, art. 204, I, 5°, b.
[570] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61.

3 (copie numérique « fiable ») fournissent un niveau de fiabilité suffisant pour détruire les documents originaux papier[571]. Or, à l'instar des conditions énoncées par le Décret relatif à la copie présumée fiable, et bien que les conditions devant être respectées pour être conforme à ces paliers soient assez détaillées, l'établissement de santé n'a pas la certitude que ce qu'il a mis en place corresponde effectivement au niveau exigé pour l'un de ces paliers.

Il aurait été intéressant, en plus de ce référentiel, de prévoir un système de labélisation, délivrée par l'ANS (ou un autre organisme délégué), attestant la conformité du processus mis en place par l'établissement à un des deux paliers, afin de garantir à l'établissement le bon respect des exigences. A la place d'une labélisation, il aurait été envisageable de s'appuyer sur l'existant : le référentiel prévoit déjà que pour qu'une copie corresponde au palier 3, c'est-à-dire à la copie fiable, sa conservation doit être réalisée au sein d'un SAE certifié conforme à la norme NF Z42-013. Cette certification permet de garantir à l'établissement qu'en cas d'utilisation d'un SAE certifié, la contestation de l'intégrité du document dans le temps est presque impossible à démontrer. Pour autant, la contestation de l'intégrité pourrait intervenir lors de la réalisation de la copie, qui elle, n'a pas l'obligation d'être réalisée conformément à la norme NF Z42-026. L'obligation de respecter cette norme pourrait garantir d'un bout à l'autre de la chaîne, la fiabilité de la copie de manière certaine.

Pour autant, il apparaît que ce n'est pas tant le procédé de reproduction qui compte, mais le système de conservation utilisé, puisque l'ANS précise que la destruction d'un document original ayant fait l'objet d'une copie simple (palier 1 correspondant à une simple numérisation) pourrait « *être envisagée à condition que des mesures d'archivage a minima identiques à celles décrites pour une copie sécurisée aient été mises en œuvre* »[572].

221. **Le(s) risque(s) encouru(s)**. Finalement le risque encouru par l'établissement de santé de voir la valeur probante de sa copie diminuée dépendra des mesures mises en place pour garantir sa fiabilité. Plus les mesures mises en place sont élevées, moins l'est le risque, permettant ainsi la destruction des documents originaux ; sachant également que le niveau de fiabilité ne sera réellement important lors d'un contentieux, que s'il y en a contentieux, et que la fiabilité de la copie est contestée.

Or la fiabilité de la copie, comme nous avons pu le voir précédemment, a également une importance pour la prise en charge du patient. Le professionnel doit pouvoir avoir confiance

[571] ANS, *Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation,* PGSSI-S, 2021.
[572] *Ibid.*

en la copie réalisée et être certain que le dossier patient copie numérique est absolument identique au dossier patient papier, notamment si celui-ci est détruit car il ne sera plus possible d'avoir accès à l'original. La fiabilité de la copie n'est donc pas seulement nécessaire pour se prémunir d'un écrit bénéficiant d'une valeur probante mais également pour avoir un document dans lequel la personne peut avoir confiance, pour une bonne prise en charge du patient.

§2 La réalisation de la destruction

222. **L'encadrement juridique de la destruction**. Dès lors qu'un établissement de santé souhaite détruire des documents de santé, soit par anticipation à la suite de leur dématérialisation ou soit à la fin de leur durée de conservation, celui-ci doit respecter le cadre légal applicable.

En effet, les documents de santé, qui sont des archives, ne peuvent être détruits par une simple « mise à la poubelle »[573] mais doivent respecter les dispositions prévues par le Code du patrimoine, relatives aux archives (A) et par la règlementation sur les données de santé (B).

A) Le régime juridique propre aux archives publiques

223. **La nécessité des archives.** Comme on a pu le voir précédemment, la nécessité de conserver des documents et donc des archives est multiple : pour des besoins juridiques (durée légale de conservation et/ou en tant que preuve) ou encore pour des besoins liés à l'activité professionnelle[574]. Les archives, notamment les archives publiques, ont également un rôle historique et patrimonial. Selon la déclaration universelle sur les archives adoptée en 2011 par l'UNESCO, « *les archives consignent les décisions, les actions et les mémoires* […], *constituent un patrimoine unique et irremplaçable transmis de génération en génération* [et] *jouent un rôle essentiel dans le développement des sociétés* »[575]. Leur conservation, et notamment leur bonne conservation est un enjeu primordial pour chaque pays. A ce titre, un régime juridique propre aux archives dites publiques est mis en place[576].

[573] C'est-à-dire simplement prendre le document papier et le mettre aux déchets ou alors cliquer sur « supprimer » lorsqu'il s'agit d'un document informatique.
[574] C. patr., art. L. 211-1 : « *La conservation des archives est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche* ».
[575] ICA, « Déclaration universelle sur les archives », 2011. Disponible à l'adresse : https://www.ica.org/ (consulté le 12/12/2022).
[576] Françoise BANAT-BERGER et Antoine MEISONNIER, « La gestion des archives dans le secteur médical à

224. **Distinction entre archives publiques et archives privées.** En France, les archives sont divisées en deux types et disposent d'un régime juridique qui leur est propre : les archives publiques[577] définies à l'article L. 211-4 du Code du patrimoine qui regroupent notamment les archives produites par une personne morale de droit public ou une personne morale de droit privé investie d'une mission de service public ; et les archives privées, qui sont toutes les archives n'entrant pas dans la définition de l'archive publique[578]. Des dispositions particulières entourent les archives publiques, qui bénéficient d'un régime juridique plus strict que pour les archives privées, notamment quant à leur destruction. En effet, les archives publiques, ne peuvent en aucun cas faire l'objet d'une destruction, sans le visa préalable de la direction des archives départementales[579] que cette destruction soit anticipée, ou non. Toute destruction d'une archive publique sans visa peut être sanctionnée d'une peine d'emprisonnement de trois ans et de 45 000 euros d'amende[580].

225. **L'obtention du visa pour les archives publiques[581].** Afin d'obtenir le visa des archives départementales, l'organisme producteur de l'archive doit tout d'abord réaliser un tri de ses archives, afin de sélectionner celles vouées à être détruites et celles conservées définitivement (en cas d'utilité administrative, ou d'intérêt historique) par les services d'archives compétents. Une fois ce tri réalisé, l'organisme public soumet une demande d'élimination *via* un bordereau, reprenant succinctement les documents proposés à l'élimination, ainsi que leur volumétrie. La signature du bordereau d'élimination par l'organisme producteur permet d'attester que les documents soumis à élimination n'ont plus d'utilité administrative, et que les délais légaux de conservations sont dépassés. Le bordereau est ensuite transmis aux archives départementales où une vérification des délais de conservation et de l'absence d'intérêt historique est effectuée. Dès lors que l'organisme producteur réceptionne un exemplaire du bordereau d'élimination visé par le directeur des archives départementales, la destruction des archives peut avoir lieu. En effet, ce visa permet de décharger l'administration à l'origine de l'archive, de toute responsabilité de conservation.

---

l'ère numérique », *Médecine & Droit*, 2015, vol. 2015, Issue 131, pp 36-49.

577 C. patr., art. L. 211-4 : « *Les archives publiques sont : 1° Les documents qui procèdent de l'activité de l'Etat, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public. Les actes et documents des assemblées parlementaires sont régis par l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires ; 2° 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 ; 3° Les minutes et répertoires des officiers publics ou ministériels et les registres de conventions notariées de pacte civil de solidarité* ».

578 C. patr., art. L. 211-5.

579 C. patr., art. L. 212-2.

580 C. patr., art. L. 214-3.

581 Charlotte MADAY, « Autorisation d'élimination d'archives et vérification du représentant du contrôle scientifique et technique », *spark archives*, 2017.

Ce bordereau est à conserver par l'organisme producteur permettant de prouver l'autorisation des archives départementales.

226. **Le visa comme atout.** Contrairement aux archives publiques, la destruction des archives privées ne nécessite pas de visa d'élimination laissant penser à une contrainte supplémentaire pour les archives publiques. Or est-ce réellement une contrainte[582] ? Ce visa apparaît de prime à bord comme défavorable, car nécessite la mise en place d'une procédure particulière, obligeant à attendre le feu vert pour pouvoir éliminer les documents ; or ce visa permet également de démontrer que l'organisme a détruit les documents conformément à la règlementation en vigueur puisque, par principe, le visa permet de décharger l'organisme producteur de son obligation de conservation et de rendre compte du contrôle réalisé par les archives départementales. En effet, les directeurs des archives départementales ont en charge le contrôle scientifique et technique portant *« sur les conditions de gestion, de collecte, de sélection et d'élimination ainsi que sur le traitement, le classement, la conservation et la communication des archives »*[583]*. « Ce contrôle est le moyen juridique dont l'État dispose pour garantir, au nom de l'intérêt général, la constitution d'un patrimoine informationnel national de qualité* »[584]. Aussi, pour pouvoir autoriser la destruction d'archives, les archives départementales doivent s'assurer de la pérennité et de la fiabilité des copies. Ce visa permet, de manière détournée, d'approuver le processus de dématérialisation mis en place par l'organisme demandeur. Pour cela, les Archives de France ont créé un Vade-mecum dont l'objectif est de « *donner une liste de critères à examiner avant d'autoriser ou non la destruction de documents sur support papier ayant été numérisés dans le cadre du cadre réglementaire régissant notamment l'écrit numérique* »[585]. A titre d'exemple, les Archives départementales du Nord ont autorisé la destruction anticipée des originaux papiers des dossiers personnels des agents du Centre hospitalier de Tourcoing après leur dématérialisation et leur archivage dans des conditions conformes aux normes NF Z 42-026 et NF Z 42-013[586].

227. **L'exception du visa.** Ce Vade-mecum introduit notamment une exception, permettant aux organismes de détruire des archives publiques sans visa. Il s'agit des

[582] Charlotte MADAY, « Autorisation d'élimination d'archives et vérification d'archives et vérification du représentant du contrôle scientifique et technique », *op. cit.*
[583] C. patr., art. R. 212-3.
[584] Françoise BANAT-BERGER et Antoine MEISONNIER, « La gestion des archives dans le secteur médical à l'ère numérique », *op. cit*.
[585] Archives de France, « *autoriser la destruction de documents sur support papier après leur numérisation – quels critères de décision ? »*, Vade-mecum du Service interministériel des Archives de France, 2014.
[586] GIP SIB e-SIS, « Numérisation fiable et destruction des originaux : le CH de Tourcoing l'a fait !! », *DSIH,* 2019.

« *documents qui, reçus sous forme papier -leurs expéditeurs n'ayant pas été en mesure de les fournir sous forme électronique -, sont numérisés dès leur réception afin d'être intégrés dans des dossiers électroniques ; on considérera alors en effet que ces documents ont été reçus sous forme électronique* »[587]. Cette numérisation dite « au fil de l'eau » permet de considérer que le document produit est un document original, ne nécessitant pas un visa pour la destruction de la version papier.

228. **Une évolution souhaitable de la règlementation ?** Le visa d'élimination permet en grande partie à l'Etat de pouvoir extraire certains documents et de les conserver comme archives définitives dans un but patrimonial et historique. Or dans le cadre d'une dématérialisation de document papier, le document original sera certes détruit, pour autant, son contenu informationnel ne le sera pas. Est-il donc vraiment pertinent de soumettre ces documents au visa d'élimination ? Pour certains documents, cela est nécessaire. Bien que la valeur juridique de la copie puisse être équivalente à l'original, sa valeur historique ne l'est pas forcément. En effet, la copie « *entraîne la perte d'éléments matériels (papier, encre, reliure, couleur, etc.) de l'original. Cette perte peut se révéler inacceptable pour les besoins de la recherche historique, mais aussi d'un point de vue esthétique ou symbolique, lorsque le document d'archives est, davantage encore qu'un support d'informations, un objet d'art ou un lieu de mémoire* »[588]. Ce visa d'élimination va bien au-delà des considérations juridiques ne permettant pas de pouvoir s'en passer dans le cadre de la dématérialisation, bien que les archives soient toujours disponibles. En revanche, à l'instar des documents numérisés au « fil de l'eau », il serait intéressant de déterminer d'autres exceptions permettant de s'abstenir du visa d'élimination.

B) La destruction anticipée du dossier médical papier

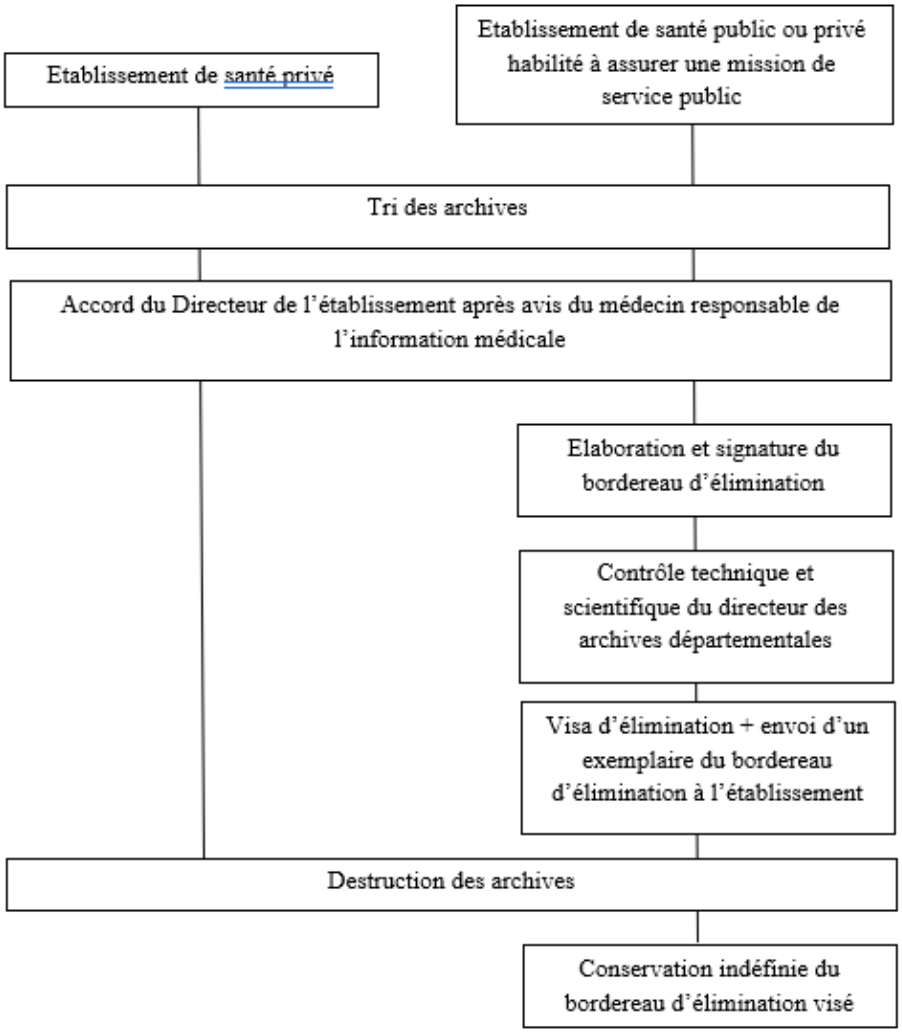
229. **La décision de destruction du dossier médical papier[589]**. Dans le cadre de l'élimination d'archives contenant des données de santé, et notamment le dossier médical du patient, des dispositions supplémentaires sont à prendre en considération par rapport au Code du patrimoine.

---

[587] Archives de France, « modalités de délivrance du visa d'élimination des documents papier transférés sur support numérique ou micrographique », 2005.
[588] *Ibid.*
[589] Aurélie LEROY, Christine RIOU, et Julie SCHOENZETTER-LAUTE, « Procédure d'élimination des dossiers médicaux », *Journal de Gestion et d'Economie Médicales,* 2017/1 (Vol.35), pp. 32-42.

Dès lors qu'un établissement de santé, privé (assurant ou non un service public) ou public, souhaite détruire des dossiers patients, la décision est prise par « *le directeur de l'établissement après avis du médecin responsable de l'information médicale* »[590]. Cette décision engage la responsabilité du directeur. A l'instar de toutes les archives publiques, son élimination *« est en outre subordonnée 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 »*[591]. Cette obligation de visa est notamment rappelée textuellement pour la destruction des documents de santé originaux ayant fait l'objet d'une dématérialisation[592].

Schématiquement, cela peut se représenter de la manière suivante :



[590] C. santé publ., art. R. 1112-7.
[591] C. santé publ., art. R. 1112-7.
[592] C. santé publ., art. L. 1111-26.

230. **La destruction effective**. Dès lors que l'établissement a trié les archives, s'est assuré de la possibilité de les détruire et, le cas échéant, a obtenu le visa d'élimination des archives départementales, celui-ci peut procéder à leur destruction effective.

Les modalités de destruction doivent être plus ou moins strictes selon le type de données présentes sur les documents. En l'espèce, le dossier médical contient des données de santé à caractère personnel soumis au RGPD, dès lors qu'un traitement a lieu sur ces données. La question qui se pose est de savoir si la destruction est un traitement de données. Selon le RGPD, c'est le cas[593]. Aussi, la destruction des archives doit être réalisée selon des mesures de sécurité appropriées au traitement et à la donnée,[594] garantissant notamment la confidentialité de ces données[595]. Cette confidentialité doit être assurée d'un bout à l'autre de la chaîne de destruction, du tri des dossiers patients en passant par son stockage temporaire, jusqu'à leur destruction effective.

Dans le cas où la destruction est réalisée par un prestataire, l'établissement doit conclure un contrat avec ce dernier, reprenant les mesures de sécurité à mettre en place telles que l'utilisation d'un conteneur scellé pour l'acheminement des archives vers le lieu de destruction, garantissant ainsi le respect de la confidentialité des données. De plus, les modalités de destruction proposées par le prestataire, ne doivent pas permettre la reconstitution des documents.

A l'issue de la destruction, le prestataire doit fournir à l'établissement de santé, un procès-verbal attestant la destruction effective des archives.

---

[593] 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, JOUE, L 119, 04 mai 2016, art. 4. Est un traitement de données « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

[594] Aurélie LEROY, Christine RIOU, et Julie SCHOENZETTER-LAUTE, « Procédure d'élimination des dossiers médicaux », *op. cit.*

[595] 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, JOUE, L 119, 04 mai 2016, art. 32.

Section 2 : La Droit face à la dématérialisation

231. **La dématérialisation et le Droit**. La dématérialisation, bien que faisant maintenant partie de notre quotidien, est un concept difficile à définir, tant il est utilisé dans de nombreux domaines et sait s'y adapter. En Droit, la notion de dématérialisation n'est pas non plus définie, bien que de plus en plus, cette terminologie soit utilisée dans les textes. A titre d'exemple, il est prévu que le partage d'informations de santé concernant un patient *« entre des professionnels ne faisant pas partie de la même équipe de soins, […] requiert son consentement préalable, recueilli par tout moyen,* ***y compris de façon dématérialisée*** *»*[596]. Le Droit admet textuellement la possibilité de dématérialiser le consentement du patient, alors même que l'expression « par tout moyen » l'englobait déjà.

Une définition juridique de la dématérialisation n'est pas nécessairement pertinente car il ne s'agit pas d'un concept juridique mais d'un concept technique qui pourra s'appliquer sous plusieurs formes selon le contexte. En revanche, cette dématérialisation aura pour effet d'entraîner des conséquences juridiques, en plus des changements de pratiques.

232. **Les conséquences juridiques de la dématérialisation**. Qui dit dématérialisation dit changement d'état de quelque chose, de base tangible, vers quelque chose d'immatériel, grâce à l'implication de technologies. C'est surtout l'utilisation de ces technologies qui vont entraîner des conséquences juridiques, d'une part, sur les droits que détiennent les personnes (facilitation d'accès aux services publics, meilleure prise en charge du patient etc.) et d'autre part, sur le Droit lui-même. En effet, la dématérialisation a entraîné, entraîne et va encore entraîner, des évolutions de règles de Droit existantes, mais également la création de nouvelles règles notamment pour venir encadrer des pratiques inédites. Par exemple, l'avènement des technologies a conduit à la création d'un Droit du numérique. Dans le cadre de la preuve par écrit, la dématérialisation a de nombreux impacts sur le Droit (§1) nécessitant encore quelques évolutions pour parfaire son encadrement (§2).

§ 1 L'appréciation de la preuve par document électronique

233. **La mutation de la preuve par écrit**. La Loi de 2000[597] a adapté et a fait évoluer le Droit pour prendre en compte les nouvelles pratiques tendant à se développer :

[596] C. santé publ., art. L. 1110-4.
[597] Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62, 14 mars 2000, texte n°1.

l'apport de la preuve sous format électronique. Ce « nouveau » mode de preuve impliquant les technologies met à rude épreuve tant le Droit lui-même (A) que les juridictions (B).

A) Le Droit à l'épreuve de la technologie et la technologie à l'épreuve du Droit

234. **Une adaptation du Droit.** Avant la Loi du 13 mars 2000, la preuve par écrit n'était pas définie par le Code civil, pour autant elle était déjà nécessaire dans certains cas (par exemple, la preuve d'un contrat excédant la somme de 1500 euros[598]). L'absence de définition de la preuve par écrit papier se justifie au regard de sa nature même, qui est considérée comme fiable ; l'utilisation du papier permet de lier le support et l'information sans pouvoir la modifier rendant son contenu par principe intègre contrairement à l'écrit électronique. Pour autant, l'évolution de notre société a conduit le législateur à admettre une valeur juridique à l'écrit électronique, alors même que sa fiabilité n'est par principe pas garantie, au regard de l'implication des technologies. Pour pallier cette insécurité juridique que revêt le caractère électronique de l'écrit, le législateur est venu poser des conditions à respecter pour pouvoir reconnaître une valeur juridique équivalente entre l'écrit papier et l'écrit électronique, conférant ainsi toujours à l'écrit, la qualification de preuve parfaite.

Or on a pu constater tout au long des développements, que les conditions à respecter pour admettre la valeur probante de l'écrit électronique nécessitent toujours l'utilisation d'une ou plusieurs technologie(s) informatique(s). Cela va même plus loin : l'utilisation de telle ou telle technologie permettra de donner une valeur probante plus ou moins forte au document. Prenons l'exemple de la condition d'identification : on l'a vu, l'identification peut être réalisée par de nombreux moyens allant de la trace à la signature. Or l'utilisation de la signature électronique dite qualifiée, permet de présumer de sa fiabilité et donc de l'identification de la personne alors même qu'une signature électronique plus faible ne permet qu'une simple fiabilité. C'est donc la technologie qui va conditionner la force et la valeur probante de l'écrit alors même que c'est cette technologie qui a nécessité de mettre en place des conditions pour admettre la fiabilité de l'écrit électronique.

235. **La technologie comme nerf de la guerre.** On le voit bien, la technologie est autant l'élément qui fait perdre de la valeur à la preuve écrite, que l'élément qui permet de lui en faire gagner. La prise en compte de la technologie est donc obligatoire pour reconnaître la valeur de l'écrit et en est véritablement le nerf de la guerre. Pour autant, même si ces

---

[598] C. civ., art. 1341 version en vigueur du 13 juillet 1980 (Loi n° 80-525 du 12 juillet 1980) au 01 octobre 2016.

conditions font référence à des conditions techniques, force est de constater qu'aucune technologie n'est visée notamment pour la conservation des documents. « *On ne peut qu'adhérer à une telle solution dans la mesure où la loi ne pouvait faire une quelconque référence à une technologie particulière. A défaut, non seulement elle n'aurait pas respecté le principe de neutralité technologique, mais au surplus, eu égard à la célérité des évolutions technologiques, elle aurait risqué d'être rapidement obsolète* »[599]. Aussi, l'application du Droit et la reconnaissance de la valeur juridique de l'écrit dépendra à la fois des technologies utilisées mais également de leur évolution dans le temps rendant le Droit dépendant de la technologie.

236. **L'évolution des technologies.** La technologie étant l'élément central de la valeur probante de l'écrit électronique, le Droit a dû s'adapter pour faire face à ces particularités, comme l'obsolescence technologique. Cette obsolescence *« désigne le fait qu'un produit encore en bon état de fonctionnement apparaisse comme dépassé à cause de l'innovation technologique »*[600] rendant la durée de vie des solutions très courte et nécessitant le transfert des documents vers de nouvelles solutions, ou leur modification pour s'adapter aux nouveaux formats en vigueur. Pour faire face à cela, le Droit précise que « *les opérations requises pour assurer la lisibilité de la copie électronique dans le temps ne constituent pas une altération de son contenu ou de sa forme dès lors qu'elles sont tracées et donnent lieu à la génération d'une nouvelle empreinte électronique à la copie »*[601]. Ces opérations de lisibilité sont par définition une modification de l'écrit (par changement de support par exemple) allant à l'encontre de la définition même de l'intégrité. Cependant, cette exception introduite par le Droit est nécessaire au regard du temps de conservation des documents pouvant être long (un minimum de vingt ans pour les dossier médicaux) par rapport à la durée de vie d'une technologie.

Comme on peut le voir, le Droit a dû s'adapter pour admettre la preuve écrite électronique et est dépendant des technologies utilisées pour son application. Pour autant, l'inverse est également vrai.

237. **Le Droit à l'épreuve de la technologie**. « *Le Droit, est l'ensemble des dispositions interprétatives ou directives qui à un moment et dans un Etat déterminés, règlent le statut des personnes et des biens, ainsi que les rapports que les personnes publiques ou*

[599] Éric CAPRIOLI, « L'archivage des documents électroniques », *Caprioli Associés*, 2013.
[600] Bertrand BATHELOT, « Obsolescence technologique », *Définitions marketing*, 2015.
[601] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61, art. 4.

privées entretiennent »[602]. Ce Droit permet d'apporter une sécurité juridique à toute personne physique ou morale dont les dispositions doivent être respectées sous peine de sanctions. Il permet notamment de garantir les droits que détient une personne.

Aussi, dès lors qu'une technologie est utilisée, sa mise en œuvre doit respecter le Droit applicable. Dans le cadre de la reconnaissance de la valeur probante de l'écrit électronique, le Droit a dû certes prendre en compte les particularités de la technologie ; pour autant, il fixe des conditions à remplir pour garantir la valeur juridique de ce document. A titre d'exemple, si la technologie ne permet pas la traçabilité des actions réalisées sur le document lors de sa conservation, son niveau de fiabilité sera amoindri.

La technologie doit également s'adapter aux évolutions des textes et des recommandations. Dans le cadre de la valeur probante présumée fiable d'une copie, le référentiel force probante de l'ANS impose la conservation des documents dans un SAE certifié. Or pour cela, la technologie devra s'adapter aux dispositions de la norme, au fur et à mesure de ses évolutions.

Pour terminer, le Droit prévoit certaines règles que la technique ne peut pas encore appliquer. Prenons l'exemple de la signature qualifiée en santé. Le Code civil prévoit qu'est présumée fiable la signature qualifiée. Or en santé, actuellement, c'est la CPS qui est le moyen d'identification et d'authentification du professionnel de santé, et celui qui lui permet de signer électroniquement des documents. En revanche la fonction signature n'est pas à ce jour qualifiée, au sens du règlement eIDAS. Pour autant, cela est envisageable ; « *la mise en œuvre de cette signature qualifiée à distance pourrait se faire dans des conditions similaires à celle de la signature électronique avancée par certificat dérivé de l'identité numérique du titulaire de la carte CPx. Le certificat délivré serait qualifié (sur la base de l'authentification à deux facteurs) et la signature obtiendrait le statut qualifié grâce au dispositif de signature à distance qualifié* »[603].

Aussi, bien que la technologie oblige le Droit à évoluer, le Droit met également certains garde-fous afin encadrer l'utilisation des technologies et notamment respecter les droits d'une personne, obligeant la technologie à s'adapter à son tour. Même si la technologie ouvre le champ des possibilités, tout n'est pas pour autant permis.

---

[602] Serge BRAUDO, *définition « Droit »*, Dictionnaire du Droit Privé.

[603] ANS, *Référentiel force probante des documents de santé – Annexe 3 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques*, PGSSI-S, 2021.

B) L'appréciation de la preuve par les juridictions : toujours une réalité ?

238. **L'appréciation de la preuve par le juge.** En Droit français, les juges du fond jugent à la fois le Droit, mais également les faits dont ils ont le monopole. Cette prérogative, contrairement à la Cour de cassation qui ne juge que le Droit[604], leur permet d'apprécier souverainement un élément de fait, c'est-à-dire échappant au contrôle de la Cour de cassation.

Les juges du fond bénéficient par principe, d'un large pouvoir d'appréciation notamment concernant la preuve par écrit. En effet, le Code civil précise qu'« *à défaut de dispositions ou de conventions contraires, le juge règle les conflits de preuve par écrit en déterminant par tout moyen le titre le plus vraisemblable »*[605]. *« L'appréciation du juge consistera à rechercher ce qui lui semble vrai ou bien le titre qu'il considère comme étant le plus crédible »*[606]. En effet, cela est textuellement rappelé par exemple pour la copie, dont l'appréciation de la fiabilité est laissée à l'appréciation du juge[607].

239. **Les limites de l'appréciation**. Pour autant, cette liberté d'appréciation peut être limitée de plusieurs manières : par l'utilisation d'une convention de preuve établie entre les parties, les présomptions légales et l'absence de compétences du juge. En revanche, même si son appréciation est limitée, cela ne signifie pas forcément qu'elle est nulle :

i. La convention de preuve. Le Code civil admet la validité des conventions de preuves[608] permettant aux parties de s'accorder sur la validité des moyens de preuve ou encore la charge de la preuve. Ces conventions viennent établir un accord entre les parties que le juge doit respecter. En revanche, celui-ci n'est pas lié par cette convention de preuve et peut en apprécier la validité, lui permettant de l'écarter, en cas de déséquilibre abusif entre les parties.

ii. Les présomptions légales. Les présomptions légales, c'est-à-dire les présomptions posées par la Loi permettent un renversement de la charge de la preuve (voire pour les présomptions irréfragables, de ne pas pouvoir présenter de preuve contraire, telle que l'autorité de la chose jugée). Pour autant, même si la Loi renverse la charge de la preuve, le juge sera parfois chargé de l'apprécier. A titre d'exemple, le Code civil prévoit une présomption de fiabilité de la copie, dès lors que celle-ci résulte « *d'une reproduction à l'identique de la forme et du*

[604] C. proc. civ., art. 604.
[605] C. civ., art. 1368.
[606] Eric CAPRIOLI, « Le juge et la preuve électronique. Réflexions sur le projet de Loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique », *Caprioli Associés*, 2014.
[607] C. civ., art. 1369.
[608] C. civ., art. 1356.

contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'Etat »[609]. Pour renverser la charge de la preuve et admettre par principe la fiabilité de la copie, un certain nombre de conditions sont à remplir. Le juge aura la charge d'apprécier le respect de ces conditions et de déterminer si effectivement, la copie est présumée fiable.

iii. L'absence de compétences du juge[610]. En revanche, et comme on a pu le voir précédemment, les conditions à respecter tiennent davantage du champ informatique que juridique, sortant, de ce fait, du champ de compétences des juges du fond. La question est de savoir si le juge peut réellement apprécier le respect des conditions dès lors que celles-ci sont purement techniques. Cette question ne se limite pas à la copie électronique, mais s'applique à toutes les preuves impliquant la technologie. Le juge est-il compétent pour apprécier le niveau de fiabilité de la signature électronique utilisée ? A l'instar d'autres domaines tels que le médical, le juge va devoir se faire épauler par des experts sur le sujet et se rapporter à l'état de l'art en la matière comme le respect de certaines normes. Pour autant, le juge ne sera pas nécessairement lié par les conclusions de personnes expertes[611] ou le respect de ces normes, et pourra en apprécier la portée.

On constate tout de même que le juge est, dans la plupart des cas, seul compétent pour apprécier la vraisemblance de l'acte écrit papier, tandis que l'écrit électronique nécessite davantage de connaissances informatiques venant restreindre, dans une certaine mesure la portée de son appréciation.

240. **Une mutation de la preuve par écrit**. Outre l'appréciation des juges du fond qui se trouve remodelée par l'utilisation de technologies, la dématérialisation entraîne peu à peu une mutation de la preuve par écrit, allant de *« l'écrit juridique fiable vers un écrit aux qualités probatoires beaucoup plus incertaines »*[612]. En effet, les juges ont été amenés à valider des pratiques qui étaient autrefois non permises.

Prenons le cas de la signature scannée. Comme on a pu le voir, la signature scannée (c'est-à-dire, la réalisation d'une copie de l'image de signature manuscrite aux fins de l'insérer dans un document) n'est pas une signature électronique. Pendant de nombreuses années, les juges

[609] C. civ., art. 1379.
[610] Frédérique FERRAND, « Preuve », *op. cit. « L'expert, auxiliaire de l'administration de la preuve qui intervient en qualité de technicien reconnu, joue un rôle central dans les contentieux complexes nécessitant, pour leur résolution, des connaissances techniques dont le juge ne peut disposer ».*
[611] *Ibid.*
[612] Etienne PAPIN, « De la disparition de la signature et des mutations de la preuve écrite », *village justice,* 2021.

ont effectivement invalidé l'utilisation de ces signatures scannées[613] sur des écrits électroniques. Néanmoins, on assiste depuis peu à une évolution des pratiques impliquant la validité des signatures scannées par les juges et notamment par la Cour de cassation. A titre d'exemples, la Cour d'Appel d'Aix en Provence a validé l'utilisation de signature scannée dans le cadre d'un contrat de prêt bancaire car celle-ci identifiait son auteur, et était la manifestation de son consentement[614]. Ou encore très récemment, la deuxième chambre civile de la Cour de cassation a rendu un arrêt en date du 12 mai 2021[615], indiquant que la signature scannée « *ne permet pas à elle seule, de retenir que son signataire était dépourvu de la qualité requise pour décerner cet acte* »[616]. Bien que cette signature scannée tende à être acceptée, elle n'est pas pour autant une signature électronique.

Malgré les garde-fous érigés par le Droit pour garantir la fiabilité des modes de preuves utilisant des technologies, on constate que la pratique liée à la dématérialisation incite les juridictions à faire évoluer et assouplir leur position. *« La Haute juridiction est confrontée à cette mutation non-maîtrisée de l'écrit et à l'évidente nécessité de ne pouvoir disqualifier une pratique à l'aune de l'efficacité juridique »*[617].

Le Droit lui-même, comme les juridictions en charge de l'appliquer, évoluent et s'adaptent au gré des nouvelles pratiques engendrées par la technologie.

§ 2 Une évolution des règles de Droit nécessaire ?

241. **Une vingtaine d'années après la reconnaissance de la valeur probante de l'écrit électronique.** Depuis maintenant plus de vingt ans, la preuve par écrit électronique a été admise au même titre qu'une preuve papier par les textes afin de prendre en compte l'évolution des pratiques qui tendaient à se développer vers la dématérialisation des écrits. Au fil du temps, les textes ont été perfectionnés pour encadrer davantage ce « nouveau » mode de preuve, afin qu'il puisse être pleinement utilisé. A titre d'exemple, la loi pour la confiance dans l'économie numérique du 21 juin 2004[618] est venue affirmer la validité des contrats

[613] On peut citer comme exemples un arrêt rendu le 17 mai 2006 par la chambre sociale de la Cour de cassation, rendant irrégulière une lettre de licenciement contenant une signature manuscrite scannée (Cass. Soc., 17 mai 2016, 04-46.706, Inédit) ou encore une décision de la Cour d'Appel de Fort de France en date du 14 décembre 2012, rejetant une demande d'enregistrement d'une marque à l'INPI signée par signature scannée (CA, Fort de France, 14 décembre 2012, n°12/00311).

[614] CA, Aix-en-Provence, 8e chbre b, 27 avril 2017, n° 15/06339.

[615] Cass. Civ., 2ème, 12 mai 2021, 20-10.584 20-10.826, Inédit.

[616] *Ibid.*

[617] Etienne PAPIN, « De la disparition de la signature et des mutations de la preuve écrite », *op. cit.*

[618] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1), JORF n°0143, 22 juin 2004, texte n°2.

produits en format électronique, sous réserve de respecter les dispositions relatives à l'écrit et à la signature électronique[619]. Ils se sont notamment adaptés aux dispositions européennes sur la signature électronique, au regard de la création du règlement eIDAS.

Aujourd'hui, le Droit français pousse à la dématérialisation dans tous les domaines en prévoyant expressément l'obligation de dématérialiser (les procédures de marchés publics[620] ou encore la déclaration de revenus par voie électronique[621]), ou en incitant à la dématérialisation (possibilité de détruire les dossiers médicaux papier une fois dématérialisés[622]).

Or on constate que dans le cadre de la preuve par écrit, la portée de ces dispositions reste encore incertaine (A), si bien que l'on peut se demander si l'écrit électronique est toujours la meilleure des preuves (B).

A) Une règlementation encore incertaine

242. **Une évolution suffisante ?** Bien que la preuve par écrit électronique soit admise et qu'au fil du temps les textes ont été amenés à évoluer, pendant de nombreuses années, ces textes ne paraissaient pas suffisants. Dix ans après la Loi de 2000, la doctrine estimait que **«** *l'insécurité en matière de dématérialisation est la règle, dès lors que les acteurs doivent s'en remettre aux dispositions du Code civil issues de la réforme de 2000, la sécurité l'exception, quand l'absence de cadre général clair et applicable a pu être palliée ici ou là par des règlements particuliers »*[623]. En effet, en l'absence de directives claires permettant de dématérialiser les documents papier en toute sécurité, le droit spécial est venu, dans certains domaines, préciser ce qui devait être mis en œuvre. A titre d'exemple, le Décret de 2005 relatif aux actes établis par les notaires[624] définit les conditions à respecter pour pouvoir effectivement dématérialiser les actes notariés. Aussi, bien que le Droit général ait admis le principe de reconnaissance de l'écrit électronique, les dispositions générales ne permettaient pas de dématérialiser en toute sécurité.

---

[619] Ancien article 1108-1 du Code civil recodifié à l'article 1174 du Code civil en vigueur.
[620] C. com. publ., R. 2132-7 et s.
[621] C. gén. impôts, art. 1649 quater B quinquies.
[622] C. santé publ., art. L. 1111-26.
[623] Emmanuel CAUVIN, « Loi du 13 mars 2000 sur la preuve électronique : le grand bug (législatif) de l'an 2000 », *village justice*, 2010.
[624] Le décret n° 2005-973 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires a été pris le 10 août 2005, JORF n°186, 11 août 2005, texte n°34.

L'Ordonnance du 10 février 2016[625] est venue préciser davantage le régime juridique de l'écrit électronique et notamment la place de la copie électronique. Pour cela, et contrairement à l'écrit original électronique, les directives particulières ajoutées par Décret ont permis d'avoir un support juridique objectif des conditions à respecter pour avoir une copie fiable. Pour autant, ces dernières évolutions ne paraissent pas encore suffisantes.

243. **Une question encore en suspens**. Une question et pas des moindres, dans le cadre d'un projet de dématérialisation, reste encore en suspens car n'est pas expressément envisagée par le Droit général : peut-on détruire les documents papier après leur dématérialisation ?

Comme on a pu le voir précédemment, la doctrine est mitigée à ce sujet. Certains rejettent cette possibilité, tandis que d'autres estiment cela possible dès lors que des précautions sont mises en place (et notamment les Archives de France). En santé, cette question ne se pose plus, avec la possibilité expresse de pouvoir détruire les documents papier dématérialisés. On ne peut que regretter que le Droit général n'ait pas introduit également cette disposition, ce qui aurait permis de lever le voile sur cette question[626].

244. **Des évolutions à envisager.** La preuve électronique bien que nécessaire dans notre société actuelle présente des insécurités par rapport à l'écrit papier, insécurités que le Droit a mises en lumière en prévoyant des conditions à respecter pour qu'elle puisse bénéficier d'une valeur probante. Or ces conditions abstraites laissent une grande latitude quant à leurs applications permettant à la fois de pouvoir prouver par de nombreux moyens la fiabilité de la preuve électronique, mais en même temps, de ne pas pouvoir garantir à la personne morale ou privée, sa réelle valeur probante.

Pour pallier ce manque de précision encore présent, le Droit spécial continue à prévoir des spécificités, complétant les dispositions générales afin de donner des directives concrètes d'application ; c'est notamment le but du référentiel force probante établi par l'ANS en santé.

Autant, certaines spécificités sont forcément nécessaires au regard de la nature des données traitées au sein des documents (exemple : la sécurité renforcée pour les documents contenant des données de santé), autant, certaines dispositions peuvent devenir communes, limitant la

[625] Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations**,** JORF n°0035, 11 février 2016, texte n°26.

[626] Et pourtant, le rapport au président de la République prévoit expressément la possibilité de détruire les originaux papiers. La doctrine reste tout de même mitigée. (Paul AGOSTI et Éric CAPRIOLI, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *op. cit. « Comme le souligne le rapport au président de la République, la destruction des originaux papier est désormais consacrée »).*

multiplicité des applications et permettant une uniformisation du Droit (exemple : la possibilité de détruire les documents dématérialisés) sans pour autant être bloquées par l'évolution technologique.

Afin de garantir une valeur probante réelle au document, ne pourrait-on pas s'inspirer du Luxembourg qui a mis en place des PSDC[627] garantissant ainsi la fiabilité des copies dématérialisées mais également l'intégrité des documents lors de la conservation ? En France, nous pourrions nous appuyer sur nos normes existantes, NF Z42-026 (pour le processus de dématérialisation) et NF Z42-013 (pour la conservation), cette dernière ayant été transposée en norme internationale ISO 14641-1, afin de garantir à toute personne la fiabilité de son écrit électronique dès lors que le processus de dématérialisation mis en place est conforme à ces normes ; d'autant que les juges du fond s'appuient déjà dessus pour emporter leur conviction.

En revanche, l'application de ces normes ne serait pas une obligation, mais simplement un moyen de garantir la présomption de fiabilité de l'écrit électronique.

Le référentiel force probante de l'ANS va déjà en ce sens en obligeant la conservation *via* un SAE certifié conforme à la norme NF Z 42-013 dès lors que l'on souhaite une copie fiable.

B) L'écrit électronique comme la meilleure des preuves

245. **L'écrit comme la reine des preuves**. L'écrit fait partie d'une des preuves dites parfaites liant le juge. Cette preuve écrite revêt une valeur probante de haut niveau, au regard de la place qu'elle possède au sein des textes. En effet, le Code civil prévoit par principe, que la preuve d'un acte juridique[628] dont la valeur excède 1500 euros, doit être réalisée par écrit[629] (sauf exceptions).

En revanche, dès lors que l'on souhaite prouver un fait juridique, tous les modes de preuves sont admis, à l'instar d'autres domaines comme en matière pénale ou commerciale[630]. Pour autant, l'écrit apparaît tout de même pour tout un chacun, comme la preuve suprême. En effet,

---

[627] PSDC : Prestataires de Services de Dématérialisions ou de Conservation.

[628] C. civ., art. 1100-1. « *Les actes juridiques sont des manifestations de la volonté destinées à produire des effets de droit* ».

[629] C. civ., art. 1359.

[630] Frédérique FERRAND, « Preuve », *op. cit. « Les raisons du principe de liberté sont évidentes : les pratiques et transactions commerciales doivent pouvoir être rapides, simples et faciles. Souvent en outre, les contrats passés le sont de façon régulière, renouvelée, voire répétitive. Il convenait donc d'opter pour la souplesse en matière de preuve des actes de commerce, ceci d'autant plus que certains usages écartent la rédaction d'un écrit dans diverses situations. Il n'empêche que, comme le relèvent certains auteurs, le principe de liberté probatoire présente de réels inconvénients, car il menace la sécurité juridique et ne tient en outre pas compte de nombreuses négociations commerciales complexes et touffues qui nécessitent en général des écrits qui pourraient dès lors être exigés afin que soient établis de façon certaine les différents éléments de l'accord* ».

qui n'a pas entendu le proverbe « les paroles s'envolent, les écrits restent » indiquant que les écrits laissent des traces pouvant être utilisées par une personne autant à son avantage que contre elle. De plus, la pratique veut que l'on conserve ses échanges, ses documents, et tout écrit pouvant être utilisé en tant que preuve « au cas où ».

La preuve par écrit est toujours apparue comme un élément sûr, dans lequel on peut avoir toute confiance, auquel on peut se fier, et qui sera plus difficilement contestable. Or est-ce toujours le cas avec la preuve par écrit électronique ? Est-elle toujours aussi fiable ?

246. **La fiabilité de la preuve électronique**. On peut se demander si l'utilisation des technologies ne rend pas moins fiable l'écrit. Dans un sens oui, mais dans un autre non. Certes, seule, la technologie permet la manipulation, notamment la modification plus facile d'un écrit, or, elle permet également de mettre en place des mesures, garantissant, davantage même que l'écrit papier, son intégrité. Aujourd'hui, nous possédons les outils nécessaires pour garantir la fiabilité d'un écrit, grâce aux signatures électroniques qualifiées ou encore les SAE.

La difficulté que représente véritablement l'écrit électronique est l'évolution des technologies. En effet, rien ne nous garantit que les signatures électroniques qualifiées qui présentent un haut niveau de sécurité, ne seront pas obsolètes d'ici quelques années.

Le véritable nerf de la guerre est la prise en compte, autant que possible, des évolutions technologiques, notamment lorsque la durée de conservation des documents est supérieure à la durée de vie de ces technologies[631]. L'établissement de santé doit pouvoir être en capacité de démontrer par tout moyen, que ni l'intégrité ni la fiabilité de ses documents n'ont été compromises dans le temps, malgré ces évolutions.

247. **L'application du Droit et la jurisprudence**. En revanche, ce qui pourrait faire perdre de la crédibilité envers la preuve écrite électronique, est la souplesse de la jurisprudence au regard des pratiques. En effet comme nous avons pu le voir, la jurisprudence tend à valider l'utilisation d'une signature scannée[632], or toute personne est en capacité de l'introduire sur un document dès lors qu'elle en a un exemplaire. A l'heure actuelle, les décisions rendues ne permettent pas de garantir une valeur probante à la signature scannée par rapport à la signature électronique et l'on peut s'en réjouir. En effet, ces décisions étaient

[631] A l'instar du dossier patient qui doit être conservé pour un minimum de vingt ans. Aucune technologie ne peut durer aussi longtemps.
[632] Cass. Civ., 2ème, 28 mai 2020, 19-11.744, Publié au bulletin.

fondées sur d'autres éléments permettant de démontrer le consentement au contrat, par l'exécution de celui-ci, ou encore une double preuve permettant d'identifier la personne.

On s'aperçoit que la jurisprudence tend à simplifier les choses pour prendre en compte la pratique en s'accordant quelques largesses d'interprétation. Bien que pour la pratique, cela soit souhaitable, il ne faudrait pas que ces simplifications viennent, à terme, faire perdre de la valeur à l'écrit.

Conclusion du chapitre. L'évolution des technologies et leur utilisation a engendré le développement de nouvelles pratiques comme la dématérialisation des documents écrits qui fait partie aujourd'hui de notre quotidien, tant dans la sphère personnelle (démarches administratives en ligne, notamment la déclaration d'impôt, la création d'un carte grise, le paiement de redevances etc.) que professionnelle (envoi de mails, conservation des dossiers clients de manière informatique etc.).

Cette dématérialisation a conduit inévitablement le Droit à évoluer et s'adapter pour prendre en compte ces nouvelles pratiques et établir des garde-fous permettant de garantir une valeur juridique équivalente entre l'écrit papier, qui par principe est fiable, et l'écrit électronique, qui lui ne l'est pas au regard de l'utilisation des technologies. Pour autant, il s'agit de ces mêmes technologies qui vont permettre d'attester de la fiabilité du document électronique produit, qu'il soit copie ou natif numérique. Ces technologies, devenues des critères de Droit tant pour garantir la fiabilité de l'écrit, mais également pour déterminer son niveau de valeur probante, ont conduit à limiter en partie l'appréciation des juges.

Cette force probante accordée à l'écrit numérique a conduit les professionnels à vouloir atteindre le « zéro papier », en détruisant les documents papier dématérialisés, afin de ne pas conserver de doublons (version papier, et version informatique). Cette destruction anticipée, bien que présentant de nombreux avantages pour les professionnels, peut présenter quelques risques, notamment en cas de contestation de la fiabilité des copies réalisées. Charge au professionnel en amont, de se constituer un dossier de preuves pouvant emporter la conviction du juge. De plus, cette destruction anticipée, bien qu'expressément autorisée par le Code de la santé publique pour les documents contenant des données de santé, ne l'est pas en Droit général. Cette absence d'autorisation et les conditions abstraites à remplir pour créer une copie fiable rendent mitigée la doctrine quant à la possibilité effective de détruire les documents papier.

On se rend compte que la dématérialisation des écrits a fait évoluer le Droit, mais également l'appréciation qui en est faite par les juges, pour prendre en compte les nouvelles pratiques, mais également les nouveaux risques. En revanche cette évolution bien que souhaitée et attendue est encore aujourd'hui insuffisante laissant une légère marge d'incertitude quant à la véritable valeur juridique de l'écrit, que le Droit spécial tente de pallier, à l'instar du Droit de la santé.

Conclusion du titre. Bien qu'il reste encore quelques incertitudes, la dématérialisation est un enjeu majeur pour notre société, et notamment pour les établissements de santé, afin

d'améliorer notre système de santé. Aussi, afin de pouvoir dématérialiser en toute sécurité, y compris les dossiers patients, l'établissement de santé doit mettre en place un processus complet permettant de détailler la politique de dématérialisation mise en œuvre en son sein.

Pour mettre en place cette politique de dématérialisation, l'établissement doit recenser au préalable ses besoins et ses objectifs (par exemple détruire les dossiers patients papier), faire une analyse des obligations légales et réglementaires applicables, et impliquer dans le processus toutes les personnes concernées (la direction, le responsable de la sécurité des systèmes d'informations, le responsable du service des archives, le service juridique, le DIM, le délégué à la protection des données, ou encore les archives départementales, le cas échant). En effet, la dématérialisation des dossiers patients n'a pas qu'un enjeu juridique, mais également médical (améliorer la prise en charge du patient), technique (garantir la pérennité et l'intégrité du document), organisationnel (permettre l'accès plus aisé à la donnée) ; aussi, il est nécessaire d'impliquer dans la démarche, toutes les personnes ayant un rôle à jouer dans la mise en place du processus. Chaque acteur dans son domaine apportera sa pierre à l'édifice qu'est la politique de dématérialisation de l'établissement afin de garantir que le/les processus mis en place sont conformes aux obligations en vigueur et répondent aux besoins métier.

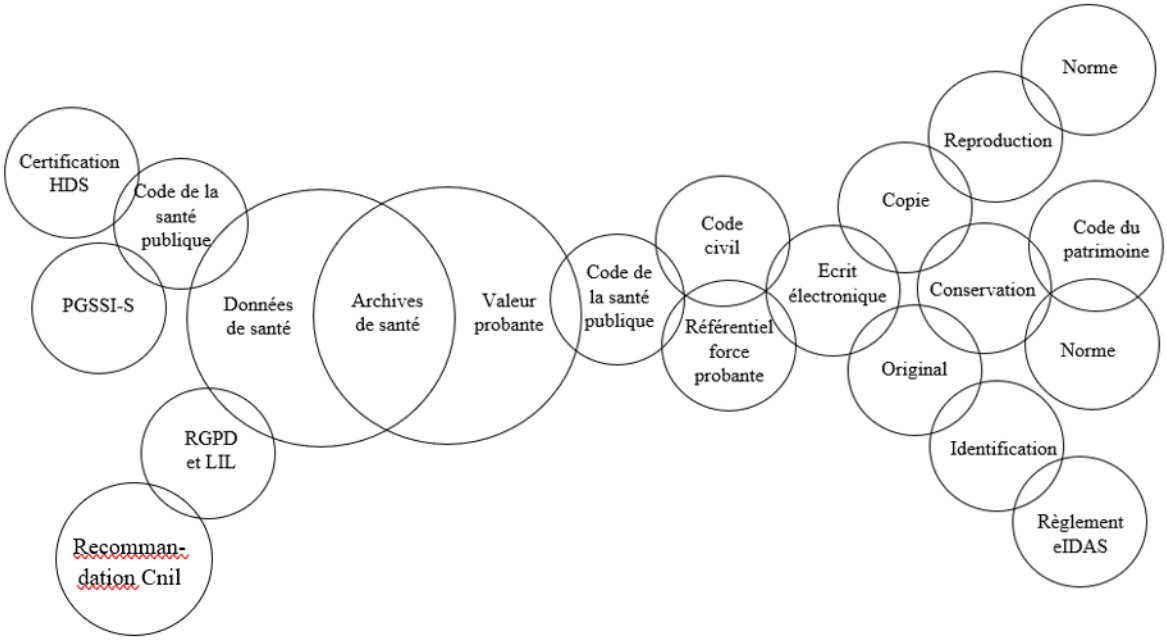
Cette politique de dématérialisation nécessairement écrite, sera un élément de preuve permettant de montrer au juge, en cas de contestation de la fiabilité de l'écrit électronique, que le document produit est fiable. Aussi, cette politique doit être minutieusement détaillée (choix faits par l'établissement, mesures de sécurité et type de conservation mis en place tout au long du cycle de vie du document, modalités de destruction des dossiers papier etc.), doit être respectée par l'établissement, et doit faire l'objet d'actualisations récurrentes, afin de prendre en compte les évolutions technologiques, légales ou organisationnelles au sein de celui-ci.

La politique de dématérialisation permet de garantir la bonne gestion des données pendant tout son cycle de vie, et ainsi garantir leur fiabilité tant pour les besoins métier (garantir au professionnel que l'information est juste) que juridiques (garantir la valeur probante de l'écrit) qui sont finalement intimement liés. En effet, les mesures juridiques devant être mise en place pour garantir la valeur probante de l'écrit, permettront à l'établissement de garantir la fiabilité des données nécessaires à la prise en charge du patient, aux professionnels de santé.

Conclusion de la partie. La question qui nous intéressait dans le cadre de cette partie était de déterminer la valeur probante des documents dématérialisés contenant des données de santé. Comme nous avons pu le voir tout au long des développements, contrairement à l'écrit papier qui bénéficie par nature d'une valeur probante, l'écrit électronique doit respecter certaines

conditions pour bénéficier d'une valeur équivalente à celle de l'écrit papier. Nous nous sommes également rendu compte que la dématérialisation n'entraînait pas que des obligations juridiques liées à la valeur probante du document, mais aussi des obligations liées à la nature même de la donnée telles que la mise en place d'une sécurité appropriée. Le respect de ces obligations inhérentes au domaine de la santé permet également de contribuer à la fiabilité des documents dématérialisés.

Aussi, dans le cadre de la dématérialisation de documents contenant des données de santé, une multitude de règles sont à respecter :



L'enjeu de la valeur probante du document ne se situe pas tant sur son admissibilité car par principe, un document électronique est admissible en tant que preuve au même titre qu'un document papier, mais davantage sur son poids. En effet, nous avons pu constater que les modalités techniques mises en place pour dématérialiser le document (choix de la signature, du type de conservation, des modalités de reproduction), détermineront qui a la charge de la preuve, le niveau d'appréciation qu'a le juge, et la possibilité ou non de détruire l'original. C'est donc le poids que l'établissement souhaite accorder au document qui déterminera son poids en tant que preuve.

En tout état de cause, la valeur probante du document n'aura réellement d'importance que si la fiabilité de l'écrit électronique est remise en doute par la partie adverse. Pour autant, même si la fiabilité du document n'est pas remise en cause, un document non fiable peut tout de même entraîner des contentieux dès lors que ce document est à la base d'un diagnostic médical établi par le médecin, ayant entraîné un préjudice pour le patient.

La dématérialisation des documents contenant des données de santé au sein d'un établissement est un projet à part entière nécessitant une réflexion approfondie et aboutie, tant pour des questions juridiques que pour des questions métier.

DEUXIEME PARTIE : LES CONSEQUENCES DE LA DEMATERIALISATION EN SANTE

248. **La dématérialisation des documents : une évolution majeure**. La dématérialisation des documents au sein de n'importe quel établissement, entreprise ou encore structure, permet de réduire considérablement la production et/ou la conservation de documents en version papier au profit de documents en format numérique. Elle a certes permis de réduire le volume de documents papier produit, mais n'a pas que cet avantage.

En effet, elle permet notamment de fluidifier l'échange d'informations. Prenons l'exemple des correspondances de leur forme archaïque à une forme plus moderne : avant l'invention du numérique, les échanges d'informations au sein d'une même entreprise devaient être réalisés en main propre, par téléphone ou encore par courriers postaux, dès lors que cette entreprise avait plusieurs établissements. Avec l'invention de l'Internet et notamment des mails, ces échanges qui prenaient du temps ou alors dont qui n'avaient pas de support écrit ont fini par laisser place à des échanges instantanés par mail avec des informations à jour en temps réel.

Outre le gain financier ou encore la facilité de correspondance, la dématérialisation des documents a permis notamment de réduire le traitement des dossiers ou encore des procédures. En effet, la commande publique impose aux pouvoirs adjudicateurs[633] tels que les personnes morales de droit public et aux entités adjudicatrices[634] d'utiliser au mieux les deniers publics pour ces besoins en mettant sur un pied d'égalité toutes les entreprises susceptibles de répondre à leur besoin et en toute transparence[635]. Pour cela, ils ont l'obligation de mettre ces dernières en concurrence selon les modalités définies au sein du Code de la commande publique. Auparavant, les candidatures et les offres étaient déposées en version papier obligeant les pouvoirs adjudicateurs et les entités adjudicatrices de laisser un temps suffisant aux entreprises pour formuler leur offre. Avec la dématérialisation des procédures de la commande publique, ce temps a été considérablement réduit permettant d'attribuer plus rapidement le marché public. Prenons simplement l'exemple de la réception des candidatures et des offres d'un appel d'offre ouvert : « *le délai minimal de réception des candidatures et des offres est de trente-cinq jours à compter de la date de l'envoi de l'avis de marché* »[636]. Ce délai « *peut être ramené […] à trente jours si les candidatures et les offres sont ou peuvent être transmises par voie électronique* »[637]. Rien qu'à cette phase de la procédure, la dématérialisation a permis de faire gagner cinq jours sur la procédure ce qui représente un gain de temps considérable pour les acheteurs.

[633] C. com. publ., art. L. 1211-1.
[634] C. com. publ., art. L. 1212-1.
[635] C. com. publ., art. L. 3.
[636] C. com. publ., art. R. 2161-2.
[637] C. com. publ., art. R. 2161-3 2°.

Aussi, la dématérialisation matérielle et physique du document n'a pas eu que l'avantage de réduire la production de papier mais a eu de nombreux impacts et conséquences sur le fonctionnement même des différentes entités.

249. **La dématérialisation des processus.** Il apparaît donc évident, à la lumière de ces quelques exemples, que la dématérialisation des documents, qu'ils soient natifs numériques ou copies numériques, permet et incite à faire évoluer les pratiques pour optimiser au mieux les bénéfices de la dématérialisation des documents et permet de tendre vers l'objectif de dématérialiser à 100% une structure.

En effet, la dématérialisation d'un document n'est qu'un moyen technique qui permet de mettre sous format numérique des supports. Or, pour tendre vers l'objectif du 100% dématérialisé, il est nécessaire d'avoir une vision plus large et de s'attaquer à la « *dématérialisation des processus* »[638]. La dématérialisation d'une structure passe donc par le changement des pratiques permettant notamment d'éviter de devoir dématérialiser des documents produits préalablement sur papier, parce que produire un document directement en format numérique est impossible ou est incompatible avec l'utilisation qui en est faite.

Au sein d'un établissement de santé, la dématérialisation est en plein essor, permettant notamment de faire évoluer la prise en charge globale du patient. Il a été évoqué précédemment qu'une des difficultés rencontrées au sein d'un établissement de santé, était un accès restreint et différé pour les professionnels de santé au dossier du patient, lorsque celui-ci est en format papier[639]. En effet, pour pouvoir le consulter pour la prise en charge du patient, il est nécessaire que le service des archives procède au rapatriement de ce dossier dans le service concerné. Or, bien qu'il soit aujourd'hui techniquement possible d'avoir un dossier patient informatisé, des établissements de santé, notamment de grands hôpitaux n'en possèdent pas encore, ou ne dématérialisent que partiellement leurs dossiers. La dématérialisation du support n'est donc qu'un moyen de parvenir à la dématérialisation totale des établissements de santé.

250. **L'impact de la dématérialisation dans les établissements de santé.** Bien qu'il soit évident que la dématérialisation du support ne suffit pas à elle seule à atteindre le « zéro papier » au sein d'un établissement de santé, elle permet de faire évoluer la prise en charge du patient (titre 1) ainsi que les droits du patient (titre 2).

---

[638] LOCARCHIVES, « Numérisation fidèle & destruction des originaux », *livre blanc,* 2017, p.12.

[639] Mathias BEJEAN, Frédéric KLETZ et Jean-Claude MOISDON, « Création de valeur organisationnelle et technologies de l'information à l'hôpital : le cas du dossier patient informatisé », *Gestion et Management Public,* 2018/2, vol. 6/n°4, pp. 9-24

TITRE 1 : Une prise en charge du patient en pleine évolution

251. **La prise en charge.** La prise en charge peut être entendue de plusieurs manières différentes selon le contexte dans lequel le terme est utilisé et la portée que l'on souhaite lui accorder.

A titre d'exemple, la prise en charge peut être la part du remboursement effectuée par l'assurance maladie et/ou la mutuelle d'un patient pour la réalisation d'un acte médical ou la prise de médicaments ; ou encore le fait pour un professionnel de santé, de suivre un patient médicalement, que ce soit pour un suivi régulier comme le ferait un médecin traitant ou de façon plus ponctuelle pour une sage-femme dans le cadre d'une grossesse ; mais aussi dans le cas de la prise en charge médicamenteuse correspondant « *à un processus complexe comprenant de nombreuses étapes : prescription, dispensation, administration, impliquant de nombreux acteurs* »[640].

En l'espèce, on entend par prise en charge du patient, la période complète pendant laquelle le patient est suivi au sein d'un établissement de santé, de son admission à sa sortie, voire jusqu'à la fin des soins nécessaires pour la pathologie pour laquelle il est venu consulter, comprenant ainsi les rendez-vous de contrôle et les liens nécessaires avec les professionnels de santé libéraux pour les soins à domicile. Sont donc inclus dans la prise en charge du patient tous les actes de soins pratiqués, le parcours de soin élaboré, ou encore le suivi global du patient.

252. **L'évolution de la prise en charge du patient grâce à la dématérialisation**. La dématérialisation des supports écrits a permis de faire évoluer considérablement la prise en charge du patient au sein d'un établissement de santé ; d'une part, en permettant de mettre en place des modalités techniques novatrices de prise en charge grâce à l'utilisation des technologies de l'information et de la communication (chapitre 1) et d'autre part, en créant des outils nécessaires au suivi du patient dans le cadre de sa prise en charge, outils qui peuvent être encore améliorés (chapitre 2).

640 HAS, *prise en charge médicamenteuse*, 2013.

Chapitre 1 : Des modalités techniques de la prise en charge médicale du patient

253. **La e-santé.** La e-santé est le *« produit de la digitalisation active de notre société, […] rencontre des secteurs de la santé et du numérique. Porté*[e] *par l'usage des nouvelles technologies de l'information et de la communication,* [elle] *se destine à la fonction d'une « santé augmentée » »*[641]. La e-santé permet en d'autres termes d'utiliser les TIC pour l'ensemble des activités en rapport avec la santé dans le but de faire *« progresser notre système de santé »*[642] et ce, dès les années 70, même si elle n'a connu un véritable succès qu'à partir des années 2000.

Initialement, la e-santé pouvait-être décomposée en plusieurs sous catégories :

i. la robotique, alliant l'humain et le robot pour la santé du patient telle que la création de dispositifs permettant de détecter si une personne en perte d'autonomie a fait une chute.

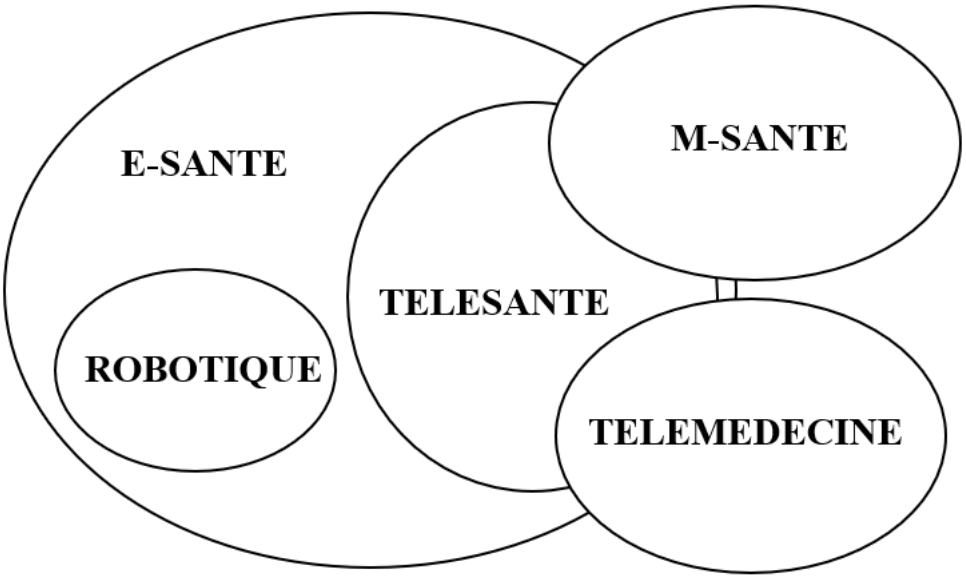
ii. la télésanté, définie par l'Organisation Mondiale de la Santé comme « *les activités, services et systèmes liés à la santé, pratiqués à distance au moyen des technologies de l'information et de la communication, pour les besoins planétaires de promotion de la santé, des soins et du contrôle des épidémies, de la gestion et de la recherche appliquées à la santé* »[643]. Il pouvait s'agir par exemple, d'un service de messagerie sécurisée ou encore du Répertoire Opérationnel des Ressources (ROR) qui est « *un référentiel recensant l'ensemble de l'offre sanitaire et médico-social, et comprenant un volet sur la disponibilité des lits en établissement de santé »*[644]. La télésanté pouvait être décomposée en deux sous-catégories : iia. La m-santé (santé mobile ou encore mobile health) qui « *recouvre un univers large et divers de produits matériels (objets connectés) ou d'applications logiciels en rapport avec la santé ou le « bien-être » »*[645]. Il s'agit notamment des outils permettant à toute personne de surveiller sa santé en toute autonomie grâce, par exemple, à sa montre connectée indiquant le nombre de pas réalisée dans la journée ou encore un lecteur de glycémie.

---

641 ANS, *La petite histoire de la e-santé,* 2021. Disponible à l'adresse : http://esante.gouv.fr/. (Consulté le 12/01/2022).
642 *Ibid.*
643 Guy ROSSIGNOL, « Soigner au-delà des frontières. La télématique au service de la santé mondiale », *ADSP* déc. 1998, n° 25, p. 53.
644 Ministère de la santé et de la prévention, « Le répertoire national de l'offre de santé et d'accompagnement médicosocial – ROR – un socle d'informations utiles sur l'offre de santé », 2022. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 26/07/2022).
645 HAS, *e-santé,* 2016.

iib. La télémédecine qui est « *une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport un professionnel médical avec un ou plusieurs professionnels de santé, entre eux ou avec le patient et, le cas échéant, d'autres professionnels apportant leurs soins au patient »*[646].

On pouvait schématiser cette répartition de la manière suivante[647] :



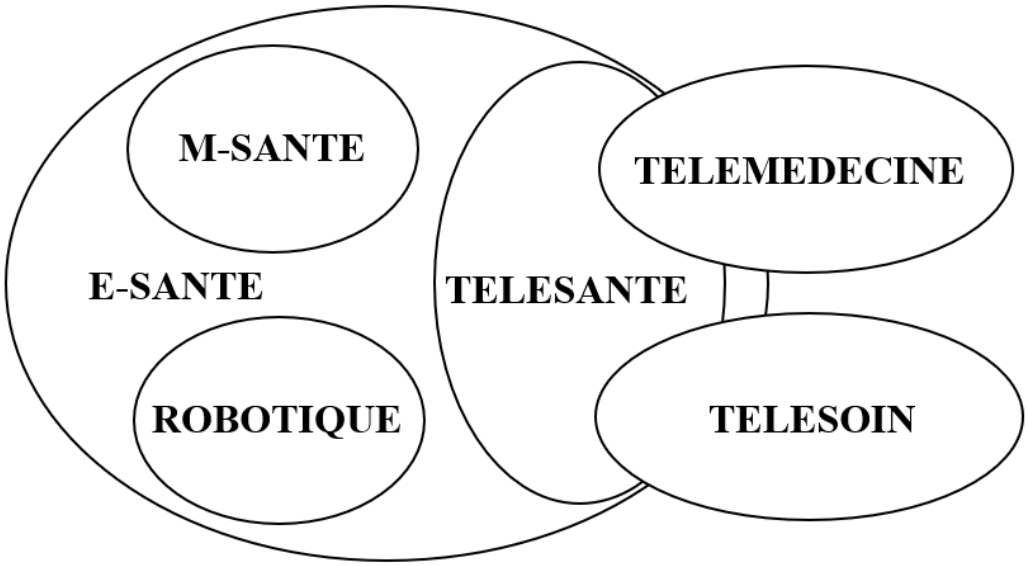
254. **Un changement sémantique**. Cependant, notamment avec la Loi du 24 juillet 2019[648] relative à l'organisation et à la transformation du système de santé, dite Loi Ma Santé 2022, on assiste à un changement sémantique modifiant l'organisation initiale et clarifiant les termes.

En effet, il apparaît que la télésanté soit *« considérée dans la loi Ma santé 2022 comme une pratique professionnelle »*[649] et non plus comme un ensemble de services ou d'activités liés à la santé. Elle est le regroupement de deux activités[650], la télémédecine et le télésoin. Le télésoin qui 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*

[646] C. santé publ., art. L 6316-1.
[647] CNOM, « Santé connectée – De la e-santé à la santé connectée », *Livre Blanc du Conseil national de l'Ordre des médecins,* 2015.
[648] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1), JORF n°0172, 26 juillet 2019, texte n°3.
[649] Pierre SIMON, « Ne confondons pas les services de l'e-santé avec les pratiques professionnelles de télésanté », *telemedaction,* 2019.
[650] Ministère de la santé et de la prévention, « La télésanté – pour l'accès de tous à des soins à distance », 2020. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 26/07/2022).

pharmaciens ou auxiliaires médicaux dans l'exercice de leurs compétences »[651] a été créé par la loi du 24 juillet 2019[652]. Aussi, ce qui n'entre pas dans l'une de ces deux activités, n'est plus considéré comme de la télésanté mais de la e-santé au sens large. Cela semble confirmé par le titre du chapitre du Code de la santé publique au sein duquel sont regroupés la télémédecine et le télésoin : la télésanté.

L'organisation peut aujourd'hui être représentée de la manière suivante :



255. **La e-santé et la dématérialisation**. La e-santé est donc étroitement liée à la dématérialisation des données puisqu'elle n'est possible qu'avec elle. On peut même aller plus loin en ce qui concerne la télémédecine, en osant considérer qu'une pratique médicale réalisée à distance peut s'apparenter à une dématérialisation de l'acte de soin en tant que tel (section 1). On s'aperçoit en particulier, à la suite de la crise sanitaire due à l'épidémie du COVID 19, que la e-santé est au cœur de la prise en charge actuelle (section 2), mais est-elle suffisamment encadrée juridiquement ?

[651] C. santé publ., art. L. 6316-2.
[652] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1), JORF n°0172, 26 juillet 2019, texte n°3.

Section 1 : La dématérialisation de l'acte de soin ?

256. **L'inclusion de la télémédecine dans le Code de la santé publique**. La notion d'e-santé n'a pas été définie au sein du Code de la santé publique contrairement à la notion de télémédecine qui a été introduite et définie au sein du Code de la santé publique à l'article L. 6316-1 par la Loi n°2009-879 du 21 juillet 2009[653]. En effet, la télémédecine étant un acte médical réalisé au moyen des TIC, un encadrement juridique particulier et renforcé semblait nécessaire, d'autant plus que cette notion ne recouvre qu'un champ restreint de la e-santé qu'il était possible d'encadrer. A ce titre, le Décret n°2010-1229 du 19 octobre 2010 relatif à la télémédecine est venu définir les différents actes de télémédecine « *ainsi que leurs conditions de mises en œuvre* »[654].

Jusqu'à très récemment, la télémédecine n'était pas considérée comme une pratique « normale » et courante de la médecine[655]. Il a fallu mettre en place des garde-fous techniques et juridiques pour éprouver cette nouvelle forme de prise en charge. Il était nécessaire de s'assurer que cette pratique puisse permettre une prise en charge aussi bonne du patient qu'une prise en charge dite « traditionnelle » et ainsi éviter certaines dérives ou une moins bonne prise en charge (§1). Aujourd'hui, les règles concernant la télémédecine ont été assouplies pour faire de la télémédecine, un mode « normal » de prise en charge du patient qui est même parfois à privilégier (§2).

§1 L'utilisation de la télémédecine : une pratique médicale « nouvelle »

257. **La télémédecine : un moyen de pratiquer la médecine.** Depuis le début du XXIème siècle, la télémédecine a fait son entrée dans notre système de santé par son introduction dans le Droit commun *via* des expérimentations au sein du territoire. En même temps, le principe même de la télémédecine a été déterminé afin d'en définir les modalités d'application (A) pour permettre une réelle innovation dans la prise en charge des patients ainsi que pour répondre aux problématiques rencontrées par notre système de santé comme la

[653] C. santé publ., art. L. 6316-1 : La télémédecine est *« une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. Elle permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients ».*

[654] C. santé publ., art. L. 6316-1.

[655] Stéphanie LANGARD, Approche juridique de la télémédecine. Entre Droit commun et règles spécifiques, *op. cit.*

désertification médicale (B). *« « Faire voyager ses données plutôt que le patient » est devenu le nouveau slogan de la politique de santé »*[656].

A) Le principe de la télémédecine

258. **La télémédecine dans les grandes lignes**. La télémédecine est définie comme une pratique médicale à distance réalisée par le biais des technologies de l'information et de la communication impliquant plusieurs protagonistes. Il y a d'un côté un professionnel obligatoirement médical, qui est le professionnel requis pour la réalisation de l'acte de télémédecine, et de l'autre côté, un ou plusieurs professionnels (que l'on peut qualifier de professionnels requérants), de santé ou non, se trouvant avec le patient, voire simplement le patient[657]. La télémédecine implique que le professionnel requis ne se trouve pas avec le patient, mais qu'il pourra le prendre en charge par le biais des TIC, grâce à un appui du professionnel requérant, le cas échéant.

259. **Le champ d'application de la télémédecine.** Le champ d'application de la télémédecine est très clairement identifié au sein du Code de la santé publique, *« elle permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients »*[658]. En dehors de cette liste énumérative, l'acte ne pourra pas être réalisé par télémédecine, dans les conditions définies au sein du Code de la santé publique.

260. **Les cinq actes de télémédecine**. Pour aller plus loin et pour spécifier les modalités de réalisation de l'acte de télémédecine en fonction du champ d'application concerné, cinq actes de télémédecine ont été identifiés :

i. La téléconsultation, *« qui a pour objet de permettre à un professionnel médical de donner une consultation à distance à un patient. Un professionnel de santé peut être présent auprès du patient et, le cas échéant, assister le professionnel médical au cours de la téléconsultation »*[659]. Dans le cadre de la téléconsultation, un professionnel requis réalise une consultation à distance d'un patient. Ce patient peut être seul ou accompagné d'un

[656] Morgan GRIT, « La naissance de deux actes de télémédecine en EHPAD », *RDS*, 2017, n°78, pp. 551-552.
[657] C. santé publ., art. L. 6316-1.
[658] *Ibid.*
[659] C. santé publ., art. R. 6316-1.

professionnel requérant. Ce type d'acte est obligatoirement synchrone, signifiant que le professionnel requis s'entretient en direct avec le patient, via les TIC. Certains actes médicaux peuvent être réalisés, malgré la distance séparant le professionnel requis et le patient. En effet grâce aux TIC, le professionnel requis peut demander au professionnel requérant de réaliser certains actes médicaux afin qu'il puisse exploiter les résultats comme la prise de tension, la réalisation d'un fond d'œil, une visualisation plus poussée d'un grain de beauté grâce à un microscope connecté etc.

ii. La téléexpertise, *« 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 »*[660]. Dans ce cas, un professionnel requérant, sollicite un professionnel requis, au regard de ses compétences particulières. Cette demande d'expertise peut être réalisée en mode synchrone ou asynchrone, puisque la demande d'expertise n'a pas besoin d'être immédiate. Par exemple, il s'agit de la téléexpertise pour l'interprétation d'examens radiologiques, que l'on appelle aussi téléradiologie. En effet, la pénurie de radiologues que l'on constate depuis de nombreuses années en France (environ 12,9 radiologues / 100 000 habitants[661]) peut être palliée par le recours à la téléradiologie, permettant aux radiologues d'un cabinet d'analyser à distance les radios réalisées au sein d'un établissement de santé par exemple, lorsque ce dernier ne possède pas en son sein, assez de radiologues pour assurer notamment la permanence des soins.

iii. La télésurveillance médicale, *« qui a pour objet de permettre à un professionnel médical d'interpréter à distance les données nécessaires au suivi médical d'un patient et, le cas échéant, de prendre des décisions relatives à la prise en charge de ce patient »*[662]. Ce procédé est notamment utilisé dans le cadre d'une grossesse à risque afin de suivre en direct l'évolution de la situation.

iv. La téléassistance médicale, *« 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 »*[663]. Dans le cadre de la téléassistance médicale, un professionnel médical guide un autre

[660] *Ibid.*
[661] Louis BOYER (Pr), *Démographie médicale radiologique en France*, JFR de printemps – Nimes, 2019.
[662] C. santé publ., art. R. 6316-1.
[663] *Ibid.*

professionnel de santé pour la réalisation d'un acte de soin[664]. Cette téléassistance permet le partage de connaissances entre professionnels.

v. La réponse médicale *« qui est apportée dans le cadre de la régulation médicale »*[665].

B) L'innovation dans la prise en charge et les opportunités en découlant

261. **Les problématiques de santé actuelles**. Notre système de santé français fait face depuis quelques années, à de nombreuses problématiques[666] de taille telles que :

i. le vieillissement de la population : d'après une étude réalisée par l'INSEE, « *au 1er janvier 2020, la population française continue de vieillir. Les personnes âgées d'au moins 65 ans représentent 20,5% de la population, contre 20,1% un an auparavant et 19,7 % deux ans auparavant. Leur part a progressé de 4,7 points en vingt ans* ».[667] Ce phénomène résulte notamment de l'amélioration de la qualité de vie de la population et des avancées médicales. Si ce rythme est conservé, on estime qu'en 2040, « *plus d'un habitant sur quatre aurait 65 ans ou plus. […] En 2070, leur part pourrait atteindre 28,7% »*[668]. Or, les personnes de plus de 65 ans sont plus susceptibles d'avoir recours aux soins, et notre système de santé devra être capable de répondre aux besoins. Aussi, il est impératif que ce dernier évolue, d'autant plus qu'il doit faire face à d'autres problématiques venant compliquer considérablement la prise en charge de la population. ii. Il y a notamment l'augmentation des maladies chroniques.[669] D'après le rapport annuel de propositions de l'Assurance Maladie de 2019, « *près de 20 millions de personnes [sont concernées], un effectif en constante croissance* »[670]. Ces maladies chroniques nécessitent de nombreux soins sur de longues durées. Or sur le territoire, la population fait face à (iii.) une inégalité d'accès aux soins, notamment due à une désertification médicale[671]. En effet, 30,2%, soit « *près d'un tiers des Français résident […]*

[664] Stéphanie LANGARD, Approche juridique de la télémédecine. Entre Droit commun et règles spécifiques, *op. cit.*
[665] C. santé publ., art. R. 6316-1.
[666] ANS, *La petite histoire de la e-santé, op. cit.*
[667] INSEE, *Tableaux de l'économie française,* 2020. Disponible à l'adresse : https://www.insee.fr/ (consulté le 08/07/2022).
[668] *Ibid.*
[669] Ministère de la santé et de la prévention, *Vivre avec une maladie chronique,* 2012. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 25/07/2022). « *Une maladie chronique est une maladie de longue durée, évolutive, avec un retentissement sur la vie quotidienne. Elle peut générer des incapacités, voire des complications graves* ».
[670] Assurance Maladie, « *Améliorer la qualité du système de santé et maîtriser les dépenses* », Rapport au ministère chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et des produits de l'Assurance Maladie au titre de 2020 (loi du 13 août 2004), 2019.
[671] Vie publique, « Les déserts médicaux : définition et mesures des pouvoirs publics », *Fiche thématique,* 2021. « *Par « désert médical », on entend l'impossibilité ou la très grande difficulté pour les patients à accéder*

dans un « désert médical »[672], impliquant que près de 51% des 1,6 million de Français qui renoncent chaque année à des soins médicaux, le font « *pour des raisons liées à l'insuffisance de la démographie médicale* »[673].

262. **La télémédecine comme un moyen de réponse.** « *La télémédecine est aujourd'hui considérée comme une réponse moderne aux problématiques de santé* »[674]. En effet, elle permet, en partie, de pallier les problématiques de santé énoncées précédemment. A titre d'exemple, les patients peuvent avoir la possibilité de bénéficier d'une consultation à distance par un professionnel spécialisé, sans avoir pour autant besoin de faire parfois des centaines de kilomètres pour aller le consulter, d'autant plus qu'avec l'inflation des coûts du carburant, les déplacements représentent un coût considérable pour le patient. Prenons l'exemple de la télésurveillance pour un patient dialysé. Une dialyse est réalisée trois fois par semaine au sein d'un établissement équipé pour le traitement. Or des patients habitant dans des zones reculées peuvent mettre jusqu'à plusieurs heures pour arriver jusqu'à un établissement de santé ce qui entraîne de la fatigue (pouvant engendrer d'autres maladies) et représente un coût pour le patient et/ou pour l'état, en cas de prise en charge par un véhicule médical. Pour éviter ces déplacements, des unités de dialyse sont mises en place dans les zones ne bénéficiant pas d'établissement proche, permettant la dialyse, avec une équipe médicale sur place. Une télésurveillance est assurée par un médecin néphrologue à distance afin qu'il puisse superviser la séance de dialyse[675]. *« Offrant une mutation spatiale et temporelle de l'exercice médical, les TIC déplacent les frontières traditionnelles »*[676].

263. **La télémédecine comme remède miracle** ? Pour autant, peut-on considérer que la télémédecine est « la » réponse aux problématiques de santé actuelles ? C'est un moyen de réponse, mais seul, il n'est pas suffisant. En effet, « *la télémédecine constitue un moyen opportun de pallier certaines consultations en présentiel, voire de traiter ponctuellement des patients sans solution d'offre médicale, mais il n'est pas souhaitable que la télémédecine devienne l'unique voie d'entrée dans le parcours de santé. Le toucher et la*

---

sur un territoire aux professionnels de santé du fait de leur absence ou de leur nombre trop limité ».

[672] Bruno ROJOUAN, « *Rapport d'information fait au nom de la commission de l'aménagement du territoire et du développement durable (1) par la mission d'information sur les perspectives de la politique d'aménagement du territoire et de cohésion territoriale (2), sur le volet « renforcer l'accès territorial aux soins »,* Rapport d'information n°589, 2022.

[673] *Ibid.*

[674] Stéphanie LANGARD, *Approche juridique de la télémédecine – entre Droit commun et règles spécifiques,* Thèse dactylographiée, Nancy, 2012, p. 30.

[675] HAS, « Les conditions de mise en œuvre de la télémédecine en unité de dialyse médicalisée », *Recommandations en santé publique - Synthèse et recommandations,* 2010.

[676] Claire DEBOST, Rodolphe BOURRET, Éric MARTINEZ et François VILLA, « La télémédecine, lecture contingente d'un cadre juridique invariant », *RDS,* 2014, n°58, pp. 1016-1032.

palpation sont des éléments majeurs de la prise en charge et du diagnostic des symptômes du patient. Il est important de préserver l'alternance entre consultations à distance et consultations physiques entre le soignant et le soigné : à défaut, le risque de développement d'une médecine à deux vitesses est bien réel, numérique pour les moins favorisés et humaines pour les plus favorisés »[677]. Il apparaît donc que la prise en charge médicale à distance est possible et souhaitable dans certains cas, mais n'est pas toujours possible ni opportune, car même s'il existe des outils permettant l'examen du patient, cela ne remplace pas le contact entre le praticien et le patient.

264. **Un acte de soin dématérialisé ?** Il apparaît que la télémédecine est un réel moyen de pallier les problématiques de santé et une réelle innovation dans la prise en charge du patient. Mais peut-on considérer l'innovation au point de considérer que télémédecine signifie dématérialisation de l'acte de soin ? La réponse semble davantage négative. *« La télémédecine n'est pas une dématérialisation de l'acte de soin, comme d'ailleurs l'utilisation de la visioconférence n'est pas une dématérialisation de l'audience mais signale l'existence d'une interface entre les personnes »*[678]. En effet, la relation et l'interaction patient-médecin requis sont certes dématérialisées, mais nous venons de voir que la manipulation du patient, si manipulation il y a besoin, est réalisée par un autre professionnel se trouvant avec le patient. Aussi, l'acte de soin en lui-même est réalisé physiquement, mais les données, elles, sont dématérialisées. Il a notamment été fait état précédemment que « *le toucher et la palpation sont des éléments majeurs de la prise en charge et du diagnostic des symptômes du patient »*[679], ce qui pour l'instant, n'est pas possible à distance pour le médecin requis.

En revanche, nous pouvons tout à fait parler d'une prise en charge dématérialisée. En effet, certaines d'entre elles ne nécessitent pas d'auscultation telles qu'une consultation préanesthésique ou une consultation pour un renouvellement d'ordonnance que le patient peut faire seul, de son domicile, avec le médecin requis.

§2 L'inclusion de la télémédecine dans le droit commun

265. **Une prise en charge « ordinaire ».** Bien que la télémédecine présente de nombreux avantages et perspectives, il apparaît qu'elle possède également des limites. Pour

[677] Bruno ROJOUAN, « *Rapport d'information fait au nom de la commission de l'aménagement du territoire et du développement durable (1) par la mission d'information sur les perspectives de la politique d'aménagement du territoire et de cohésion territoriale (2), sur le volet « renforcer l'accès territorial aux soins », op. cit.*
[678] Valérie OLECH, *Le secret médical et les technologies de l'information et de la communication*, *op. cit.*, p. 103
[679] *Ibid.*

autant, depuis 2010, son utilisation ne fait que s'accroitre permettant plus d'une centaine de cas d'usage de la télémédecine et du télésoin[680]. Afin de pouvoir au mieux utiliser la télémédecine, en adéquation avec les besoins, et afin de s'assurer qu'elle présente des garanties suffisantes par rapport à une prise en charge « traditionnelle », le statut juridique de la télémédecine n'a fait qu'évoluer ces dix dernières années (A), de telle sorte qu'elle est aujourd'hui, véritablement reconnue comme étant un mode de prise en charge « ordinaire » (B).

A) L'évolution du statut de la télémédecine

266. **L'instauration d'un cadre juridique de la télémédecine[681].** Le cadre juridique de la télémédecine a été introduit dans le Code de la santé publique par la loi HPST[682] accompagnée de son décret d'application[683]. Ces dispositions ont permis de poser un socle juridique à la télémédecine en définissant ce qu'était la télémédecine ainsi que ses modalités de mise en œuvre et de financement. En 2010, le recours à la télémédecine était très encadré : concernant les conditions de mise en œuvre, un des points majeurs était que l'acte de télémédecine devait être réalisé avec le consentement libre et éclairé de la personne concernée, ce consentement devait donc être exprès. Il était également précisé que les professionnels pouvaient, « *sauf opposition de la personne dûment informée, échanger des informations relatives à cette personne* »[684]. De plus, l'activité de télémédecine devait faire l'objet d'une organisation particulière : « *1° Soit d'un programme national défini par arrêté […] 2° Soit d'une inscription dans l'un des contrats pluriannuels d'objectifs et de moyens ou l'un des contrats ayant pour objet d'améliorer la qualité et la coordination des soins […] 3° Soit d'un contrat particulier signé par le directeur général de l'agence régionale de santé et le professionnel de santé libéral ou, le cas échéant, tout organisme concourant à cette*

[680] Thierry MOULIN et Pierre SIMON, *Télémédecine et télésoin – inclus 100 cas d'usage pour une mise en œuvre réussie*, Elsevier Masson, 2021.
[681] Claire DEBOST, Rodolphe BOURRET, Éric MARTINEZ et François VILLA, « La télémédecine, lecture contingente d'un cadre juridique invariant », *op. cit. « Cette introduction nouvelle dans le code la santé publique de la télémédecine ne doit pas faire oublier l'ancienneté d'une pratique généralisée auprès des professionnels médicaux. La télémédecine, en tant que médecine à distance, est sollicitée par le médecin qui répond à l'appel téléphonique de l'un de ses patients en demande de conseil, ou encore par le médecin qui sollicite l'expertise d'un confrère, par impératif déontologique ».* En effet, malgré son introduction dans le code de la santé publique depuis 2009, la télémédecine était déjà pratiquée par les professionnels de santé.
[682] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (1), dite HPST (hôpital, patients, santé et territoires), JORF n°0167, 22 juillet 2009, texte n°1.
[683] Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine, JORF n°0245, 21 octobre 2010, texte n°13.
[684] C. santé publ., art. R. 6316-2, version en vigueur du 22 octobre 2010 au 05 juin 2021.

activité ».[685] Qui plus est, les établissements et professionnels organisant une activité de télémédecine entre eux, devaient conclure une convention en adéquation avec les contrats et/ou programmes dans lequel l'activité s'inscrivait. Ce formalisme complexifiait le développement du recours à la télémédecine.

267. **La mise en place d'expérimentation et de projet locaux.** Des expérimentations ont ensuite vu le jour telles que le programme ETAPES en 2014 (expérimentations de télémédecine pour l'amélioration des parcours en santé) afin d'encourager et d'apporter un soutien financier pour la création de projet de télémédecine. Ce programme portait sur la télésurveillance de certaines affections de longue durée. « *Initialement menées dans neuf régions, ces expérimentations s'étendent en 2017 à tout le territoire »*[686].

Des projets plus locaux ont également vu le jour grâce à des appels à projet pour le financement d'équipement de télémédecine ou simplement des enveloppes de financement pour le développement de la e-santé en région. Pour cela, les ARS (Agences Régionales de Santé) qui « *sont responsables de la déclinaison régionale des politiques nationales de santé »*[687] ainsi que de « *la politique numérique en santé »*[688] s'appuient sur des structures régionales, les Groupements Régionaux d'Appui au Développement de la e-Santé (GRADeS) afin de mener à bien et décliner la politique nationale sur la e-santé en région. Ces GRADeS ont notamment pour mission de proposer aux professionnels et structures de santé des régions, des outils permettant la e-santé dont l'utilisation peut parfois être financée par des financements publics.

268. **Le financement dans le Droit commun**. Ce n'est qu'à partir de 2016 avec la signature de la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie, que les premiers remboursements par l'Assurance Maladie ont été réalisés ; ils ne concernaient que des actes de téléconsultation et de téléexpertise en EHPAD[689]. Dès 2018, l'avenant 6 à cette convention est venue faire entrer dans le Droit commun, le remboursement des actes de téléconsultation et de téléexpertise par l'Assurance

[685] C. santé publ., art. R. 6316-6, version en vigueur du 22 octobre 2010 au 15 septembre 2018.
[686] Vie publique, « La télémédecine, une pratique en voie de généralisation », *Eclairage,* 2020.
[687] Instruction n°SG/DSSIS/2017/8 du 18 janvier 2017 relative à l'organisation à déployer pour la mise en œuvre de la stratégie d'e-santé en région.
[688] *Ibid.*
[689] Arrêté du 20 octobre 2016 portant approbation de la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016, JORF n°0248, 23 octobre 2016, texte n°10.

Maladie[690]. *« Des précisions sur la mise en œuvre des aménagements et exceptions aux grands principes conditionnant la prise en charge de la téléconsultation ont depuis été introduites par l'avenant n° 8 à la convention médicale et plus récemment par l'avenant n° 9, qui simplifie et élargit le cadre de la prise en charge, notamment pour les patients résidant en zones sous-denses »*[691]. En revanche, pour être pris en charge, l'acte de téléconsultation doit répondre à trois conditions : « *inscription dans le respect du parcours de soins coordonné avec orientation préalable du médecin traitant, alternance obligatoire nécessaire de consultations en présentiel et de téléconsultations, inscription dans une logique d'ancrage territorial aux soins* »[692].

269. **Une augmentation des actes de télémédecine.** Malgré l'encadrement juridique mis en place depuis plus d'une dizaine d'année, les expérimentations, les appels à projet et les aides au financement, « *l'usage de la télémédecine s'est révélé très anecdotique en 2017, avec seulement 1 500 actes de téléconsultations, et 2018 avec 5 985 actes de téléconsultations et moins de 1% des médecins concernés par cette pratique »*[693]. Grace au remboursement des actes par l'Assurance Maladie, ceux-ci augmentent progressivement. « *En 2019, on recense 136 882 téléconsultations facturés au total, et les deux premiers mois de 2020 ont permis d'enregistrer chacun plus de 20 000 actes de téléconsultations facturés »*[694], réalisés par 13% des médecins.

Pourtant, l'utilisation de la télémédecine par les praticiens peine à décoller pour les raisons suivantes : *« des raisons technologiques. C'est la mauvaise couverture numérique du territoire qui est le plus souvent citée : 11 millions de citoyens n'ont pas accès à des connexions de qualité, les privant ainsi de l'hospitalisation à domicile et des services de téléassistance. Sont également invoqués le manque d'interopérabilité entre les systèmes, l'absence d'identifiant national de santé unique, une protection insuffisante des données, le retard dans la généralisation du DMP… Des raisons juridiques et techniques avec l'absence totale de dématérialisation des prescriptions médicales, préalable légal à la télémédecine en permettant la traçabilité des soins, les incertitudes sur les responsabilités des acteurs*

[690] Arrêté du 1er août 2018 portant approbation de l'avenant n°6 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016, JORF n°0183, 10 août 2018, texte n°16.
[691] Bruno ROJOUAN, « *Rapport d'information fait au nom de la commission de l'aménagement du territoire et du développement durable (1) par la mission d'information sur les perspectives de la politique d'aménagement du territoire et de cohésion territoriale (2), sur le volet « renforcer l'accès territorial aux soins », op. cit.*
[692] *Ibid.*
[693] *Ibid.*
[694] *Ibid.*

(médecins, opérateurs, industriels…). Des raisons politiques, les pouvoirs publics ayant privilégié la mise en œuvre d'actions expérimentales, plutôt qu'une reconnaissance officielle du dispositif. On peut ajouter un manque de continuité dans les actions avec, par exemple, l'abandon en 2012 du plan national de déploiement de la télémédecine présenté en 2011 par le ministère de la santé. Des raisons économiques, avec l'absence d'un modèle tarifaire pérenne pour les actes de télémédecine. La question du financement, à la fois son volume et sa pérennité, est toujours vitale, quel que soit le projet. La télémédecine n'y échappe pas (SALIBA et autres, 2012). Des raisons liées au manque d'information des médecins et du grand public, à la maîtrise insuffisante de l'outil informatique, à la crainte d'une déshumanisation de la médecine… ».[695] Pour autant, on constate ces dernières années, une volonté des pouvoirs publics et du législateur de venir endiguer ces freins au développement de la télémédecine et par extension, au télésoin, en développement des structures de proximité ayant recours à la télésanté, ou encore en incluant la télémédecine dans le droit commun.

270. **La télémédecine comme réponse à la pandémie Covid-19.** La pandémie du Covid-19 a également joué un rôle dans le développement de la télémédecine et plus particulièrement de la téléconsultation ; elle a fait considérablement évoluer le volume d'actes de téléconsultations réalisés à cause de la mise en place des différents confinements mais également du risque de contamination. Un allègement des règles de réalisation a été mis en place compte tenu de l'état d'urgence sanitaire dans laquelle se trouvait le pays, notamment une prise en charge à 100% par l'assurance maladie de toutes les téléconsultations. En avril 2020, près de 4,4 millions de téléconsultations ont été comptabilisées. Pendant cette période, plus de 71% des médecins, principalement des médecins libéraux, ont réalisé des téléconsultations.

A la suite des déconfinements, *« le volume de téléconsultation baisse significativement […]. En juin 2020, l'assurance maladie a ainsi enregistré 521 000 téléconsultations la première semaine, puis 506 000 la suivante, 427 000 la troisième et 396 000 durant la dernière ».*[696] Pour autant, même si le nombre d'actes de téléconsultation a baissé, il reste très élevé par rapport à avant le confinement, laissant penser que *« les actes médicaux à distance s'inscrivent progressivement comme des pratiques pérennes »*[697]*, « l'habitude ayant été prise,*

[695] Jean-François NYS, « La télémédecine, simple évolution ou véritable révolution des usages dans le système de santé français ? », *Marché et organisations*, 2020/2, n°38, pp. 15-36.
[696] Vie publique, « La télémédecine, une pratique en voie de généralisation », *op. cit.*
[697] Bruno ROJOUAN, « *Rapport d'information fait au nom de la commission de l'aménagement du territoire et du développement durable (1) par la mission d'information sur les perspectives de la politique d'aménagement du territoire et de cohésion territoriale (2), sur le volet « renforcer l'accès territorial aux soins », op. cit.*

la téléconsultation va rapidement devenir un acte banal »[698]. Il est estimé que le *« Covid-19 a fait gagner cinq ans en matière d'acculturation à la télémédecine, tant du côté des patients que de celui des professionnels de santé »*[699].

B) Une prise en charge devenue « ordinaire »

271. **Un allègement des mesures.** Un allègement progressif de la mise en œuvre de la télémédecine a été effectué : tout d'abord en 2018, avec la suppression de l'obligation de faire partie d'un programme ou de signer un contrat pour sa mise en œuvre et d'autre part avec la suppression de l'obligation de conventionner entre les participants d'une telle activité[700]. Ces changements permettent de favoriser la mise en place d'une activité de télémédecine en simplifiant ses modalités de mise en œuvre.

Ce qui marque d'autant plus l'entrée de la télémédecine comme un mode de prise en charge « ordinaire », est la suppression en 2021, du consentement exprès du patient pour la réalisation de l'acte[701]. En revanche, il ne faut pas confondre le consentement à l'acte de télémédecine et le consentement à la réalisation d'un acte médical. Dans le cas d'espèce, seul le consentement à l'utilisation des TIC est supprimé. Cette suppression montre très clairement que l'utilisation des TIC pour la prise en charge d'un patient n'est plus une exception nécessitant un accord du patient, mais un mode « normal » de prise en charge.

272. **Une pratique ordinaire pour les professionnels de santé et les patients ?** Les chiffres liés à la montée en puissance du recours à la téléconsultation même après le confinement tendent à montrer que les professionnels de santé sont favorables à l'utilisation de la télémédecine et continuent de proposer ce mode de prise en charge. La télésanté est d'autant plus favorisée par l'inclusion dans le Code de la santé publique du télésoin[702] qui « *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 »*[703]. Ce dernier *« vient compléter*

---

[698] Jean-François NYS, « La télémédecine, simple évolution ou véritable révolution des usages dans le système de santé français ? », *op. cit.*
[699] Laura LETOURNEAU, « Transformations numériques et entrepreneuriales – l'improbable transformation numérique de la santé », *op. cit.*
[700] Décret n° 2018-788 du 13 septembre 2018 relatif aux modalités de mise en œuvre des activités de télémédecine, JORF n°0212, 14 septembre 2018, texte n°11.
[701] Décret n°2021-707 du 3 juin 2021 relatif à la télésanté, JORF n°0128, 4 juin 2021, texte n°15.
[702] Intégré par la Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (OTSS), JORF n° 0172, 26 juillet 2019, texte n° 3, article 53.
[703] C. santé publ., art. L. 6316-2.

la télémédecine dans la nouvelle organisation des professionnels de santé au sein d'un territoire de santé numérique. C'est probablement l'innovation la plus attendue des professionnels de santé non médicaux. Le télésoin, après la télémédecine, va contribuer à façonner une nouvelle organisation des soins à distance au sein d'un territoire de santé numérique »[704], permettant ainsi aux usagers d'avoir un plus large choix quant aux modalités de leur prise en charge médicale.

Quant aux usagers, ces derniers sont ouverts à utiliser la télémédecine et le télésoin. Dans une étude réalisée par Harris Interactive en janvier 2020, « *de plus en plus, les Français se déclarent favorables au développement de la téléconsultation en France (68%, +5points). Elle est soutenue particulièrement par les plus jeunes (78% chez les moins de 35 ans), les Français les plus aisés (73%) et ceux habitant en région parisienne (75%). […] 58% d'entre eux déclarent aujourd'hui qu'ils pourraient y recourir (+6 points), principalement les plus jeunes (69%), les Français les plus aisés (67%), les habitants de région parisienne (66%), c'est-à-dire les personnes déjà plus favorables que la moyenne au développement de la téléconsultation, mais également les parents (66%) ou les Français qui ont l'habitude de changer de médecin (75%). Seuls les Français les plus âgés (52% contre 42% de l'ensemble) se montrent majoritairement plus réticents »*[705].

Ces chiffres, combinés au nombre de téléconsultations réalisés par mois, ainsi que la projection du nombre des futures téléconsultations montrent que la télémédecine ne va faire que s'accroitre et qu'elle est devenue un mode traditionnel de prise en charge.

273. **Les limites du recours à la télémédecine.** Bien que la télémédecine soit entrée maintenant dans les mœurs, certaines limites restent identifiées telles que :

i. L'avenant 9 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie prévoit qu'un « *médecin conventionné ne peut […] pas réaliser plus de 20% de son volume d'activité globale conventionnée à distance (téléconsultations et téléexpertises cumulées) sur une année civile »*[706], limitant ainsi le recours à la télémédecine pour un médecin.

[704] Jean-François NYS, « La télémédecine, simple évolution ou véritable révolution des usages dans le système de santé français ? », *op. cit.*
[705] Harris interactive, « *Baromètre : les français et la téléconsultation – vague 2 »,* Enquête Harris Interactive pour Livi, 2020.
[706] Arrêté du 22 septembre 2021 portant approbation de l'avenant no 9 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016.

ii. Le remboursement des actes se font sous certaines conditions, ce qui ne permet pas le remboursement de la totalité des actes de téléconsultation, malgré des exceptions énoncées. Aussi, tous les patients ne sont pas éligibles au remboursement des actes, ce qui provoque une inégalité de traitement entre les patients.

iii. Comme évoqué précédemment, l'impossibilité de recourir à des actes de télémédecine, lorsque des actes de soins particuliers sont à réaliser comme une palpation.

Pour pallier ces limites, des propositions sont apportées comme l'élévation de la marge de 20%. *« Ce principe aurait pour avantage de prévenir l'émergence de télémédecins à plein temps, même si une réflexion pourrait être menée pour prévoir des exceptions au profit de certaines activités médicales ou certains types de praticiens ».*[707]

[707] Bruno ROJOUAN, « *Rapport d'information fait au nom de la commission de l'aménagement du territoire et du développement durable (1) par la mission d'information sur les perspectives de la politique d'aménagement du territoire et de cohésion territoriale (2), sur le volet « renforcer l'accès territorial aux soins », op. cit.*

Section 2 : La e-santé, au cœur de la prise en charge actuelle

274. **La télémédecine et la télésanté : un champ restreint.** La télémédecine, et maintenant le télésoin, sont des pratiques identifiées par le public comme étant de la e-santé ou de la santé numérique. Or, ces derniers ne couvrent qu'une petite partie du champ de la e-santé.

275. **La e-santé : un champ bien plus vaste.** En effet, la e-santé recouvre donc un champ bien plus vaste de services et de systèmes, qui deviennent petit à petit indispensables pour la prise en charge d'un patient (§1). Cependant, avec la multitude d'outils d'e-santé au niveau national, peut-on affirmer que ces derniers sont tous fiables (§2) ?

§1 Les outils de la e-santé : des incontournables

276. **Un outil de la e-santé**. Un des sens du mot outil peut être défini comme « *un élément d'une activité qui n'est qu'un moyen, un instrument* »[708], « *qui permet d'obtenir un résultat, d'agir sur quelque chose »*[709]. A titre d'exemple du domaine quotidien, la tonte d'herbes dans un jardin : elle est réalisée par une personne à l'aide d'une tondeuse, qui n'est autre qu'un outil ou encore un instrument permettant la réalisation de la tâche visée.

En e-santé, le principe est le même. La e-santé est l'alliance des TIC et de la santé si bien que les TIC, peu importe le type de technologie utilisé, est l'outil ou l'instrument nécessaire au profit de la santé. Cet outil peut prendre plusieurs formes comme un logiciel ou encore un service.

277. **Des outils réellement incontournables ?** L'outil en tant que TIC est indispensable afin de pouvoir considérer que l'activité réalisée est de la e-santé, il s'agit d'une condition impérative. Mais est-ce que l'e-santé est vraiment incontournable dans notre système de santé actuel et futur pour la prise en charge du patient ?

L'Agence du Numérique en Santé, qui « *contribue à l'amélioration du système de santé »*[710] et qui est en charge d'accompagner au développement du numérique en santé expose que la e-santé est présente à tout moment en santé : *« La e-santé est là pour vous accompagner à*

[708] Larousse, *V° « outil »*, nom masc.
[709] TLFi, *V° « outil »*, subst. masc.
[710] ANS, *Bienvenue sur le portail de l'ANS.* Disponible à l'adresse : https://esante.gouv.fr/ (consulté le 15/07/2022). L'ANS travaille « *aux côtés de la Délégation ministérielle au numérique en santé, des agences régionales de santé, des Groupements Régionaux d'Appui au Développement de la e-santé et de l'ensemble des acteurs de l'écosystème ».*

toutes les étapes de votre parcours de soin, et tout au long de votre vie pour pérenniser ou améliorer votre santé, parfaire votre pratique médicale et, in fine, vous permettre d'appréhender la santé de demain »[711]. Elle peut aussi bien intervenir au moment de la consultation, notamment avec la télémédecine et le télésoin, que pendant le suivi médical du patient (A), mais également à toutes les étapes de la prise en charge du patient, laissant un nombre infini d'opportunités et de possibilités (B).

A) Un suivi médical à tous les niveaux

278. **Le suivi médical**. Le suivi médical peut être envisagé de deux façons :

i. soit par le suivi régulier d'une personne afin de contrôler son état de santé et/ou réaliser des examens médicaux périodiques ; il peut s'agir du suivi médical du nourrisson pour lequel quatre examens sont prévus de sa naissance jusqu'à ses deux mois, afin de procéder à la mise en place de la vaccination, mais c'est également « *un moment privilégié qui permet au médecin de répondre aux interrogations des parents »*[712]. Par la suite, d'autres rendez-vous seront prévus pour réaliser le rappel des vaccins mais également pour s'assurer que le nourrisson se développe normalement.

ii. Soit par un suivi médical pour garantir la prise en charge du patient à la suite d'un acte médical, tel qu'une opération chirurgicale. En effet, à sa sortie, le patient pourra se voir prescrire des séances de kinésithérapie, un suivi par une infirmière à domicile ; il sera sans doute convoqué pour un examen de contrôle par le chirurgien en post-opératoire. Que ce soit l'un ou l'autre des suivis, ceux-ci sont favorisés par l'utilisation de la e-santé.

279. **Le suivi du patient au sein de l'établissement de santé.** Comme cela a déjà été évoqué, la dématérialisation du dossier patient au sein des établissements de santé permet pour tous les professionnels de santé habilités et prenant en charge un patient, l'accès en temps réel à ses données de santé. Ainsi, en cas de changement de service d'un patient au cours d'une hospitalisation, son dossier reste accessible par toutes les équipes favorisant son suivi pendant toute sa prise en charge.

280. **Le lien ville-hôpital favorisé**. Outre le suivi du patient favorisé au sein même de l'établissement de santé, la e-santé permet de favoriser le lien ville-hôpital qui est encore aujourd'hui trop peu utilisé. La fédération Hospitalière de France a présenté un rapport le 9

[711] ANS, *Ce que la e-santé fait pour vous.* Disponible à l'adresse : http://esante.gouv.fr/ (consulté le 07/08/2022).
[712] Améli, *Suivi médical jusqu'aux 2 mois du nourrisson,* Santé comprendre et agir, 2022.

mars 2018, proposant des solutions afin de favoriser le lien ville-hôpital. Parmi les dix-sept propositions, on peut retrouver notamment la simplification des échanges entre la ville et l'hôpital en nommant une personne identifiée comme « *leur interlocuteur institutionnel »*[713] ou encore *« rendre obligatoire la communication des résultats médicaux aux médecins généralistes. Réciproquement, rendre obligatoire la transmission des éléments aux Centres hospitaliers avant une admission »*[714].

C'est un des objectifs de la stratégie « Ma Santé 2022 » qui est d'améliorer la coopération entre les différents acteurs de santé et de procéder au décloisonnement des liens entre la ville, l'hôpital et le médico-social. C'est notamment ce qu'a énoncé Agnès Buzyn lors de son discours d'inauguration de la Paris Healthcare Week du 29 mai 2019[715]. A ce titre, la DGOS a lancé « *le programme HOP'EN qui constitue le nouveau plan d'action national des systèmes d'information hospitaliers à 5 ans et l'action 19 de la feuille de route « accélère le virage du numérique » »*[716] qui fait partie d'un des chantiers de Ma Santé 2022[717]. Un des objectifs de ce programme est de « *développer et simplifier les liens entre l'hôpital et ses partenaires, notamment la ville et le médico-social dans une logique de prise en charge décloisonnée, via le déploiement et l'usage de services socles tels que les messageries conformes à l'espace de confiance MS Santé, l'alimentation du DMP (Dossier médical Partagé), et d'autres outils régionaux ou nationaux (mis à disposition via le programme e-parcours notamment)* »[718].

Des projets plus régionaux ont également vu le jour tels que le projet Harpicoop[719] afin de pallier, à plus petite échelle, aux problématiques rencontrées : « *l'outil d'information du CHRU de Nancy, Harpicoop, fluidifie la communication avec les médecins de ville. Grâce à ce dispositif, les médecins traitants sont informés en temps réel de l'admission de l'un de leurs patients dans un service d'hospitalisation programmé ou d'urgence des établissements du Groupement Hospitalier Territorial (GHT) Sud Lorraine dont fait partie le CHRU de Nancy. A l'hôpital, le système d'information génère, de façon automatisée, l'envoi d'un mail*

[713] Jean-Pierre JARDRY (Dr), *« Renforcer le lien ville hôpital »*, Rapport de la FEMAS, 2018.
[714] *Ibid.*
[715] Agnès BUZYN, « *Discours* », Inauguration de la Paris Healthcare Week, 2018.
[716] Ministère de la santé et de la prévention, « La programme HOP'EN », 2022. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 23/07/2022).
[717] Agnès BUZYN, Laura LETOURNEAU, Dominique PON, « *Feuille de route « accélérer le virage numérique » »*, Dossier d'infirmation – conférence ministre, 2019.
[718] Instruction n°DGOS/PF5/2019/32 du 12 février 2019 relative au lancement opérationnel du programme HOP'EN.
[719] Harmonisation à l'Admission en hospitalisation des pratiques de Recueil et de Partage d'Informations facilitant la COOrdination des Professionnels.

au médecin traitant. Grâce à ce courriel, le médecin traitant peut ainsi adapter sa prise en charge lors du retour à domicile du patient, pour éviter toute rupture de soins. »[720].

On constate donc que le lien ville-hôpital est une des priorités pour améliorer notre système de santé, que les outils de la e-santé sont fortement sollicités et qu'ils sont les facteurs clés de la réussite de cet objectif.

281. **Une nouvelle organisation en ville.** Bien qu'un décloisonnement ville-hôpital soit en marche, une coopération plus accrue en ville est également souhaitée. Une des organisations mises en place pour répondre à ce besoin est la création, par la Loi de modernisation de notre système de santé de 2016, des Communautés Professionnelles Territoriales de Santé (CPTS). Elles *« constituent un dispositif souple à la main des professionnels qui veulent travailler ensemble pour répondre aux besoins de santé spécifiques d'un bassin de population »*[721] en créant ensemble, un projet de santé commun. Aussi, plusieurs professionnels, exerçant différentes professions peuvent *se regrouper afin de « mieux structurer leurs relations et mieux se coordonner »*[722] et ainsi *« concourir à la structuration des parcours de santé »*[723], notamment au suivi du patient. Ce dispositif n'est pas limité aux professionnels de santé de ville, mais aux acteurs de santé en général, puisque des établissements de santé ou encore des acteurs du médico-social et du social peuvent participer au projet et faire partie de la CPTS.

Les CPTS ayant souscrit à l'accord conventionnel interprofessionnel en faveur du développement de l'exercice coordonné et du déploiement des communautés professionnelles territoriales de santé signé le 20 juin 2019[724], ont notamment l'obligation de *« contribuer au développement télémédecine* »[725]. En effet, *« les partenaires conventionnels s'accordent pour reconnaitre que la télémédecine constitue un nouveau mode d'organisation utile pour améliorer l'accès aux soins de certains patients rencontrant des problèmes de mobilité »*[726]. Ces structures organisées favorisent donc le décloisonnement des acteurs de santé afin de

[720] ARS Grand Est, *« Rapport d'activité 2020 »*, Rapport, 2020.
[721] Ministère de la santé et de la prévention, « Les communautés professionnelles territoriales de santé (CPTS) », 2022. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 15/07/2022).
[722] ARS, « les communautés professionnelles territoriales de santé », 2021. Disponible à l'adresse : https://www.ars.sante.fr/ (consulté le 15/07/2022).
[723] C. santé publ., art. L. 1434-12.
[724] Arrêté du 21 août 2019 portant approbation de l'accord conventionnel interprofessionnel en faveur du développement de l'exercice coordonné et du déploiement des communautés professionnelles territoriales de santé signé le 20 juin 2019, JORF n°0196, 24 août 2019, texte n°5.
[725] Arrêté du 21 août 2019 portant approbation de l'accord conventionnel interprofessionnel en faveur du développement de l'exercice coordonné et du déploiement des communautés professionnelles territoriales de santé signé le 20 juin 2019, JORF n°0196, 24 août 2019, texte n°5, art. 5.1.1.
[726] *Ibid.*

permettre une meilleure prise en charge du patient et notamment de son suivi, en utilisant la télémédecine (et bientôt le télésoin)[727] donc plus généralement la e-santé.

282. **Le suivi du patient, par le patient.** Au fur et à mesure, on assiste à un changement de la place du patient dans sa prise en charge. Autrefois simple spectateur, il est aujourd'hui au cœur de sa prise en charge et est même devenu acteur, au même titre qu'un professionnel.

Prenons l'exemple d'une maladie chronique : cette dernière « *nécessite un investissement du malade qui doit apprendre à vivre avec, comprendre sa maladie, savoir adapter son traitement par rapport à son projet de vie, conserver son « capital santé » optimum. Pour cela, il doit être éduqué, accompagné, voire même encouragé, et certainement pas culpabilisé. Le rôle du médecin et de tous les « soignants » consiste donc à permettre au patient de devenir acteur de sa santé. […] Créer le changement des comportements des professionnels, c'est transformer notre système de soins en système de santé, c'est accepter l'expertise profane du patient, et reconnaître le rôle d'aidant aux associations de patients* »[728].

Le changement de la place du patient en tant qu'acteur est d'autant plus marquant que de nombreux outils accessibles au public, lui permettent de prendre soin de sa santé en toute autonomie, même en dehors des maladies chroniques. Bon nombre d'objets connectés tels que les montres, permettent de suivre le rythme cardiaque de la personne, calculent le nombre de calories dépensées en une journée, ou encore évaluent la qualité de son sommeil. Tous ces éléments permettent à la personne de contrôler et suivre son état de santé, éventuellement consulter un spécialiste au besoin, notamment en fonction des données recueillies à la suite de l'utilisation de ces objets connectés. Ces objets connectés *« représentent de véritables assistants en situation d'exercice médical ou para médical assurant au patient d'être maître*

[727] Lina WILLIATTE-PELLITTERI, « Le télésoin et la télésanté selon le décret et l'arrêté du 3 juin 2021 », *RDS*, 2021, n°103, pp. 790-788. A juste titre Lina WILLIATTE-PELLITTERI a énoncé ceci : « *À n'en pas douter, le télésoin est entré dans la pratique du soin beaucoup plus rapidement que ne l'a été la télémédecine. Crise sanitaire ? Leçon du passé ? La télésanté fait d'ores et déjà partie des modalités de réalisation du soin. Si les textes sont synchronisés avec les attentes du terrain, ils sont cependant en avance au regard du comportement des professionnels de santé qui voient, à tort, dans la télésanté une pratique dégradée du soin. Une telle façon de penser démontre que ces mêmes professionnels n'ont pas saisi le sens même d'une telle évolution des pratiques, car in fine, il s'agit de faire en sorte de maintenir le lien, même virtuel, entre le patient et le soin, afin que celui-ci puisse bénéficier d'une prise en charge continue et de qualité, et certainement pas d'éluder la prise en charge physique au profit d'une virtualisation du soin ».* Aussi ne faut-il pas voir la télésanté comme un moyen de se soustraire, pour un professionnel de santé, de voir le patient en tête à tête, même si la technologie le permet. Rappelons-le, la télésanté n'est qu'un moyen de prise en charge et non le moyen de prise en charge.

[728] Gérard RAYMOND, « Le patient acteur de sa santé », *Bull. Acad. Méd ?*, 2013, n°8, pp-1545-1546.

des activités de détection précoce de la maladie, de suivi ou de soins, jusque-là assurées uniquement par les professionnels de santé […] En termes de santé et en complément de l'éducation à la santé assurée par les informations et des services en ligne, trois vertus aux objets connectés lui ont été reconnus : prévention accrue et meilleure qualité de vie, systèmes de santé plus efficients et plus durables, patients plus responsables. »[729].

B) Les possibilités infinies de la e-santé

283. **Les termes de la e-santé.** Comme cela a été évoqué, la e-santé bénéficie d'une définition extrêmement large permettant d'inclure en son sein, de nombreux domaines, activités, services ou encore savoirs, impliquant une constante évolution de son champ d'activités. On peut y intégrer : la santé mobile, la prise de rendez-vous médicaux en ligne, le dossier patient informatisé, la télésanté, la e-prescription, les outils d'indentification (e-CPS, e-carte vitale), dossier médical partagé, compte-rendu dématérialisé, robotique au profit de la santé et bien d'autres encore. D'autres terminologies et champs sont voués à être ajoutés au fur et à mesure, au regard de l'implication grandissante du numérique dans le domaine de la santé et du champ large que recouvre la e-santé.

284. **La e-santé à tous les stades de la santé**. Cela est d'autant plus vrai que la e-santé est présente à tous les stades de la santé : de la prévention, soit en amont de la prise en charge du patient, au moment de la consultation et du diagnostic, mais aussi pour le suivi du patient ou encore pour toutes les questions de recherche et de statistiques.

En effet, *« un des aspects de la e-santé réside dans le partage et la mise à disposition des données de santé pour la recherche. C'est d'ailleurs un des principaux objectifs de la plate-forme Health Data Hub, qui s'inscrit dans la stratégie « Ma santé 2022 ». […] La recherche comprend un volet important consacré à la prévention de certaines maladies ou affections qui visent notamment à identifier les facteurs de risques »*[730]. Ces recherches permettent notamment la prévention en santé.

285. **La e-santé, la santé d'aujourd'hui et de demain**. On assiste à un développement des pratiques, ou encore l'utilisation d'une technologie déjà existante, mais au profit de la santé. Prenons l'exemple de l'intelligence artificielle : *« Anticiper une*

[729] Jihane SEBAI, « La e-santé et le patient 2.0 : la colonisation démocratique ! », *Marché et organisations*, 2020/2, n° 38, pp. 123-144.

[730] AG2R La Mondiale, « La e-santé, un outil de prévention ». Disponible à l'adresse : https://www.ag2rlamondiale.fr/ (consulté le 16/07/2022). La plateforme Helath Data Hub a été créé par l'arrêté du 19 novembre 2019.

épidémie, prédire une maladie ou son évolution, accélérer un diagnostic, personnaliser les traitements à l'individu ou encore accélérer les cycles de recherche & développement grâce aux algorithmes… Ce n'est désormais plus une promesse, mais la réalité des multiples possibilités offertes par l'intelligence artificielle appliquée à la santé et ses acteurs »[731]. L'IA pourra notamment être utilisée dans le cadre des diagnostics en fonction des données collectées.

Le numérique bénéficie d'un haut potentiel ouvrant les portes à la modernisation de la santé et aux développements de nouveaux services, activités et autre, à la limite de la science-fiction lorsque l'on en parle aujourd'hui. *« Lorsqu'on imagine la façon dont nous serons soignés en 2030, les images sont séduisantes : jumeau digital pour tester les médicaments virtuellement avant de les prescrire à chaque patient, carte génétique de la tumeur en quelques secondes avant d'entrer dans le bureau du cancérologue, analyse de chaque cellule par l'intelligence artificielle… »*[732].

Le Leem[733] a réalisé une étude prospective en 2019, de l'innovation en santé pour 2030, exposant les innovations pouvant être attendues ces dix prochaines années dans notre système de santé, notamment avec l'utilisation de la e-santé et les changements qui devront être nécessaires dans notre organisation actuelle. Le champ des possibilités est vaste, par exemple avec la création du jumeau digital ou numérique : « *grâce à la biostimulation par ordinateur, la technique permettra, à terme, de modéliser notre propre « jumeau numérique » et de tester sur lui la réaction de notre organisme à différentes approches médicales. […] Certains tests de médicaments ou de prothèses s'effectueront sur un patient virtuel, non plus in vivo mais in silico en référence au composant clé des ordinateurs. Cette approche permettra d'étudier des maladies rares ou pédiatriques pour lesquelles il est difficile de recruter des patients pour des essais cliniques. Le jumeau numérique sera à même de transformer l'étude du vivant, le développement et la mise au point de nouvelles solutions thérapeutiques (anticipation de la toxicité d'un médicament, accélération de la recherche clinique, simulation des différentes options thérapeutiques, personnalisation des traitements) »*[734]. Le jumeau numérique est la dématérialisation de la personne afin de pouvoir la soigner mieux, d'abord en testant numériquement les effets des thérapeutiques ou pour réaliser des recherches, avant toute

[731] David GRUSON, « Saurez-vous décrypter les enjeux santé de demain ? », *MSN Connect*, 2022.
[732] Leem, « Santé 2030 : quels défis pour la santé de demain ? », *Analyse prospective de l'innovation en santé,* 2019.
[733] L'organisation professionnelle des entreprises du médicament opérant en France.
[734] Leem, « Santé 2030 : quels défis pour la santé de demain ? », *Analyse prospective de l'innovation en santé,* 2019, p. 48.

intervention sur l'Homme. Cette dématérialisation de l'Homme permet d'avoir des données et des résultats au plus près des effets réels.

Mais est-on prêt pour toutes ces avancées technologiques au profit de la santé ?

§2 La fiabilité des outils de la e-santé

286. **e-santé = fiabilité ?** Est-ce que la e-santé rime forcément avec fiabilité ? C'est-à-dire, est-ce que l'on est certain de l'absence de défaillance en cas d'utilisation de l'e-santé au profit de la santé, ou en tous cas, les soins seront-ils prodigués avec une qualité identique et présenteront-ils les mêmes garanties ?

En effet, avec la multitude de secteurs concernés par la e-santé et les possibilités qu'offre le numérique au profit de la santé, on assiste à une invasion de nouvelles technologies. Bien que ces outils aient pour objectifs d'améliorer la santé au sens général, tant dans la prise en charge du patient que pour des questions de prévention ou encore de recherche, l'améliorent-ils réellement et sont-ils aussi fiables qu'une prise en charge traditionnelle par exemple (A) ? Outre la fiabilité au niveau santé, il est également nécessaire de s'interroger sur la fiabilité de ces outils au niveau juridique (B). En effet, ce n'est pas parce que la e-santé *via* la technologie permet des avancées en santé et notamment dans la prise en charge du patient, qu'elles sont forcément conformes au Droit ou qu'elles bénéficient d'un encadrement juridique suffisant.

A) Une fiabilité de la prise en charge à deux vitesses

287. **Une prise en charge à deux vitesses.** Tout au long des développements, il a été démontré que la e-santé permet de faire évoluer la santé et notamment la prise en charge globale et dématérialisée du patient grâce à la multitude d'outils créés. Cependant, peut-on avoir une confiance aveugle en ces outils, et être certain que l'utilisation de la e-santé est aussi performante, fiable et sécurisée, qu'une prise en charge sans l'utilisation des TIC c'est-à-dire en présentiel ?

288. **Une prise en charge aussi efficace et sécurisée qu'une prise en charge en présentiel grâce à la télémédecine ?** L'utilisation des TIC et la dématérialisation de la prise en charge entraînent des difficultés supplémentaires qui n'ont pas toujours vocation à s'appliquer pour une prise en charge en présentiel. Dans un rapport de 2021 réalisé par la société Kaspersky[735], on peut dénombrer cinq problématiques liées à la dématérialisation de la

[735] KASPERSKY, *« Telehealth take-up : the risks and opportunities »*, Healthcare report 2021, 2021.

prise en charge du patient : une divulgation des données de patients à la suite d'un acte de télémédecine, une mauvaise protection des données ainsi qu'un système d'exploitation ancien. En effet, la dématérialisation des échanges entraîne davantage de risques liés au transit d'informations qu'un échange d'informations en présentiel. Ces problématiques peuvent être minimisées par le respect des standards en vigueur, notamment la PGSSI-S. Pour autant, il existera toujours un risque, d'autant que les équipements et les systèmes de sécurisation ont une durée de vie très courte, nécessitant des mises à jour constantes et des changements d'équipements qui peuvent être coûteux. Les deux dernières problématiques sont : un logiciel inadapté, car les logiciels proposés dans le commerce ne répondent pas totalement aux besoins des praticiens car non adaptés à la pratique ; et des erreurs de diagnostic du fait des limites techniques. Il est vrai que les solutions proposées pour des téléconsultations et des téléexpertises sont de plus en plus performantes, notamment par la qualité des images ou d'éléments mobiles pouvant être utilisés comme un stéthoscope ou un microscope. Cependant, il arrive encore qu'il y ait une mauvaise qualité de clichés, pouvant entraîner une erreur de diagnostic, bien que les préconisations soient telles qu'il est recommandé de ne pas réaliser de diagnostic si les conditions ne sont pas optimales pour la prise de décision.

En revanche, pour pallier toutes ces problématiques dues à la dématérialisation de la prise en charge, des solutions sont mises en place. C'est pour cela que les logiciels permettant la e-santé sont en constante évolution et suivent les évolutions technologiques, que les GRADeS ont été créés pour répondre au mieux au besoin des professionnels et proposer des outils les plus adaptés possibles, et que des référentiels sont disponibles pour sécuriser au maximum cette prise en charge. Aujourd'hui, de très nombreux professionnels et établissements utilisent un dossier informatisé, méthode susceptible d'occasionner des fuites de données.

289. **La remise en cause de la fiabilité d'un outil national.** *« Initialement conçu en 2007 pour répondre aux besoins d'orientation en urgence, le ROR a progressivement évolué pour devenir un référentiel recensant l'ensemble de l'offre sanitaire et du médico-social, et comprenant un volet sur la disponibilité des lits en établissement de santé »*[736]. Celui-ci a vocation à évoluer pour recenser également les offres dans le secteur libéral telles que celles des médecins, infirmiers ou encore masseurs-kinésithérapeutes ainsi que l'offre en télémédecine.

[736] Ministère de la santé et de la prévention, « Le répertoire national de l'offre de santé et d'accompagnement médicosocial – ROR – un socle d'informations utiles sur l'offre de santé », *op. cit.*

L'objectif du ROR est de *« faciliter l'orientation des patients et de leur entourage vers la structure la plus adaptée à leurs besoins, éviter le risque de rupture dans leur prise en charge, améliorer la coordination entre les acteurs du parcours de santé, de soins et de vie, en particulier pour les personnes âgées, en perte d'autonomie et en situation de handicap »*[737].

Bien que l'offre de soin et de prise en charge soit précise, une des fonctionnalités du ROR n'est pas totalement exploitée et peut entraîner une perte de chance pour le patient : la disponibilité des lits en établissement.

Les établissements recensent au sein du ROR leurs disponibilités en lits par service. Un système de code couleur est mis en place afin de voir la fiabilité de ces données[738] :

La couleur verte indique que les données ont été mises à jour il y a moins d'une heure, la jaune, moins de trois heures, la rouge, moins de six heures, la violette, moins de douze heures, la bleue, moins de vingt-quatre heure et la noire, plus de vingt-quatre heures. Cependant, de nombreux établissements ne mettent pas à jour régulièrement leurs données empêchant d'avoir une vision claire de la disponibilité. Soit, avec une mise à jour de moins de six heures, s'il restait un seul lit disponible, il est tout à fait possible que ce dernier soit finalement pris. Cette fonctionnalité permet donc d'avoir une idée générale des disponibilités afin d'orienter le patient vers un service disponible ; mais une vérification est obligatoire avant de l'y envoyer, notamment pour éviter une perte de temps et de chance en cas d'indisponibilité et une réorientation immédiate.

En soi, la fiabilité n'est pas totalement remise en cause, mais il est nécessaire de procéder à une vérification pour s'assurer de la véracité des données à l'instant *t*.

[737] *Ibid.*
[738] *Ibid.*

290. **Les applications e-santé, un danger pour le citoyen ?** Les applications en e-santé pouvant être téléchargées par tout citoyen sont très nombreuses. Elles permettent de prendre sa tension, contrôler son rythme cardiaque ou encore évaluer la gravité d'un bouton sur la peau etc. Ces applications utiles pour tout citoyen afin d'être acteur de sa santé, ne remplacent pas pour autant la consultation d'un professionnel de santé. « *Nombreux sont les professionnels de santé qui mettent en garde le suivi aveugle des conseils qu'elles prodiguent* »[739] ou des résultats qui sont donnés.

La RTBF[740] a fait appel au Docteur François SALES, un chirurgien oncologique spécialiste du cancer travaillant à l'institut Border à Anderlecht pour avoir son avis d'expert sur certaines de ces applications. Un test a été réalisé sur un de ses patients qui, ayant pris une photo d'une lésion sur sa peau, a consulté une de ces applications ; le résultat s'avérait être bénin à 72%. Or c'est un patient opéré par le Docteur SALES d'un mélanome. « *Ça veut dire que si le patient à l'époque avait utilisé cette application, il aurait été faussement rassuré. Et il n'aurait probablement pas consulté un médecin pour ça. Quand on regarde les études qui ont été effectuées sur ce type d'application, on constate qu'il y a des erreurs dans 20% des cas* ».[741]

Aussi, les résultats de ces applications ne sont pas toujours à prendre au pied de la lettre, la consultation d'un médecin reste toujours une nécessité. Certaines applications ont mêmes été retirées du marché telles qu'une application mesurant la tension artérielle en 2015 pour laquelle la tension de près de 80% des personnes hypertendues était sous-évaluée[742].

Pour autant, toutes ces applications ne sont pas à mettre dans le même panier. La Belgique a par exemple mis en place un site gouvernemental[743] référençant certaines applications de e-santé classées selon leur degré de fiabilité et étant considérées comme un dispositif médical.

---

[739] M comme Mutuelle, « Les applications e-santé sont-elles fiables ? », *Magazine M comme Mutuelle*, 2018.
[740] Radio-télévision belge de la Communauté française.
[741] Thomas DECHAMPS et Maurizio SADUTTO, « Les applications e-santé sont-elles fiables ? », *RTBF*, 2022.
[742] Stéphane KORSIA-MEFFRE, « HTA : une célèbre application mobile pour iPhone mésestime les chiffres tensionnels », *VIDAL*, 2016.
[743] MHealth Belgium, « Présentation ». Disponible à l'adresse : https://mhealthbelgium.be/ (consulté le 04/06/2022). *« mHealthBelgium, également connue sous le nom de mobile health Belgium, est la plate-forme belge pour les applications mobiles qui portent le marquage CE en tant que dispositif médical.*
Cette plateforme unique centralise toutes les informations pertinentes et nécessaires sur les applications mobiles pour les patients, les professionnels de santé et les établissements de santé en trois langues (néerlandais, français et anglais). Les informations sont liées au marquage CE, à la protection des données, à la sécurité des communications, à l'interopérabilité avec d'autres systèmes informatiques et au mode de financement de l'application. mHealthBelgium consiste en une pyramide de validation à trois niveaux. Une application entre toujours au niveau inférieur, M1, et peut monter dans la hiérarchie via M2 jusqu'au niveau supérieur, M3 ».

291. **Une fiabilité à vérifier.** Les outils de la e-santé sont très nombreux et présentent des niveaux de fiabilité variables. Il est donc nécessaire d'être vigilant, en tant que professionnel de santé, établissement ou encore patient, de choisir les outils les plus adaptés et les plus fiables permettant une prise en charge aussi bonne, qu'une prise en charge sans l'utilisation de la e-santé.

B) Des garde-fous juridiques nécessaires

292. **L'absence d'un Droit spécifique sur la e-santé.** La e-santé ne bénéficie pas de dispositions juridiques propres permettant d'encadrer cette pratique. En revanche, ce n'est pas parce qu'elle n'en bénéficie pas, que la e-santé n'est pas du tout encadrée. La télésanté, avec la télémédecine et le télésoin en est un exemple. Rappelons-le, le Code de la Santé Publique vient encadrer le télésoin au travers des articles L. 6316-1, L. 6316-2 et R. 6316-1 et suivants. Pour autant, les autres champs de la e-santé tels que les objets connectés, les services d'aide à la prise en charge du patient ou encore l'intelligence artificielle n'ont pas de régimes spécifiques. Il faut se rapprocher du Droit annexe pour en mesurer les contours juridiques. Mais l'utilisation des Droits annexes est-il suffisant ?

293. **L'encadrement juridique de la e-santé.** A l'instar de la dématérialisation d'un document, la dématérialisation de la prise en charge d'un patient par l'utilisation de la e-santé implique le cumul de plusieurs Droits spécifiques liés à leurs particularités. e-Santé suppose notamment l'application :

i. du RGPD pour la protection des données à caractère personnel[744], d'autant plus que les données traitées sont des données de santé, identifiées comme étant sensibles et devant faire l'objet d'une protection renforcée[745]. En effet, la dématérialisation des échanges et du traitement de données pour la prise en charge du patient, nécessitent la mise en place d'une protection particulière pour garantir la sécurité et la confidentialité des données de santé.

ii. de la règlementation sur l'hébergement de données, le cas échéant. Rappelons-le, dès lors qu'un hébergement de données a lieu chez un tiers, une certification doit être obtenue certifiant que les données sont conservées dans un environnement suffisamment sécurisé

[744] Renato BRASSELET, *La circulation de la donnée à caractère personnel relative à la santé, - disponibilité de l'information et protection des droits de la personne,* Thèse dactylographiée, Nancy, 2018.
[745] 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, JOUE, L 119, 04 mai 2016.

compte tenu des données traitées[746]. Cette certification certifie que les données sont conservées dans un environnement bénéficiant d'une sécurité suffisante et satisfaisante au regard de l'état de l'art en la matière.

iii. de la règlementation sur les dispositifs médicaux. Le cadre juridique des dispositifs médicaux est clairement établi par le Règlement (UE) 2017/745 du Parlement Européen et du Conseil du 5 avril 2017[747] ; ce dernier en donne une définition très claire[748]. Les produits et services d'e-santé entrant dans cette définition, doivent respecter ce Règlement selon la catégorie de risque à laquelle ils appartiennent. Plus le risque est grand, plus le régime de mise sur le marché est complexe. De manière générale, *« l'appareil doit assurer des fonctions précises concordant avec ce qui est indiqué sur son emballage, être sûr et efficace. Il détient également des informations confidentielles sur la patiente, le matériel doit donc être protégé contre toute interférence extérieure pour éviter le piratage de ces données. […] De ce fait, il ne peut être mis sur le marché qu'à la condition de ne pas porter atteinte à la santé et à la sécurité des patients et de leurs utilisateurs sous peine de retrait »*[749].

iv. de la règlementation sur la bioéthique. *« Encadrer les progrès de la science et de la médecine pour en éviter les dérives : tel est l'objectif des lois de bioéthique. Pionnière en la matière, la France se dote d'un cadre législatif dès 1994 »*[750] puis modifié récemment en 2021[751]. Cette Loi particulièrement intéressante pour la e-santé prévoit un encadrement plus élaboré de l'intelligence artificielle ou encore rappelle les interdictions sur certains domaines

[746] C. santé publ., art. L1111-8.
[747] 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 90/385/CEE et 93/42/CEE du Conseil, JOUE, L 117, 5 mai 2017.
[748] 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 90/385/CEE et 93/42/CEE du Conseil, JOUE, L 117, 5 mai 2017, art2. *« Tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes : diagnostic, prévention, contrôle, prédiction, pronostic, traitement ou atténuation d'une maladie ; diagnostic, contrôle, traitement, atténuation d'une blessure ou d'un handicap ou compensation de ceux-ci ; investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique ; communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain, y compris les dons d'organes, de sang et de tissus, et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens.*
Les produits ci-après sont également réputés être des dispositifs médicaux : les dispositifs destinés à la maîtrise de la conception ou à l'assistance à celle-ci ; les produits spécifiquement destinés au nettoyage, à la désinfection ou à la stérilisation des dispositifs visés à l'article 1er, paragraphe 4, et de ceux visés au premier alinéa du présent point ».
[749] Marie BASTIAN, « e-Santé : où est le droit ? », *SIH Solutions*, 2019.
[750] Ministère de la santé et de la prévention, « Bioéthique », 2019. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 10/08/2022).
[751] Loi n°2021-1017 du 2 août 2021 relative à la bioéthique (1), JORF n°0178, 3 août 2021, texte n°1.

de recherches comme le clonage humain, qui pourrait pour autant être réalisé avec les évolutions technologiques.

v. ou encore les Droits des patients appliqués à la e-santé, qui seront développés dans le titre 2 de la seconde partie.

294. **Un encadrement suffisant ?** La multitude de règles de Droit applicables à la e-santé permet globalement un bon encadrement. Pour autant est-ce suffisant ? *« Le décalage entre la lenteur des institutions et l'évolution exponentielle de la société de l'information prouve que le droit n'est pas, en l'état actuel, totalement armé pour ces nouveaux défis. Certes, les textes existent, en France et en Europe, mais ils ne sont pas suffisamment efficients parce qu'ils sont très souvent sous-appliqués »*[752].

Pour autant, le Droit est en constante évolution ou création afin de pallier les avancées technologiques, comme la proposition de Règlement du Parlement Européen et du Conseil sur l'intelligence artificielle : AI Act[753]. En effet, l'utilisation de plus en plus fréquente de l'intelligence artificielle implique une règlementation particulière en la matière, au regard des possibilités infinies que permet l'intelligence artificielle comme la notation sociale qui est réalisée en Chine et qui présente donc des risques de dérive inacceptables.

L'évolution très rapide de la e-santé et les possibilités infinies qu'elle présente nécessite une vigilance accrue et une rapide réactivité pour adapter ou créer le Droit, en réponse à ces innovations. « *Ainsi, si les nouvelles technologies permettent des avancées considérables dans le domaine de la santé, le patient doit rester au cœur des préoccupations juridiques et sa protection doit rester la priorité »*[754].

295. **Des garde-fous techniques au service du Droit.** Mais modifications ou créations de nouvelles dispositions du Droit ne sont pas les seules réponses ; la technologie en elle-même en est une. En effet, ce n'est pas parce que la technologie permet certaines choses que le Droit doit s'adapter pour répondre aux nouveaux enjeux. Prenons l'exemple du secret professionnel : par principe, toute personne prise en charge *« a droit au respect de sa vie privée et du secret des informations la concernant »*[755]. A ce titre, *« la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par*

[752] Marie BASTIAN, « e-Santé : où est le droit ? », *op. cit.*
[753] Regulation of the european parliament and of the council - Laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, 21 avril 2021.
[754] Sami EL AIBA et Perrine MAILLET, « Le droit de la santé à l'heure des nouvelles technologies », *Affiches parisiennes*, 2022.
[755] C. santé publ., art. L. 1110-4.

profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende »[756] ce qui est le cas d'un professionnel de santé qui communique des informations concernant l'état de santé de son patient par exemple. Des exceptions à ce secret sont prévues par les textes, notamment le partage et l'échange d'informations pour la prise en charge d'un même patient[757]. Ces échanges et partages sont facilités par la e-santé, qui permet d'ouvrir les accès aux outils très rapidement et à grande échelle. Or si l'ouverture des droits pour certaines personnes est possible, la restriction l'est également grâce à une grille d'habilitation ainsi qu'une traçabilité permettant d'avoir une meilleure visibilité sur d'éventuelles transgressions. Dans ce cas, la technologie vient en support du Droit et permet de mettre des protections techniques au service du juridique.

296. **La e-santé, pas qu'une question de santé.** *« Les réflexions relatives aux usages de la e-Santé et aux conséquences de leur évolution sur la pratique médicale et la santé des populations ne sauraient se faire exclusivement entre « spécialistes », à savoir entre professionnels de santé et informaticiens. Il convient désormais de mobiliser les disciplines relevant des sciences humaines, sociales et juridiques afin d'aborder les enjeux éthiques du développement de la e-Santé et d'interroger ses usages. Les évolutions scientifiques et techniques dans ce domaine sont en effet susceptibles de modifier profondément les représentations des individus quant à l'acte de soin, à leur propre santé et, de manière générale, la manière de penser la santé dans nos sociétés »*[758]. Aussi, la e-santé, n'est pas qu'une question de santé ; elle doit prendre en compte également le volet éthique, social, juridique notamment, pour ne pas déshumaniser la santé afin d'adapter notre système de santé en fonction des évolutions technologiques.

[756] C. pén., art. 226-13.
[757] Le secret professionnel ainsi que l'échange et le partage d'informations seront traités au sein du titre 2 de la partie 2.
[758] Marie BASTIAN, « e-Santé : où est le droit ? », *op. cit.*

Conclusion du chapitre. La e-santé est une réelle innovation notamment grâce à la dématérialisation de la prise en charge du patient. Les outils, services, ou encore activités entrant dans ce champ sont en constante évolution et se développent très rapidement. En quelques chiffres : selon le cabinet Grost & Sullivan, l'estimation de la valeur du marché mondial en santé numérique en 2023 s'élève à 234,5 milliards de dollars, « *soit une hausse de près de 160% par rapport à 2019. Cette croissance s'explique essentiellement par les besoins liés au vieillissement de la population et à la forte augmentation des maladies chroniques, ainsi qu'au développement massif de l'informatique en santé, des technologies d'analyse de données et d'IA et de la prise en charge d'actes réalisés à distance avec la télémédecine et les objets connectés »*[759]. En France, *« selon une étude de l'Institut Montaigne, associant le cabinet McKinsley*[760]*, le déploiement de l'e-santé permettrait de générer jusqu'à 22 milliards d'euros par an mais aussi de dessiner le système de santé de demain »*[761]. Ces chiffres montrent l'évolution exponentielle de la e-santé en seulement quelques années. Or la multitude de ces outils, bien qu'en grande partie bénéfiques pour la prise en charge du patient présente quelques risques puisque leur fiabilité peut être remise en cause. Pour autant, les Français semblent, dans l'ensemble satisfait par l'utilisation de la e-santé dans leur prise en charge. Selon un sondage disponible sur le site de l'ANS, « *86% des français se disent favorables au développement de la e-santé, 71% des français disent avoir déjà eu recours à des outils et services de la e-santé, 74% des français jugent que ces outils améliorent les parcours de soin à l'avenir »*[762]. Aussi, l'e-santé a encore quelques beaux jours devant elle.

[759] Olivier BABINET, Corinne ISNARD BAGNIS, *La e-santé en question(s), op. cit.*
[760] Institut Montaigne, « *e-santé : augmentons la dose ! »,* Rapport juin 2020, 2020.
[761] Big Média, « e-santé : un marché potentiel de 22 milliards d'euros », *bpi France,* 2021.
[762] ANS, *Ce que la e-santé fait pour vous, op. cit.*

Chapitre 2 : Aux supports nécessaires au suivi du patient

297. **La dématérialisation : un indispensable**. La dématérialisation implique une modification de la prise en charge du patient pour inclure presque systématiquement l'utilisation des technologies de l'information de la communication, que ce soit pour la réalisation ou l'aide à la réalisation d'un acte médical, pour le suivi du patient à l'instant *t* à la suite d'une pathologie particulière ou le suivi de l'état général du patient. La dématérialisation est aujourd'hui devenue indispensable pour la prise en charge du patient en santé, que cette dernière soit voulue ou subie par les professionnels de santé et les patients.

298. **Les supports de la prise en charge**. La dématérialisation se retrouve à tous les stades de la prise en charge du patient, notamment lors de la rédaction des supports documentaires nécessaires à cette dernière.

Les supports écrits sont au cœur de la prise en charge du patient pour plusieurs raisons :

i. Une obligation de Droit : il est prévu par les textes que certains supports écrits soient produits lors d'une prise en charge. L'ensemble de documents le plus connu est le dossier patient qui doit être « *constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé »*[763]. Est énumérée une liste de documents, à insérer dans ce dossier, et qui doivent obligatoirement être produits par écrit, tels que les comptes-rendus opératoires, la liste des soins reçus, les motifs d'hospitalisation etc.

ii. Un besoin métier et pratique : dans le cadre d'une prise en charge patient, le professionnel de santé peut être amené à écrire des notes dites personnelles. Ces notes personnelles sont des données ou les pensées d'un professionnel qui 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 ».*[764] Or certaines notes, dites « personnelles », ont servi dans le cadre de la prise en charge médicale du patient[765]. Ces notes, bien que non obligatoires, sont rédigées sur support papier comme

[763] C. santé publ., art. R. 1112-2.
[764] Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques de l'ANAES (HAS aujourd'hui) relatives à l'accès aux informations concernant la santé d'une personne, JORF n°65, 17 mars 2004, texte n°16.
[765] François VIALLA, « Existe-t-il des notes personnelles ? Points de vue divergents », *RDS*, 2005, n°2, pp. 201-207. A la lecture des textes, il apparaît que *« la question ne soit pas à être abordée sous un angle formel mais fonctionnel. C'est la destination et l'utilité de l'information recueillie par le praticien qui importe et non le mode de formalisation. Il en découle que les notes n'ayant pas contribué à l'élaboration et au suivi du diagnostic et du*

« pense-bête » pour les professionnels, ce qui fait couler beaucoup d'encre puisqu'encore aujourd'hui, la doctrine a des avis divergents quant à l'obligation ou non de communiquer ces éléments au patient[766].

iii. Une nécessité pour le suivi du patient : des éléments peuvent être consignés dans le dossier du patient pour son suivi sans pour autant que cela soit une obligation légale. Il peut s'agir par exemple pour une sage-femme, de consigner le numéro de chaque implant contraceptif implanté à chacune de ses patientes ainsi que la date à laquelle il a été posé, afin d'être vigilante quant à la date à laquelle il doit être retiré ou encore faire une surveillance en cas de lot défectueux et informer le cas échéant, les patientes concernées.

vi. Une question de preuve : certains documents sont produits en support écrit alors même que cela n'est pas obligatoire. Pour autant, la pratique veut qu'un écrit soit produit, pour des besoins métiers certes, mais également pour une question de preuve. A titre d'exemple, le consentement. La pratique de la santé est basée sur le respect du consentement du patient. Le consentement patient est un des principes socles de sa prise en charge ; l'absence de consentement peut entraîner pour le professionnel qui a failli à ce devoir, des sanctions, notamment pénales. En cas de contentieux, c'est au professionnel d'apporter la preuve que le consentement a bien été recueilli ; de ce fait, la pratique veut qu'un consentement écrit soit établi afin que ce dernier puisse servir de preuve par tout moyen, alors même que le Droit ne fait pas mention d'un consentement écrit, mais d'un simple consentement.

299. **Les supports de la prise en charge dématérialisés.** C'est indéniable, les supports écrits sont nécessaires pour la prise en charge du patient. Avec la dématérialisation de la santé dans son ensemble, ces supports, qui sont un moyen nécessaire à la prise en charge du patient, doivent également être dématérialisés (section 1), notamment le dossier patient (section 2) qui présente un enjeu majeur dans la dématérialisation complète de notre système de santé.

---

traitement ou d'une action de prévention n'ont pas vocation à la communication. A l'inverse, celles ayant contribué à un tel travail diagnostic doivent figurer au nombre des informations formalisées faisant l'objet de la communication au patient qui en fait la demande ».

[766] A titre d'exemples : 1. le Décret n°2012-694 du 7 mai 2012 portant modification du code de déontologie médicale vient modifier l'article R. 4127-45 du Code de la santé publique prévoyant expressément que « les notes personnelles du médecin ne sont ni transmissibles, ni accessibles au patient at aux tiers ». Cependant Caroline ZORN-MACREZ fait état de la difficile application de cet article au regard des dispositions de droit venant à son encontre, à l'instar de l'article L. 1111-7 reconnaissant le droit pour le patient d'être informé de son état de santé. (ZORN-MACREZ Caroline, Les « notes personnelles » du médecin ? : les conséquences d'un décret d'arrière-garde, *RDS*, 2012, n° 49) 2. Nora BOUGHRIET et Johanne SAISON-DEMARS estiment que les notes personnelles doivent être transmisses, y compris, lorsqu'elles n'ont pas servi à la prise en charge médicale (Nora BOUGHRIET, Jeanne SAISON-DEMARS, Les notes personnelles des médecins : un point d'incertitude dans la détermination du contenu transmissible du dossier, RGDM, 2014, n°53, p. 44).

Section 1 : Les documents médicaux 100% dématérialisés : possibles, nécessaires et souhaités

300. **La dématérialisation : d'une simple possibilité à une obligation.** Les documents produits lors d'une prise en charge sont nombreux et de toute sorte : documents formalisés (compte-rendu), prise de notes libres (au sein d'un dossier patient), radiographies, ECG etc. Tous ces supports peuvent être produits de manière dématérialisée, soit directement de manière numérique, soit en réalisant une copie numérique d'un support physique (voir partie 1).

Aujourd'hui, notre système de santé tout entier tend vers le numérique avec l'utilisation de plus en plus prépondérante de la e-santé mais également avec la volonté gouvernementale de développer le numérique en santé ce qui est clairement établi par la feuille de route : « accélérer le virage numérique en santé » de Ma Santé 2022.

Aussi, les supports contenant les données de santé doivent être également dématérialisés pour suivre l'évolution de notre système de santé. Pour autant, cette transformation se fait par étape, puisque certains documents n'ont pas l'obligation d'être dématérialisés et continuent à être produits en papier (§1), tandis que d'autres le sont déjà (§2).

§1 De la simple possibilité de dématérialiser

301. **Le support papier contenant des données de santé : toujours possible**. En santé, la dématérialisation des documents contenant des données de santé n'est pas toujours une obligation pour les professionnels. Certains professionnels continuent de rédiger leurs documents à la main même si des solutions permettant la dématérialisation existent ; il peut s'agir de leur dossier de suivi patient ou encore leur prescription. Même dans de gros centres hospitaliers, certains dossiers patients sont encore rédigés en format papier[767].

302. **Vers une obligation progressive**. Pour autant, même si tous les documents ne doivent pas être dématérialisés, on tend petit à petit vers une obligation générale de dématérialisation, celle-ci se faisant étape par étape ; bien que certains réfractaires vont jusqu'à ne pas se conformer au Droit, soit par choix, soit par impossibilité.

La prescription dématérialisée, ou la e-prescription en est un exemple (A) ; la prescription ne fait pas systématiquement l'objet d'une obligation de dématérialisation pour l'instant, pour

[767] Atlas des SIH 2020, « Etat des lieux des systèmes d'information hospitaliers », 2021.

autant, la e-prescription par rapport à la prescription papier présente des avantages non négligeables améliorant grandement la prise en charge du patient (B).

A) L'exemple de la e-prescription

303. **La e-prescription : contour de la notion.** La e-prescription, ou prescription électronique a été introduite par l'Ordonnance du 18 novembre 2020 portant sur la mise en œuvre de la prescription électronique pris en application de l'article 55 de la Loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé. Cette Ordonnance « *pose le principe de la dématérialisation des ordonnances de soins, de produits de santé et de prestations établies par les professionnels de santé exerçant en ville et leur transmission à l'assurance maladie par voie électronique* »[768].

La e-prescription est donc la dématérialisation du circuit de l'ordonnance de manière native. Est donc exclue la dématérialisation de la prescription par le simple fait de transformer une prescription papier en copie numérique.

La e-prescription est un des enjeux majeurs de la stratégie Ma Santé 2022. Elle fait partie d'un des quatre services socles permettant d'« *échanger et partager les données de santé en toute confiance* »[769]. Ces quatre services numériques socles sont : le DMP, la messagerie sécurisée de santé, les services numériques territoriaux de coordinations de parcours et la e-prescription. Chacun de ces services a pour but de développer, favoriser et entériner l'utilisation du numérique en santé.

304. **L'adhésion des professionnels de santé au projet.** Actuellement, l'utilisation de la e-prescription pour les professionnels de santé n'est pas une obligation[770], bien qu'elle le devienne à terme, notamment pour les professionnels libéraux. Cependant, un projet d'une telle envergure, engendrant un bouleversement des pratiques des professionnels au vu du nombre de prescriptions réalisées par jour, nécessite leur adhésion pleine et entière afin qu'une dématérialisation totale des prescriptions puisse être réalisée. C'est pourquoi, « *afin d'assurer l'adhésion des Professionnels de Santé, l'e-prescription doit s'inscrire dans leur processus métier, ce qui nécessite un travail d'intégration dans les offres logicielles des*

[768] Vie publique, « Ordonnance du 18 novembre 2020 portant mise en œuvre de la prescription électronique », 2020.
[769] ANS, *Feuille de route « accélérer le virage numérique en santé*, 2020. Disponible à l'adresse : http://esante.gouv.fr/ (consulté le 23/08/2022).
[770] Excepté dans certains cas déjà définis par la Loi. Voir §2 « à l'obligation de dématérialiser ».

prescripteurs et des prescrits »[771] notamment pour que les professionnels ne voient que des bénéfices à la e-prescription et non pas une perte de temps ou de fiabilité.

De ce fait et « *à l'instar des nombreuses évolutions apportées dans le cadre de Ma Santé 2022, le déploiement de la e-prescription se fera étape par étape. Ce calendrier progressif a pour but d'expérimenter sur le terrain chaque type d'ordonnance, sur des échantillons restreints. Ainsi, les représentants des professionnels de santé concernés ont l'opportunité d'appréhender l'outil et de récolter les retours d'expérience du terrain avant de donner l'aval à une généralisation nationa*le »[772].

305. **Etape par étape : 1. La e-prescription médicamenteuse.** Le projet de dématérialisation des prescriptions en France date de plus de 10 ans et se fait étape par étape. « *La Cnam[773] a d'abord expérimenté, entre octobre 2017 et avril 2019, un dispositif de dématérialisation limité à la simple impression d'un QR code sur l'ordonnance papier* »[774] . Puis, à partir de juillet 2019, une expérimentation a été mise en place afin de tester la e-dématérialisation dans trois départements : le Maine-et-Loire, la Saône-et-Loire et le Val-de-Marne. A la suite de son succès, il a été décidé de généraliser la e-prescription médicamenteuse pour tous les prescripteurs, ce qui permet d'ouvrir la voie à la e-prescription à d'autres domaines.

Dans le cadre de l'expérimentation de la e-prescription médicamenteuse, cette dernière « *consiste à dématérialiser le circuit de l'ordonnance entre les médecins et les pharmaciens. Elle s'appuie sur une base de données sécurisée, hébergée par l'Assurance Maladie. Son accès est restreint aux professionnels de santé médecins et pharmaciens par l'intermédiaire d'une carte CPS. En officine, la consultation d'une e-prescription est aussi possible avec une carte CPE de préparateur. Dans un premier temps, l'ordonnance papier est conservée, elle est remise au patient. Toutes les données échangées entre le médecin et le pharmacien, sont structurées et codifiées à partir des référentiels (bases de médicaments). Le pharmacien peut notamment indiquer, dans les données structurées de dispensation, qu'il a été amené à adapter la prescription d'un médicament en fonction d'informations dont il dispose (interactions médicamenteuses, posologie…). Le patient pourra accéder à sa prescription dématérialisée via son DMP alimenté par le médecin via son logiciel métier. Le périmètre de*

[771] Catherine MORVAN SIGWARD et Alain PERIE, « e-prescription », *G.NUIS*, 2020.
[772] Mon ordo, « la e-prescription c'est quoi ? ». Disponible à l'adresse : https://www.monordo.com/ (consulté le 15/07/2022).
[773] Caisse nationale de l'assurance maladie.
[774] Cour des comptes, « *La dématérialisation des prescriptions médicales : un facteur d'efficience du système de santé, des chantiers ambitieux à faire aboutir* », Rapport, 2021.

cette expérimentation couvre toutes les prescriptions réalisées en ville. Les services de e-prescription sont intégrés dans les logiciels professionnels des médecins et des pharmaciens. Ils facilitent la tâche des professionnels de santé et évitent de la ressaisie »[775].

306. **Vers une obligation de la e-prescription ?** Bien que la e-prescription ne soit pas aujourd'hui une obligation, l'Ordonnance du 18 novembre 2020 prévoit une généralisation de la e-prescription au plus tard au 31 décembre 2024[776]. A cette date, les professionnels de santé prescripteurs devront établir et transmettre de manière dématérialisée et par l'intermédiaire de téléservices mis à disposition par la Cnam, « *les prescriptions de soins, produits ou prestations* »[777]. Les professionnels de santé exécutant ces prescriptions devront quant à eux transmettre par téléservices *« les données relatives à leurs modalités d'exécution »*[778].

Mais cette obligation de faire des e-prescriptions ne concerne pas tous les professionnels de santé. En effet, sont exclues les « *prescriptions qui sont à la fois établies et exécutées au sein des établissements de santé* »[779]. Les établissements de santé ne sont donc pas soumis à cette obligation, ce qui fait débat quant à l'égalité entre les établissements de santé et les professionnels libéraux. Cependant, toutes les prescriptions ne sont pas concernées par cette exception, « *les prescriptions effectuées en établissement, mais exécutées en ville auprès de pharmaciens d'officine, de laboratoires d'analyses biologiques et d'auxiliaires médicaux sont soumises à l'obligation posée par l'ordonnance du 18 novembre 2020. Toutefois, le précédent du recours quasi-inexistant des établissements de santé au service de e-prescription des transports de patients proposé par l'assurance maladie […] laisse augurer une difficulté certaine de participation de ces derniers à la généralisation de la e-prescription pour les soins de ville* »[780].

Outre cette exception des établissements de santé, un décret en Conseil d'Etat doit venir définir les cas dans lesquels la e-prescription pourra ne pas être appliquée comme « *l'absence d'environnement informatique adéquat ou de connexion internet suffisante* »[781] ou encore

---

[775] ANS, *e-prescription,* Doctrine technique du numérique en santé soumise à concertation, version novembre 2020.
[776] Ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique, JORF n°0280, 19 novembre 2020, texte n°46.
[777] Ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique, JORF n°0280, 19 novembre 2020, texte n°46, art 1.
[778] *Ibid.*
[779] *Ibid.*
[780] Cour des comptes, « *La dématérialisation des prescriptions médicales : un facteur d'efficience du système de santé, des chantiers ambitieux à faire aboutir* », *op. cit.*
[781] Ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique, JORF

« *les modalités selon lesquelles la mise en œuvre de la prescription électronique donne lieu à la remise au patient d'une ordonnance papier* »[782].

La prescription est donc encore aujourd'hui réalisée sous format papier, bien qu'elle tende peu à peu à se généraliser en e-prescription pour devenir finalement la seule manière de prescrire[783]. Pour autant, les exceptions à l'utilisations de la e-prescription n'étant pas encore définies, il est difficile d'imaginer la portée de ces exceptions, même si l'on peut imaginer que « l'absence d'environnement informatique adéquat » puisse être une faille à la généralisation de la e-prescription dans laquelle les professionnels pourront s'engouffrer. La prescription papier restera encore pour quelques années un standard.

B) Les bienfaits de la dématérialisation

307. **Objectifs et enjeux de la e-prescription**. La e-prescription par rapport à une prescription papier ou une prescription copie numérique, présente des avantages que seule la e-prescription peut fournir. C'est l'utilisation des technologies de l'information et de la communication qui permet à la e-prescription d'apporter d'autres effets que la « seule » prescription de soins, de produits ou de prestations. Cinq avantages à la dématérialisation de la e-prescription, peuvent être dénombrés :

i. La sécurisation des ordonnances notamment une baisse des fraudes : grâce à la e-prescription, le circuit complet de la prescription à la dispensation est simplifié mais également sécurisé. « *En effet, en certifiant numériquement les identités et en sauvegardant les données de prescription, un système informatique permet de tracer ces dernières et d'assurer ainsi l'unicité de l'ordonnance. Ici, il s'agit tout simplement de la fin des falsifications d'ordonnance* »[784]. L'authentification des prescripteurs et des exécutants permet d'identifier de manière certaine les personnes impliquées, s'assurant ainsi qu'aucune ordonnance ne pourra être réalisée par une personne non habilitée. Cette authentification couplée à la traçabilité sécurise d'un bout à l'autre le circuit de la prescription.

ii. Une meilleure prise en charge et une qualité des soins augmentée : d'une part, la e-prescription permet de pallier les inconvénients d'une prescription papier ; les prescriptions ne

n°0280, 19 novembre 2020, texte n°46, art 1.
[782] *Ibid.*
[783] Eric LE QUELLENEC, « Généralisation de l'e-prescription avec l'ordonnance du 18 novembre 2020 », *Lexing*, 2019.
[784] Mon ordo, « la e-prescription c'est quoi ? ». Disponible à l'adresse : https://www.monordo.com/ (consulté le 15/07/2022).

risquent plus d'être perdues ou endommagées, nécessitant de redemander une nouvelle ordonnance, favorisant leur falsification le cas échéant ; les difficultés de lecture d'une ordonnance manuscrite disparaissent également, diminuant les risques d'erreurs de médication. D'autre part, la e-prescription permet de « *rendre plus fluide et plus fiable les échanges entre professionnels de santé, au même titre que la transmission des informations à l'assurance maladie. In fine, la coordination des soins doit se voir renforcée par l'utilisation d'ordonnances unifiées et électroniques* »[785] qui alimenteront directement le DMP et le DP[786] (sauf opposition du patient) et ainsi « *favorisera la cohérence du parcours de soins et la réduction des risques de iatrogénie*[787]*, par la prévention et la détection de certaines incompatibilités de prescription (interactions médicamenteuses, allergies, etc.)* »[788]. Pour terminer, les logiciels d'aide à la prescription permettant la e-prescription sont dotés d'un module d'aide à la prescription pour le professionnel prescripteur qui « *contribue à renforcer la pertinence des soins et à lutter contre l'iatrogénie* »[789], grâce à « *la lecture intelligente des ordonnances* [qui] *permet* […] *en identifiant, dès l'édition de la prescription* […] *les interactions médicamenteuses* »[790].

iii. Un outil pour le patient : la e-prescription a un fort potentiel pour les patients et pour leur suivi médical. Ils peuvent accéder à leur prescription *via* leur DMP et pourront à terme, bénéficier de services liés à cette e-prescription comme la création d'un pilulier électronique ou encore des rappels automatiques pour que le patient aille renouveler son ordonnance arrivant à terme. La e-prescription ne bénéficie donc pas qu'aux professionnels ou à l'assurance maladie.

iv. La e-prescription : un trésor de données. La dématérialisation des données issues des prescriptions permet de faire avancer la recherche dans une dimension à grande échelle. La compilation des données pourra permettre de réaliser de nombreuses études, qu'elles soient épidémiologiques ou encore, sur les pratiques de prescription.

---

[785] Mon ordo, « la e-prescription c'est quoi ? ». Disponible à l'adresse : https://www.monordo.com/ (consulté le 15/07/2022).
[786] Le Dossier Pharmaceutique.
[787] Ministère de la santé et de la prévention, « iatrogénie », *Glossaire*, 2016. La iatrogénie est l'« ensemble des conséquences néfastes pour la santé, potentielles ou avérées, résultant de l'intervention médicale (erreurs de diagnostic, prévention ou prescription inadaptée, complications d'un acte thérapeutique) ou de recours aux soins ou de l'utilisation d'un produit de santé ».
[788] Cour des comptes, « *La dématérialisation des prescriptions médicales : un facteur d'efficience du système de santé, des chantiers ambitieux à faire aboutir* », *op. cit.*
[789] ANS, *e-prescription*, Doctrine technique du numérique en santé soumise à concertation, *op. cit.*
[790] Mon ordo, « la e-prescription c'est quoi ? ». Disponible à l'adresse : https://www.monordo.com/ (consulté le 15/07/2022).

v. La réduction des dépenses. L'utilisation obligatoire d'un logiciel d'aide à la prescription[791] permet de réaliser les prescriptions selon une dénomination commune et non plus avec le nom de marque d'un médicament. « *Malgré sa relative ancienneté (depuis 2009 pour les médicaments génériques et 2015 pour les princeps), l'obligation de prescription en DC est souvent inappliquée. La prescription dématérialisée de médicaments pourrait favoriser une prescription accrue de médicaments génériques, alors que le développement de l'usage des génériques en France est moindre que dans d'autres pays européens (une boîte délivrée sur trois contre quatre sur cinq au Royaume-Uni) et qu'il repose principalement sur la substitution par le pharmacien du médicament princeps prescrit par le médecin* »[792]. L'utilisation plus forte des génériques permettra de réduire les dépenses. La e-prescription, grâce au recueil de données, permettra certes la recherche, mais également l'exploitation des données par l'assurance maladie notamment quant aux durées de traitement et de posologie afin « *d'affiner les actions de maîtrise médicalisée des dépenses* » [793].

308. **Un retard de la France**. Les bienfaits de la e-prescription par rapport à la prescription manuscrite sont nombreux ; celle-ci présente un fort potentiel pour l'évolution du système de santé français. Pourtant, même si la France est un des pays les plus avancés sur l'optimisation de son système de santé, la cour des comptes dans son rapport annuel sur l'application des lois de financement de la sécurité sociale tire la sonnette d'alarme et précise que la France a un retard important à combler en la matière. La France est en retard de 5 à 10 ans par rapport aux pays voisins sur la e-prescription.

« *Plusieurs pays européens ont déployé avec succès des solutions de dématérialisation des prescriptions de médicaments, dès les années 2000 en Suède, au début des années 2010 au Royaume-Uni, en Norvège […] et à partir de 2015 en Espagne et en Italie. L'Allemagne est moins avancée : introduit en 2020, le dispositif de dématérialisation serait opérationnel en juillet 2021 ; il sera obligatoire en janvier 2022* »[794]. Un exemple concret : les professionnels de santé (médecin, sage-femme et dentiste) belges ont l'obligation d'utiliser la e-prescription pour la prescription médicamenteuse des patients en ambulatoire depuis le 1er janvier 2020. Pour autant, certaines exceptions sont prévues à cette obligation telles que la prescription

[791] Mathias BEJEAN, Frédéric KLETZ et Jean-Claude MOISDON, « Création de valeur organisationnelle et technologies de l'information à l'hôpital : le cas du dossier patient informatisé », *op. cit.* Certains auteurs semblent mitiger quant aux bienfaits de ces logiciels d'aide à la prescription ; ils parlent de « *phénomènes de désapprentissage, les jeunes médecins accordant trop de crédit aux logiciels d'aide à la prescription* ».
[792] Cour des comptes, « *La dématérialisation des prescriptions médicales : un facteur d'efficience du système de santé, des chantiers ambitieux à faire aboutir* », *op. cit.*
[793] *Ibid.*
[794] *Ibid.*

rédigée en dehors du cabinet médical du professionnel, en cas de force majeure ou si le professionnels atteint l'âge de 64 ans au 1er janvier 2020[795]. Bien que la e-prescription médicamenteuse soit généralisée, elle n'est pour autant pas imposée au citoyen belge. La e-prescription est « *un droit et non une obligation pour le citoyen* »[796]. Si le citoyen belge souhaite avoir une copie papier de sa prescription, il peut tout à fait la demander au prescripteur.

Il faudra attendre fin 2024 pour la généralisation de la e-prescription en France, tout en gardant à l'esprit que le chemin sera encore long, afin de réellement faire adhérer tous les professionnels, y compris les établissements de santé dans leurs rapports avec la ville, et de ne pas faire, des exceptions à la e-prescription, la norme.

§2 A l'obligation de dématérialiser

309. **Des données de santé obligatoirement dématérialisées.** Même si tous les documents en santé n'ont pas l'obligation, ou pas encore, d'être dématérialisés, certains documents le sont déjà. Cette obligation est soit une obligation imposée par le Droit (A), soit par la pratique (B), rendant incontournable, la dématérialisation des documents de santé.

A) L'obligation imposée par le Droit

310. **La dématérialisation imposée par le Droit**. La dématérialisation n'est qu'un moyen de parvenir à un résultat, en l'espèce, créer ou transformer un support initialement papier, en un support dématérialisé. En santé, la dématérialisation est de plus en plus présente et utilisée. Cette utilisation peut même être imposée par le Droit, ne laissant pas d'autres choix aux professionnels de santé, que de dématérialiser certains documents. Cette dématérialisation des documents est soit native numérique, ou peut parfois être une simple copie numérique.

311. **Les télédéclarations**. En France, certaines maladies font l'objet d'une déclaration obligatoire[797]. Actuellement, elles sont au nombre de trente-six, parmi lesquelles trente-quatre sont des maladies infectieuses et deux, sont non infectieuses. On y retrouve par exemple le chikungunya, le choléra, la fièvre jaune, ou encore la rage. La liste des maladies nécessitant une déclaration obligatoire est définie par décret[798]. Presque la totalité des

[795] INAMI, « Obligation de prescrire les médicaments de façon électronique », *Thème*, 2022.
[796] PETRA, « La prescription « dématérialisée » : un droit et non une obligation pour le citoyen », *recip-e,* 2021.
[797] C. santé publ., art. L. 3113-1.
[798] Décret n° 2021-573 du 10 mai 2021 complétant la liste des maladies faisant l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire, JORF n°0110, 12 mai 2021, texte n°22.

déclarations doivent avoir lieu *via* un formulaire papier que l'on peut retrouver sur le site Santé publique France[799] sauf pour l'infection par le VIH qui doit être réalisée *via* le service de déclaration en ligne e-do[800].

En effet, depuis 2015, l'Agence Nationale de Santé Publique (ou Santé publique France) a le projet de dématérialiser le processus de déclaration des maladies faisant l'objet d'une déclaration obligatoire « *afin de renforcer la qualité de la surveillance épidémiologique et des capacités d'alerte »*[801]. A ce titre, l'application e-do a été développée, et l'infection du VIH a été choisie comme première maladie devant obligatoirement faire l'objet d'une e-déclaration, dans un premier temps auprès d'établissements volontaires puis le service e-do s'est généralisé sur tout le territoire depuis le 18 avril 2016[802]. Aussi les déclarants, cliniciens et biologistes, ont depuis 2016, l'obligation de déclarer une infection par VIH *via* le service e-Do[803] et n'ont plus la possibilité d'utiliser un formulaire papier. Cette déclaration est nativement dématérialisée puisque la déclaration se fait directement en ligne en se connectant au service e-Do exclusivement avec une carte de type CPS permettant une authentification forte des professionnels déclarants. Il n'est donc pas possible de rédiger un formulaire papier et le transmettre de manière dématérialisée.

Aujourd'hui, la tuberculose peut également faire l'objet d'une déclaration *via* e-Do, même si une déclaration papier reste possible. L'objectif final est de dématérialiser complètement les déclarations obligatoires afin de « *moderniser le processus de notification, de réduire les délais mais également de faciliter les échanges entre les différents acteurs de la déclaration obligatoire »*[804].

Comme vu en introduction, la télédéclaration n'est pas seulement obligatoire en santé, elle l'est également dans notre vie quotidienne ; à titre d'exemple, les citoyens français ont aujourd'hui l'obligation de déclarer leurs revenus en ligne, dès lors qu'ils sont équipés d'une

[799] Santé Publique France, *Liste des maladies à déclaration obligatoire,* 2003 (mis à jour en 2021).
[800] L'outil est disponible à l'adresse : www.e-do.fr
[801] Instruction N°DGS/SP2/DGOS/PF5/2016/112 du 4 juillet 2016 relative au déploiement de l'application e-DO pour la télé-déclaration de l'infection par le VIH/Sida.
[802] *Ibid.*
[803] Françoise CAZEIN, Didier CHE, D. DUBOIS, Julien DURAND, F. LOT, E. LUCAS, « e-DO : retour sur le déploiement en ligne pour l'affection par le VIH et le sida », *Revue d'Epidémiologie et de Santé Publique,* 2018. *« Depuis l'ouverture du dispositif en avril 2016, l'application e-DO est utilisée de manière croissante par les biologistes et les cliniciens. Durant l'année 2016, 1896 DO électronique (15,2 %) et 10 512 DO papier (84,7 %) ont été reçues. Pour 2017 (au 1er novembre), 5869 DO électroniques (60,9 %) et 3758 DO papier (39,1 %) ont été reçu. e-DO permet de réduire le délai entre la date de diagnostic et la date de réception des données à SpFrance à 33 jours (médiane), contre 104 auparavant. En novembre 2017, on compte 896 inscrits à e-DO [526 biologistes (61,8 %) et 325 cliniciens (38,2 %)] ».*
[804] *Ibid.*

connexion internet[805]. Petit à petit, on se rend compte que toute déclaration obligatoire, dans notre vie personnelle ou professionnelle doit être réalisée sous forme dématérialisée, notamment pour en faciliter le traitement.

312. **Une dématérialisation imposée cachée**. La dématérialisation des documents devient petit à petit de plus en plus présente dans le quotidien des professionnels de santé et devient même une obligation visible dans certains cas comme l'obligation de e-déclarer les infections par le VIH, mais également une obligation davantage cachée. Prenons l'exemple du DMP : l'article L.1111-15 du Code de la santé publique prévoit que chaque professionnel de santé doit mettre dans le dossier médical partagé « *à l'occasion de chaque acte ou consultation, les éléments de diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge* »[806] tels que le compte rendu des examens de biologie médicale ou encore les documents de sortie d'hospitalisation. Cette liste de documents obligatoires va s'étendre pour inclure, à compter du 31 décembre 2022, les comptes rendus des examens radio-diagnostiques par exemple et à partir du 31 décembre 2023, les demandes d'examens radiologique[807]. En soi, ces documents n'ont pas individuellement l'obligation d'être dématérialisés, mais comme ils doivent être versés au DMP qui, lui, est informatisé, cela oblige les professionnels à dématérialiser ces documents. Pour autant, rien n'impose une dématérialisation native de ces documents. Aussi, il apparaît possible d'alimenter le DMP avec des documents copies numériques. Avec la création automatique de l'espace numérique de santé de chaque personne et donc la création automatique du dossier médical partagé (sauf opposition)[808], les professionnels seront de plus en plus amenés à devoir dématérialiser, même s'ils ne le souhaitent pas.

B) L'obligation imposée par la pratique

313. **La pratique engendre la dématérialisation**. Outre l'obligation de dématérialisation des documents imposés par le Droit, la pratique des professionnels peut également engendrer inexorablement la dématérialisation des documents. Le cas le plus évident au regard des propos précédents est l'utilisation d'un dispositif de télémédecine ou d'un service permettant le suivi d'un patient par des professionnels libéraux (1). En revanche,

[805] C. gén. impôts, art. 1649 quater B quinquies.
[806] C. santé publ., art. L. 1111-15.
[807] La liste complète des documents est disponible : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045726627
[808] C. santé publ., art. L. 1111-14.

même si la dématérialisation n'est pas imposée, elle est tout de même encadrée juridiquement et la dématérialisation est réalisée de manière sécurisée. Ce qui n'est pas toujours le cas dans toutes les pratiques (2).

1) Une dématérialisation imposée par la pratique, sécurisée

314. **La télémédecine et la dématérialisation des supports**. Comme vu précédemment, la télémédecine permet la pratique médicale à distance *via* l'utilisation des TIC. Il est prévu que le professionnel de santé intervenant en télésanté doit inscrire dans le dossier du patient et dans le DMP cinq éléments :

« 1° Le compte rendu de la réalisation de l'acte de télémédecine ou de l'activité, et, le cas échéant, de la série d'activités, de télésoin ;

2° Les actes et les prescriptions effectués dans le cadre de l'acte de télémédecine ou de l'activité de télésoin ;

3° Son identité et éventuellement celles des autres professionnels participant à l'acte de télémédecine ou à l'activité de télésoin ;

4° La date et l'heure de l'acte de télémédecine ou de l'activité de télésoin ;

5° Le cas échéant, les incidents techniques survenus au cours de l'acte de télémédecine ou de l'activité de télésoin »[809].

Lors d'une téléconsultation par exemple, l'outil utilisé permet au professionnel de compléter directement les éléments de manière dématérialisée et en faire une extraction pour son dossier patient et un lien direct, le cas échéant, pour envoyer les éléments dans le DMP du patient[810]. L'utilisation d'un dispositif de télémédecine oblige le professionnel à dématérialiser les documents inhérents à la prise en charge du patient.

315. **La dématérialisation du suivi patient post prise en charge médicale**. Un autre exemple tout aussi flagrant est le suivi du patient par des professionnels libéraux à la suite d'une prise en charge médicale. Comme vu précédemment, les professionnels libéraux prenant en charge un même patient pour une pathologie particulière, peuvent, pour favoriser la coordination entre eux, utiliser des outils de télésanté tels que des outils de e-parcours[811].

[809] C. santé publ., art. R. 6316-4.
[810] Louis MALACHANE, « Pourquoi utiliser le Dossier Médical Partagé (DMP) ?, *Leah*, 2019.
[811] ANS, « e-parcours », *les projets de l'ANS,* disponible à l'adresse : https://esante.gouv.fr/ (consulté le 20/09/2022). Le e-parcours est *« la transformation numérique du parcours de santé de l'usager »*. C'est une des actions de la feuille de route du numérique en santé.

Ce dispositif permet aux professionnels de communiquer entre eux, de s'échanger des documents concernant un patient et de suivre l'état de santé global de ce patient lors de sa prise en charge pour une pathologie précise.

316. **Une dématérialisation sécurisée**. L'utilisation de ces outils de télémédecine ou de suivi patient n'est pas obligatoire, pour autant, elle implique nécessairement la dématérialisation des supports concernant la prise en charge du patient.

2) Une dématérialisation imposée par la pratique, non sécurisée

317. **Une dématérialisation non sécurisée**. Pour autant, la pratique veut également que les documents soient dématérialisés par nécessité, mais ne respecte pas les règles de droit en vigueur. Le cas le plus marquant et le plus flagrant est la nécessité de dématérialiser des documents au regard de la pandémie de COVID-19.

318. **Le cas du COVID-19**. « *Et si, à l'heure de la Covid-19, la santé prenait le pas sur la protection des données de santé ? »*.[812] La pandémie du COVID-19 a demandé au gouvernement et aux professionnels de santé de s'adapter très vite au contexte sanitaire et d'adapter la prise en charge des patients afin qu'elle soit réalisée dans les meilleures conditions possibles, notamment afin d'empêcher au maximum de nouvelles contaminations dans le monde entier. Une des mesures mises en place était le confinement des citoyens empêchant ou limitant ces derniers, de bénéficier d'une consultation physique chez un médecin par exemple. Pour cela, des solutions de téléconsultation ont été mises en place pour continuer à suivre les patients. Or, des problèmes techniques pouvaient intervenir, empêchant les professionnels de réaliser la consultation sur un canal sécurisé ou d'envoyer les prescriptions patient de manière sécurisée. La pratique a voulu que certains documents de santé transitent *via* des canaux non sécurisés tels que la messagerie personnelle des patients.

D'autres pays tels que le Luxembourg, ont mis en place des dispositifs : lors de la vague d'augmentation des cas positifs au COVID-19 d'octobre 2020, le Luxembourg a mis en place une adresse mail (saisieCIT.cns@secu.lu) afin de réceptionner exceptionnellement les certificats d'incapacité de travail pour optimiser leur temps de traitement et limiter les déplacements des travailleurs[813]. Pour autant, l'envoi des documents *via* les adresses mails des patients, n'est pas un envoi sécurisé. Seules les ordonnances d'isolement ou de quarantaine peuvent être envoyées à cette adresse mail, bien que l'envoi postal reste toujours possible.

[812] Stéphanie ABDESSELAM, Laetitia GAILLARD, Daniel KADAR, « Données de santé : un vecteur d'innovation sous trop haute surveillance ? », *RJSP*, juin 2021, n°21, p. 43.
[813] LSGB, « Coronavirus-News : Comment transmettre vos certificats de maladie », *Divers*, 2020.

Pour terminer, parlons de l'application TousAntiCovid[814] lancée par le Gouvernement le 22 octobre 2020, permettant notamment à toute personne d'y introduire son pass sanitaire et son pass vaccinal. Rappelons-le, ces pass étaient obligatoires pour accéder à certains lieux tels que les établissements de santé, certains lieux de divertissement (cinéma, théâtre), ou de restauration. La personne avait certes, le choix de montrer son pass en version papier, mais l'application permettait d'avoir un accès facilité à ce dernier. Or, n'est-il pas étonnant de ne voir aucune mesure d'identification et d'authentification associée à cette application à l'instar d'une application bancaire, alors même qu'elle contient des informations sur nos données de santé ? En effet, il est possible de savoir si la personne a été vaccinée, le nombre de dose, ou encore le type de vaccin. Ainsi, n'importe quelle personne ayant accès au téléphone peut ainsi connaître très aisément les données de santé du détenteur.

319. **Des entorses trop régulières**. Dans le cas d'espèce, la dématérialisation non sécurisée des documents a été rendue nécessaire pour faire face à une épidémie mondiale. Or, hors contexte d'urgence, il arrive encore que les professionnels dématérialisent des données de santé et les transmettent hors canal sécurisé, toujours en envoyant des documents sur une adresse mail non sécurisée, ou en envoyant des données par SMS à un confrère ou au patient lui-même. Cette pratique, facilitant certes les échanges, est contraire au droit actuel.

[814] Direction Générale de la Santé du ministère des solidarités et de la santé, « TousAntiCovid », disponible à l'adresse : https://bonjour.tousanticovid.gouv.fr/ (consulté le 30/09/2022). *« TousAntiCovid est une application pilotée par l'État pour aider à la lutte contre le Covid-19. Elle permet d'être alerté en cas de contact avec le Covid-19, d'être informé sur l'évolution de l'épidémie, de générer ses attestations de déplacement, de stocker ses certificats sanitaires et d'être averti en cas d'éligibilité au rappel vaccinal ».*

Section 2 : Vers un dossier patient unique

320. **Le dossier médical patient.** Lorsque l'on parle de documents nécessaires au suivi de la prise en charge du patient en établissement de santé, on pense évidemment à l'ensemble de documents le plus important : le dossier médical du patient.

« *Un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé »*[815] et contient un ensemble de documents nécessaires à la prise en charge du patient, dont la liste est décrite au sein de l'article R. 1112-2 du Code de la santé publique. On y retrouve les conclusions de l'évaluation clinique initiale, le dossier d'anesthésie, la lettre du médecin à l'origine de la consultation, ou encore le dossier de soins infirmiers. *« Le dossier du patient assure la traçabilité de toutes les actions effectuées. Il est un outil de communication, de coordination et d'information entre les acteurs de soins et avec les patients. Il permet de suivre et de comprendre le parcours hospitalier du patient. Il est un élément primordial de la qualité des soins en permettant leur continuité dans le cadre d'une prise en charge pluri-professionnelle et pluridisciplinaire »*[816]. Ce dossier est un indispensable, d'une part, parce qu'il est imposé par la Loi, d'autre part, parce que les professionnels doivent pouvoir bénéficier du suivi de la prise en charge du patient pour connaître ses antécédents, les soins déjà réalisés, les traitements prescrits etc. afin de prendre en charge le patient au mieux, avec les éléments qu'ils détiennent.

Ce dossier médical est donc l'outil indispensable pour les professionnels et est commun à tous les services d'un même établissement de santé, permettant à chaque professionnel de bénéficier de toutes les informations dont il a besoin[817].

Cependant, ce dossier regroupant toutes les informations médicales d'un patient, est réservé à un usage en établissement de santé et est cloisonné, impliquant que les autres professionnels de santé prenant en charge le patient ne bénéficient pas de toutes ces informations mais seulement des éléments de la lettre de sortie et/ou des prescriptions.

D'autres « dossiers » plus spécifiques existent à l'instar de ce dossier patient, pour continuer à optimiser et réaliser au mieux, la prise en charge de celui-ci (§1), mais ne serait-il pas

[815] C. santé publ., art. R. 1112-2.
[816] ANAES, *Dossier du patient : réglementation et recommandations,* 2003. Disponible sur https://has-santé.fr (consulté le 22/06/2021).
[817] Mathias BEJEAN, Frédéric KLETZ et Jean-Claude MOISDON, « Création de valeur organisationnelle et technologies de l'information à l'hôpital : le cas du dossier patient informatisé », *op. cit.*

souhaitable de tous les rassembler, pour n'en former qu'un : un dossier patient unique national ? (§2).

§1 L'émergence de dossiers spécifiques

321. **Des « dossiers » pour les professionnels libéraux**. Les professionnels libéraux ont également l'obligation, au même titre qu'un établissement de santé, de créer un dossier médical ou une fiche d'observation pour chacun de leurs patients[818]. Or ce dossier libéral, n'a pas autant de fonctions que celui de l'établissement de santé. En effet, tous deux sont nécessaires pour compiler toutes les informations concernant la santé du patient afin de les utiliser pour le prendre en charge. En revanche, une des différences est que le médecin libéral est seul à y avoir accès, tandis qu'en établissement de santé, le dossier est accessible par tous les professionnels prenant en charge le patient et est utilisé pour coordonner les soins de ce dernier grâce au partage d'informations.

322. **Une optimisation de la prise en charge du patient.** Cette fonction, absente du dossier médical du médecin libéral mais pour autant devenue essentielle pour l'optimisation de la prise en charge du patient, est un manque en ville. De ce fait, des projets de « dossiers » vont voir le jour que ce soit au niveau de certaines structures ou au niveau régional (A), ainsi que des projets nationaux (B), pour pallier ce manque. Ces projets vont permettre une meilleure coordination des soins pour un patient lors de la prise en charge ; bien plus, ils vont répondre aux besoins de certaines professions.

A) Des projets sectorisés

323. ***« L'émergence de nouveaux modes de prise en charge : des réponses nécessaires »[819].*** Depuis une dizaine d'année, la coordination des professionnels de santé prenant en charge une personne est au cœur des préoccupations. En effet, lors d'une prise en charge, de nombreux professionnels sont amenés à intervenir pour le patient, qu'il s'agisse de médecins, infirmiers, kinésithérapeutes, ou ostéopathes, exerçant en établissement de santé ou en ville. La multitude d'intervenants pour une même prise en charge nécessite une coordination accrue, et un échange et/ou un partage d'informations, afin que le patient puisse bénéficier de la meilleure prise en charge possible.

[818] C. santé publ., art. R. 4127-45.
[819] Caroline ZORN, *Données de santé et secret partagé – Pour un droit de la personne à la protection de ses données de santé partagées, op. cit.,* p-15.

Cependant, cette coordination implique l'utilisation d'outils permettant l'échange et le partage d'informations, outils qui doivent respecter le Droit applicable et qui sont principalement des outils numériques. En établissement de santé, il y a le dossier patient, informatisé ou non, mais il ne permet pas la coordination en dehors de l'établissement. Aussi, les professionnels ont besoin d'outils fiables et répondant à leurs besoins terrain, afin d'assurer une coordination entre eux, pour une prise en charge du patient optimale.

324. **Les GRADeS**. C'est une des missions des GRADeS. Comme vu précédemment, les GRADeS sont des structures régionales venant en appui des ARS pour décliner de manière opérationnelle, la stratégie nationale mais également régionale d'e-santé. Chaque GRADeS « *anime et fédère les acteurs de la région autour de la stratégie régionale d'e-santé, promeut l'usage des services numériques en santé dans les territoires et enfin apporte son expertise aux acteurs régionaux* »[820]. A ce titre, il travaille en collaboration directe avec les professionnels de la région pour leur proposer des outils d'e-santé répondant pleinement à leurs besoins, et notamment ceux liés à leurs coordinations.

325. **Des initiatives régionales**. Deux exemples de services déployés par des GRADeS ont vu le jour, ressemblant à de petits dossiers patients limités à une discipline :

i. Krypton. Le GRADeS ESEA en Nouvelle-Aquitaine, propose Krypton, qui *« est un bouquet de services régional partagé en imagerie médicale. Il permet l'échange et le partage sécurisé d'examens d'imagerie réalisés entre les structures de santé publiques et privées adhérentes. Sa vocation première est l'amélioration de la prise en charge des patients, via l'accès facilité et sécurisé à leurs antériorités d'imagerie »*[821]. Ainsi, un professionnel prenant en charge un patient peut accéder via ce service, à l'ensemble des examens d'imagerie d'un patient et donc à ses antécédents sans transfert d'examens, notamment quand ceux-ci n'ont pas été réalisés au même endroit. Ce service permet donc au professionnel un gain de temps, une vision globale du dossier d'imagerie d'un patient, peu importe l'endroit dans lequel l'examen a eu lieu (sous réserve que l'établissement ayant réalisé l'imagerie soit adhérant du service) et permet au patient d'éviter une redondance d'examens. Ce service est un véritable dossier patient relatif à son imagerie au niveau régional.

ii. Pibio. Le second service que l'on peut citer est le service Pibio du GRADeS Pulsy en Grand Est, qui « *a pour objectif de faciliter le routage et la diffusion des comptes rendus de*

[820] Instruction n°SG/DSSIS/2017/8 du 10 janvier 2017 relative à l'organisation à déployer pour la mise en œuvre de la stratégie d'e-santé en région.
[821] esea, « Kryption ». Disponible à l'adresse : https://www.esea-na.fr/ (consulté le 03/08/2022).

biologie médicale »[822] permettant au professionnel prescripteur, au médecin traitant et au patient, d'avoir accès aux résultats de biologie de ce dernier. Ce service n'a pas en soi vocation à être un dossier complet recueillant tous les résultats de biologie d'une personne, mais permet le partage d'informations entre professionnel prescripteur et médecin traitant, favorisant la coordination des soins. Pibio alimente également le DMP du patient.

326. **Les limites de ces services**. Pour autant, ces services régionaux présentent des limites à une coordination optimale des professionnels limitant ainsi leur portée :

i. Comme cela est indiqué, les GRADeS proposent des services régionaux. Aussi, un service disponible dans un GRADeS, ne l'est pas, ou pas de la même manière dans un autre GRADeS. Donc un patient, pris en charge dans un établissement dépendant du GRADeS ESEA mais également dans un établissement dépendant du GRADeS e-santé Occitanie ne pourra pas bénéficier pleinement du service. Dans ce cas, les professionnels utilisant Krypton n'auront pas l'intégralité de l'imagerie du patient.

ii. Mais cela est également vrai au sein même d'une région. Seuls les professionnels adhérant au service peuvent en bénéficier. Aussi, si un patient réalise une imagerie au sein d'un établissement n'ayant pas adhéré à Krypton, son imagerie n'y sera pas. On ne peut donc pas considérer que les données contenues dans ce dossier régional soient exhaustives.

iii. Une autre limite apparente est la durée de conservation des données. En effet, ces services traitent des données à caractère personnel, et sont donc soumis au RGPD. A ce titre, « *le responsable du traitement, doit définir précisément la finalité du traitement et à partir de celle-ci, les données qui vont être collectées pour parvenir à la réalisation de cette finalité. […] Cette finalité devant être respectée pendant toute la durée du traitement, elles ne peuvent faire l'objet d'aucun traitement ultérieur dépassant le périmètre de la finalité initiale »*[823]. De ce fait, la durée du traitement doit être limité à la réalisation de la finalité établie, ce qui peut conduire à une conservation des données limitée dans le temps, contrairement au dossier patient d'un établissement de santé.

[822] Pulsy, « Biologie partagée - Pibio ». Disponible à l'adresse : https://www.esea-na.fr/ (consulté le 03/08/2022).
[823] Renato BRASSELET, *La circulation de la donnée à caractère personnel relative à la santé, - disponibilité de l'information et protection des droits de la personne, op. cit.*

B) Des projets nationaux

327. **Des projets nationaux**. Outre les projets régionaux, même si ceux-ci découlent de la stratégie en santé nationale, des projets nationaux ont vu le jour tendant vers la création de dossiers nationaux afin de favoriser la coordination des professionnels pour la prise en charge de leurs patients, palliant ainsi certaines limites rencontrées par les services développés en région.

328. **Le DP et le DMP**. Les deux dossiers nationaux emblématiques sont le dossier pharmaceutique (DP) et le dossier médical partagé (DMP).

Le dossier pharmaceutique[824] est un dossier informatisé recensant notamment les médicaments délivrés à un patient par un pharmacien au cours des quatre derniers mois, « *afin de favoriser la coordination, la qualité, la continuité des soins et la sécurité de la dispensation des médicaments, produits et objets définis à l'article L. 4211-1 et des dispositifs médicaux implantables* ».[825] Il permet ainsi d'éviter les redondances de traitement mais également de prévenir les problématiques en cas d'interactions médicamenteuses. Ce dossier est ouvert automatiquement pour toute personne, sauf opposition de cette dernière (ou du représentant légal) et doit être alimenté par tout pharmacien d'officine. Il est consultable, sauf opposition du patient, par les pharmaciens et les médecins prenant en charge le patient « *au sein d'un établissement de santé, d'un hôpital des armées ou de l'institution nationale des invalides ou le biologiste médical* »[826]. Après le délai de quatre mois, le dossier pharmaceutiques est conservé « *pendant une durée complémentaire de trente-deux mois afin de permettre, en cas d'alerte sanitaire relative à un médicament, un produit ou un objet défini à l'article L. 4211-1, d'en informer les patients auxquels il a été dispensé* »[827] sauf exceptions. Aussi, la consultation du dossier pharmaceutique est limitée dans le temps ; il n'est pas accessible à tous les professionnels de santé, tels que les médecins libéraux, alors même qu'un médecin travaillant au sein d'un établissement de santé peut y avoir accès.

Ce dossier est national, il est donc complété, peu importe la pharmacie dans laquelle le patient se rend, et est consultable par tous les professionnels habilités, peu importe la région dans

[824] Jean PARROT, « Le dossier pharmaceutique ou la réussite d'un projet mené par une profession », *Les tribunes de la santé*, 2011/3, n°32, pp. 101-109. « *Un projet tel que le DP ne naît pas en un jour. Il faut imaginer, créer, s'entourer de compétences, convaincre, structurer, financer, programmer, progresser, corriger, et aussi bloquer les coups tordus* ».
[825] C. santé publ., art. L. 1111-23.
[826] *Ibid.*
[827] C. santé publ., art. R. 1111-20-12.

laquelle il se trouve[828]. Pour autant, les données contenues dans le dossier pharmaceutique ne sont pas tout à fait limitées aux seuls professionnels habilités puisque, certes, les autres professionnels ne peuvent y accéder *via* le dossier pharmaceutique, mais ils pourront accéder à certaines données *via* le DMP dans la mesure où les informations « *utiles à la coordination des soins sont reportées dans le dossier médical partagé »*[829].

« Du dossier médical personnel au dossier médical partagé, il n'y avait qu'un pas que le législateur n'a pas hésité à effectuer, autorisant ainsi le partage des données de santé du patient avec des professionnels de différents horizons »[830]. Le dossier médical partagé est *un « véritable carnet de santé numérique […] [il] répond à un enjeu de santé publique : disposer de la bonne information, au bon moment, où que l'on se trouve »*[831]. Il est ouvert automatiquement à l'ouverture de l'espace numérique de santé d'un patient (ENS appelé aussi, mon espace santé)[832], sauf opposition de ce dernier. Il *contient « toutes les informations médicales »*[833] qu'il s'agisse des antécédents, des résultats d'examens ou encore des médicaments pris par le patient[834] ; il est alimenté par les professionnels de santé. Ceux-ci, en prenant en charge le patient ont la possibilité, avec le consentement de ce dernier, d'accéder à son DMP mais ne peuvent accéder qu'aux informations autorisées par la matrice d'habilitation établie[835]. Pour autant, on constate que malgré le devoir d'alimentation du DMP par les professionnels, ce n'est pas toujours le cas, le rendant non exhaustif.

---

[828] Carine WOLF-THAL, « Le Dossier Pharmaceutique, outil clé du virage numérique en santé », *DSIH*, 2021. *« Le DP est accessible depuis 2011 pour les pharmacies à usage intérieur, et depuis 2017 pour tous les médecins exerçant en établissement de santé. Cet outil professionnel qui couvre 45 millions de patients a fait ses preuves aussi bien dans l'amélioration du suivi des patients que dans le décloisonnement ville-hôpital et 500 établissements de santé y sont raccordés dans toute la France ».*

[829] C. santé publ., art. L. 1111-23.

[830] Alain MACRON, « Loi de modernisation de notre système de santé et partage d'informations de données de santé : consécration du secret partagé tous azimuts », *RDS*, 2016, n°74, pp. 919-922.

[831] Assurance Maladie, *Le Dossier Médical Partagé (DMP) en pratique*, 2022.

[832] Mon espace santé, *A propos – Mon espace santé, c'est quoi ?*. Disponible à l'adresse : https://www.monespacesante.fr/ (consulté le 23/08/2022). Pour rappel, l'ENS ou mon espace santé est « le nouveau service public qui permet à chacun de stocker et partager ses documents et ses données de santé en toute sécurité pour être mieux soigné. Mis en œuvre par le Ministère chargé de la santé et l'Assurance Maladie, Mon espace santé regroupe 2 fonctionnalités principales : Un **dossier médical**, pour stocker de manière sécurisée des documents ajoutés par vous-même ou vos professionnels de santé (ordonnances, comptes rendus d'hospitalisation, de biologie). Vous pouvez également alimenter votre profil médical pour retracer l'historique de votre vie médicale (mesures de santé, traitements, carnet de vaccination, antécédents médicaux, …) et les partager avec les professionnels de santé, en particulier en cas d'urgence ; Une **messagerie sécurisée** de santé pour échanger des informations et recevoir des documents de vos professionnels de santé en toute confidentialité ».

[833] DMP, « En savoir plus sur le DMP – FAQ ». Disponible à l'adresse : https://www.dmp.fr/ (consulté le 11/08/2022).

[834] C. santé publ., art. R. 1111-42.

[835] La matrice d'habilitation est disponible à l'adresse : https://www.dmp.fr/matrice-habilitation

Une des particularités du DMP est que le patient a lui aussi, la possibilité d'y accéder, et notamment de gérer les droits d'accès, lui permettant d'être réellement acteur de sa santé.

Finalement, ne pourrait-on pas voir le DMP comme un dossier patient national qui pourrait devenir unique ? Pour l'instant, il est bien indiqué que *« le dossier médical partagé ne se substitue pas au dossier que tient chaque professionnel de santé, établissement de santé ou hôpital des armées, quel que soit son mode d'exercice, dans le cadre de la prise en charge d'un patient »*[836], même si sa vocation est de constituer petit à petit l'historique médical du patient. « *Le DMP est donc différent de tous ces dossiers médicaux détenus par les professionnels ; lui seul regroupe l'ensemble des informations utiles à la coordination de votre parcours de soins, présentes dans les différents dossiers professionnels »*[837].

Mais regroupe-t-il vraiment tout l'historique médical du patient ? Rappelons-le, le DMP n'est pas un concept nouveau ; dès 2004, le dossier médical personnel (l'ancêtre du dossier médical partagé) a vu le jour par le biais d'expérimentations pour finalement permettre sa création par tout un chacun dès janvier 2011. « *La technologie fonctionne. Le cadre juridique est opérationnel, mais le DMP ne décolle pas »*[838]. Par la Loi de modernisation de notre système de santé de 2016, ce dossier est rebaptisé « dossier médical partagé ». Ce dernier a subi un toilettage le rendant davantage attractif et son utilisation devient de plus en plus impérative. Pour autant, on constate que son utilisation ne décolle toujours pas, certains le qualifient même de « *coquille sécurisée, mais médicalement peu pertinente »*[839] ; *« en 2019, il apparaissait que 46% des médecins généralistes le consultaient et que seulement 20% l'alimentaient*[840]*. 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 »*[841]. Pour inciter les médecins libéraux à alimenter le DMP et surtout le VSM (Volet de Synthèse Médicale), un forfait a été mis en place ; *« 1500 euros si le médecin a élaboré des VSM pour au moins la moitié de sa patientèle ALD et que ces VSM alimentent le DMP ; ce forfait est porté à 3000 euros si le médecin a élaboré des VSM pour 90% de sa patientèle ALD et que ces VSM alimentent le DMP »*[842],

836 C. santé publ., art. R. 1111-40.
837 DMP, « En savoir plus sur le DMP – FAQ », *op. cit.*
838 Valérie OLECH, Bruno PY, « La loi 24 juillet 2019 et le virage numérique, le DMP de troisième génération et l'espace numérique », *RDS*, 2019, n°92, pp.930-935.
839 Sylvain BEORCHIA, « e-Médecine, e-santé et informatique – entre espoirs technologiques et désillusion humaniste », *Hegel*, 2017, n°4, pp. 289-299.
840 ANS, Doctrine technique du numérique en santé, concertation publique, 2020, p. 2.
841 Agathe VOILLEMET, *L'usage de la donnée médicale – Contribution à l'étude du droit des données,* Thèse dactylographiée, *op. cit.*, p.87.
842 Arrêté du 22 septembre 2021 portant approbation de l'avenant n° 9 à la convention nationale organisant les

avec une majoration supplémentaire 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) »*[843].

Avec son intégration dans l'ENS, son ouverture automatique, et sa valorisation, on peut espérer une augmentation de son utilisation. Pour l'heure, « *DMP et ENS constituent des outils prometteurs, dont le cadre juridique est désormais inscrit dans la loi. […] leur efficacité collective et individuelle reste à démontrer »*[844].

329. **Une évolution de la place du DP et du DMP**. Les DP et DMP ont connu une modification majeure concernant leur modalité de création. En effet, avant la Loi n°2020-1525 du 7 décembre 2020, leur création était soumise au consentement du patient, tandis qu'aujourd'hui, elle est réalisée, sauf opposition de sa part. La création de ces dossiers s'en trouve favorisée développant ainsi la coordination des soins et donc une meilleure prise en charge des patients, dans les cas où les derniers sont réellement utilisés.

§2 Vers un dossier patient unique national au profit du patient

330. **Vers un dossier patient unique ?** Même s'il est bien précisé au sein du Code de la santé publique que le DMP n'a pas vocation à remplacer les dossiers patients des différents professionnels, on constate tout de même que l'évolution du Droit et de notre système de santé tend vers la création d'outils communs rassemblant l'ensemble des données d'un patient. L'ouverture automatique du DMP sauf opposition de la personne à la création de son espace numérique de santé en est un témoignage.

Un autre pas vers un dossier patient unique est l'obligation pour les GHT, de mettre en place un dossier patient commun, et de considérer que tous les professionnels de santé exerçant dans des établissements faisant partie du même GHT soient considérés comme faisant partie de la même équipe de soins[845], sous réserve, pour les professionnels, de participer directement à la prise en charge du patient. Aussi, chaque établissement membre d'un même GHT bénéficie d'un seul dossier patient ou au moins d'un dossier patient convergent. Ces dossiers nationaux laissent à penser qu'un dossier patient unique national pourrait voir le jour, impliquant que chaque professionnel ou établissement n'aurait plus à créer un dossier patient

rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016, JORF n°224, 25 septembre 2021, texte n° 19, art. 4.

[843] *Ibid.*

[844] Valérie OLECH, Bruno PY, « La loi 24 juillet 2019 et le virage numérique, le DMP de troisième génération et l'espace numérique », *op. cit*.

[845] C. santé publ., art. D.1110-3-4.

propre. C'est le cas aujourd'hui dans un pays voisin, l'Estonie (A). Est-il envisageable en France d'aboutir à un tel dossier, notamment au regard des bénéfices et des risques (B) ?

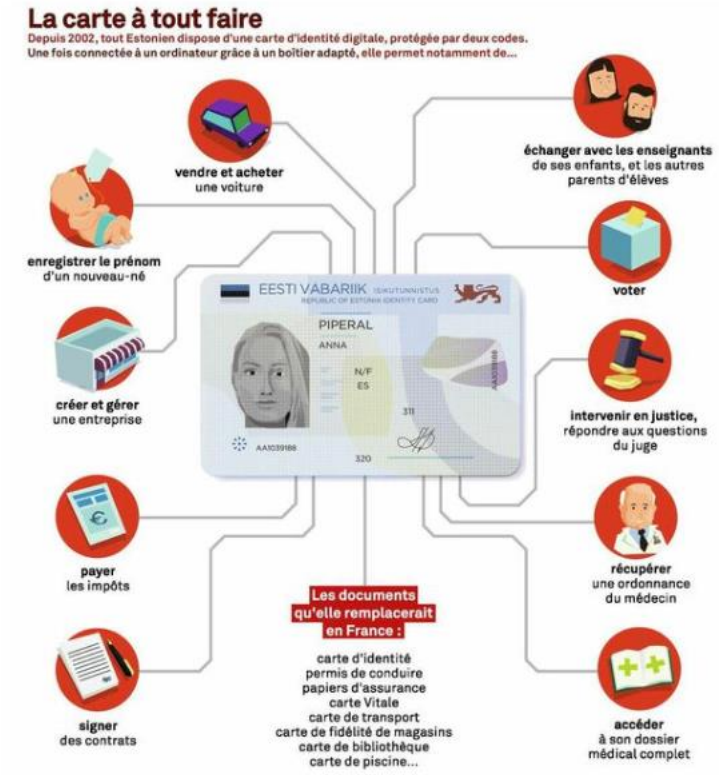
A) L'exemple d'un pays voisin, l'Estonie

331. **Le pays du tout numérique.** La dématérialisation de l'Estonie a démarré en 1991, à la suite de son indépendance découlant de la dissolution de l'Union soviétique. Ce pays partait d'une page blanche ; tout était à faire. L'Estonie a décidé de repartir de zéro et d'explorer la voie du tout numérique, notamment au regard de sa superficie par rapport au nombre d'habitants. Le but : permettre à toute personne, peu importe sa localisation sur le territoire, de bénéficier de tous les services, notamment de l'Etat. Aujourd'hui, presque tout en Estonie est réalisé par ordinateur, qu'il s'agisse de signatures des contrats, ou encore du paiement des impôts, (exceptés les actes les plus importants comme le mariage ou encore l'achat d'une maison pour le moment) puisque toutes les informations concernant la personne sont contenues sur une carte : informations personnelles, casier judiciaire, informations médicales. *« Les autorités ont calculé que chaque Estonien économisait en moyenne quarante heures par an, en paperasserie et en déplacements à la mairie, à la poste ou encore à la banque. L'équivalent d'une grosse semaine de travail »*[846].

Comment garantir juridiquement que la personne qui effectue un acte de signature par exemple, est bien celle qu'elle prétend si cette dernière est derrière un ordinateur ? Grâce à une carte d'identité électronique et connectée, permettant à l'Etat de certifier l'identité du détenteur *via* ce mode d'authentification fiable.

Par cette carte d'identité, qui est une véritable « carte à tout faire », chaque détenteur peut avoir accès à de nombreux services lui permettant d'effectuer toutes ses démarches. Elle lui sert également à remplacer toutes les autres « cartes », telles que la carte vitale, le permis de conduire ou encore les cartes de loisirs (piscine, bibliothèque etc.)[847].

[846] Benjamin JEROME, « L'Estonie, paradis du tout-numérique », *Le Parisien Week-end,* 2018.
[847] *Ibid.*



Les Estoniens n'ont plus besoin de posséder de papier, tout est sur la carte d'identité électronique.

En France, une telle carte d'identité n'existe pas encore, pour autant, nous possédons une carte électronique spécifique pour notre santé : la carte vitale qui est la carte d'assuré de la personne. *« Grâce à votre carte Vitale, votre médecin aura accès aux informations suivantes : votre identité et celle de vos ayants droit : enfants de moins de 16 ans, enfants de votre conjoint à la charge de votre foyer… ; votre numéro de sécurité sociale ; le régime d'assurance maladie auquel vous êtes rattaché : régime général (pour les salariés, les nouveaux étudiants 2018 et les indépendants), régime agricole, régimes spéciaux… ; la caisse primaire d'assurance maladie dont vous relevez, en fonction de votre lieu d'habitation »*[848]. Elle permet à l'assuré d'avoir le remboursement automatique de ses frais de santé. Cette carte Vitale est également indispensable en cas de création et d'accès au dossier pharmaceutique de la personne par le pharmacien. Elle permet notamment de s'assurer que le professionnel n'accède pas au DP sans motif légitime tel que la prise en charge de la personne.

332. **Le dossier patient dématérialisé**. L'Estonie a notamment mis en place un dossier patient qui permet à chaque Estonien d'avoir accès à son dossier médical complet *via* sa carte d'identité. Ce dossier de santé électronique *« intègre les données de tous apportées*

[848] Ameli, « la carte Vitale », 2022. Disponible à l'adresse : https://ameli.fr/ (consulté le 15/09/2022).

par les partenaires participants aux parcours de soins, chaque patient peut y accéder en ligne.
C'est une base de données nationale centralisée, le dossier de santé électronique récupère tous les documents médicaux, il les rend accessibles au patient dans un format standard via le portail e-Patient. Les médecins y ont un accès direct, ils peuvent lire les résultats biologiques, consulter les fichiers d'images, radiographies réalisées dans n'importe quel centre Hospitalier »[849].

Le patient ne fait pas qu'accéder à des documents de santé, il peut également bénéficier de services relatifs à sa santé, comme le e-transport sanitaire ou encore réaliser des formalités de santé, ce qui a eu pour effet de faire adhérer les Estoniens au dossier patient dématérialisé. Aujourd'hui, presque toute la population en possède un.

333. **La sécurité des données**. Comment garantir la sécurité d'un tel dossier au regard des données sensibles traitées ? La sécurité des données passe par plusieurs leviers :

i. Par la place centrale du dossier médical : le dossier médical en Estonie a été placé au cœur de la santé, si bien que le système de santé estonien a été construit autour du dossier patient et non l'inverse comme cela peut être le cas en France avec le DMP, ce qui donne une protection accrue du dossier[850].

ii. Par l'utilisation de la carte d'identité électronique qui permet de garantir, l'identité de la personne, grâce à son authentification par le biais de deux codes secrets, et la confidentialité et la sécurité des données grâce à la technologie Blockchain. En effet, la technologie Blockchain garantit : l'inviolabilité, par l'impossibilité de modifier ou supprimer une donnée, la transparence, par la possibilité pour toute personne d'avoir accès à ses propres données et de savoir comment elles ont été utilisées, et l'anonymat. « *Le dossier n'est ainsi accessible qu'aux personnes autorisées »*[851].

La confidentialité des données est notamment assurée par des sanctions très fortes prévues à l'encontre d'un professionnel dans le cas où il utiliserait les informations d'une personne à d'autres fins que sa prise en charge. A titre d'exemple, un médecin pourrait être interdit d'exercice. « *Mais en réalité, le nombre de plaintes est très faible : on compte 700 plaintes pour abus par an, sur plus de 500 millions de requêtes de données au total* ».[852]

[849] Nicolas BONDU et Marc SOLER (Dr.), « Chronique Estonienne chapitre II », *Innovation e-santé*, 2018.
[850] Solenne DUROX, « L'Estonie concilie e-santé et sécurité », *La Gazette des communes*, 2018.
[851] Nicolas BONDU et Marc SOLER (Dr.), « Chronique Estonienne chapitre II », *op. cit.*
[852] Pablo MAILLE, « En France, l'administration sert l'Etat, en Estonie elle sert le citoyen », *Usbek & Rica* »,

iii. Par la mise en place de X-Road, un système d'échange de données central sur lequel sont interconnectés tous les systèmes de l'Etat par des connexions temporaires, empêchant l'effondrement de la plateforme en cas d'attaque d'un des systèmes connectés.

vi. Par la création d'une « data embassy ». En effet, en 2017, l'Estonie a subi une cyberattaque de grande ampleur perturbant le fonctionnement du pays tout entier pendant près de deux semaines. De ce fait, le gouvernement estonien a ouvert une « data embassy » au Luxembourg, qui est « *une extension du gouvernement estonien sur le cloud,* [consistant] *en réalité à disposer de serveurs en dehors de son territoire pour sauvegarder une copie des données »*[853] mais qui permet également « *d'exploiter les services les plus critiques »*[854]. Cette « data embassy » permet de sécuriser le pays contre une nouvelle cyberattaque, mais également contre des catastrophes naturelles.

L'Estonie est aujourd'hui vue comme un leader en la matière et partage ses connaissances et ses outils avec d'autres pays ; par exemple, le système X-Road s'étend en Finlande.

B) La balance bénéfices/risques d'un tel projet

334. **Un dossier unique, une bonne idée ?** La question qui se pose est de savoir si la création d'un dossier médical unique pour chaque patient présente davantage de bénéfices que de risques, notamment au regard de notre système français actuel.

335. **Les bénéfices.** Comme vu précédemment, le dossier patient permet une meilleure prise en charge de la personne, grâce à la compilation des informations concernant son état de santé, notamment grâce à la coordination entre les différents professionnels qui utilisent cet outil. Or, ces informations et cette possible coordination sont simplement limitées aux professionnels pouvant accéder au dossier. Un dossier patient unique pour chaque patient permettrait une exhaustivité des données de santé d'une personne, et détiendrait son historique médical complet ; cet amas de données permettrait une coordination d'autant plus développée. N'est-ce pas un des objectifs du DMP[855] ? Les limites du DMP sont, qu'il n'est pas forcément rempli par tous les professionnels, ni même consulté, impliquant une perte du bénéfice de ce dossier. Avec sa création automatique par la création automatique de l'ENS pour chaque

2018.

[853] Anaïs CHERIF et Pierre MANIERE, « L'Estonie, royaume du tout numérique », *La Tribune,* 2018.

[854] e-Estonia, « e-Gouvernance – Ambassade des données ». Disponible à l'adresse : https://e-estonia.com/ (consulté le 10/07/2022).

[855] Hubert BALIQUE, Gaëtan GENTILE, Stéphanie GENTILE, Bernard GIUSIANO, Maeva JEGO, Roland SAMBUC, « Prise en charge des personnes sans chez-soi : intérêt du dossier médical partagé ? », *Santé Publique,* 2018/2, vol. 30, pp. 233-242.

patient, on ose espérer que son utilisation par les professionnels sera augmentée, tant dans l'alimentation que dans la consultation.

Un autre bénéfice marquant, un tel dossier permet une rapidité de prise en charge. Retournons en Estonie, pour voir les bienfaits de leur dossier en situation d'urgence : lors d'une prise en charge à la suite d'un appel aux services d'urgences ; les urgentistes ont une vision globale de l'état de santé de la personne, grâce à sa carte d'identité électronique. Des appareils interconnectés à la carte permettent de pousser directement les résultats obtenus au sein du dossier du patient tel qu'un électrocardiogramme. Toutes les informations recueillies par les urgentistes seront transmises instantanément au médecin de l'hôpital *via* la carte d'identité, ce qui permettra à ce dernier de donner, en temps réel, des instructions aux urgentistes, notamment de préconiser une hospitalisation. Il pourra également contrôler leurs actions à distance. Puisque toutes les données sont contenues dans un seul dossier, en cas d'hospitalisation, l'hôpital pourra préparer en amont de sa venue, la prise en charge du patient.[856]

Outre les bienfaits de la prise en charge des patients, un seul dossier permettrait une mutualisation des systèmes d'information et donc une réduction des dépenses. Cette mutualisation impliquerait obligatoirement une homogénéisation des pratiques, notamment une standardisation des documents médicaux facilitant la coordination entre les différents professionnels.

Pour terminer, même si ces bénéfices ne sont pas exhaustifs, un dossier patient unique pallierait la difficulté concernant la conservation des dossiers patients par les médecins libéraux décédés ou partant en retraite. D'après l'article R. 4127-45 du Code de la santé publique, le médecin doit tenir, pour chacun de ses patients, un dossier comportant les informations nécessaires à sa prise en charge, à l'instar du dossier patient en établissement de santé. Le médecin libéral est seul responsable de la conservation de ces dossiers et notamment de leur confidentialité. Mais pour quelle durée ? Les textes fixent clairement le délai de conservation pour les dossiers en établissement de santé, mais il n'en est rien pour les dossiers détenus par des médecins libéraux. *« Il a été d'usage de conseiller une conservation pendant 30 ans, durée alignée sur le délai de prescription de l'action en matière de responsabilité*

[856] Yaël GOUJON et Jérôme TOURNIER, « Nous les européens. Le coronavirus #etaprès ? Serons-nous tous fichés », *Reportage France 3*, 2020.

médicale. Ce délai a été ramené à 10 ans à compter de la consolidation du dommage par la loi du 4 mars 2002 »[857].

Pour autant, *« le CNOM recommande aux médecins d'appliquer les délais de conservation prévus pour les établissements de santé »*[858]. Mais avant cette date, quoi faire des dossiers patients en cas de cessation d'activité ? Le médecin, responsable de la conservation des dossiers, doit impérativement les conserver. Il n'a pas la possibilité de les céder à son successeur, puisque le patient a la liberté de choix de son praticien. Aussi, même en cas de cessation d'activité, le médecin reste responsable de ses dossiers et doit pouvoir répondre positivement si un patient souhaite avoir accès à son dossier médical. Pour davantage de facilité, le médecin doit informer le conseil départemental de l'ordre des médecins du lieu de conservation des dossiers. Et en cas de décès ? C'est aux ayants-droits que revient la charge et la responsabilité de conservation des dossiers ce qui implique deux problèmes majeurs[859] : d'une part, les ayants-droits se retrouvent avec une charge non désirée les obligeant à prendre des mesures de conservation et de gestion de documents de santé. D'autre part, les données de santé d'une personne seront transmises voire divulguées à des personnes non habilitées, ce qui entraîne une violation du secret professionnel. La création d'un dossier unique permettrait de pallier ce problème de conservation et déchargerait les médecins libéraux et leurs ayants-droits, de cette obligation.

Même si le DMP n'a pas, pour le moment, vocation à devenir le seul et unique dossier du patient, certains auteurs, à l'instar de Agathe VOILLEMET, estiment qu'un tel dossier offrirait au patient *« une 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. […] 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'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, tracés. 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*

[857] CNOM, *Le dossier du patient*, Information, 2022.
[858] *Ibid.*
[859] CNOM, « *Dématérialisation des documents médicaux »*, Rapport, 2010.

financière mais également de sanctions pénales et ordinales »[860]. Une parfaite connaissance de ses données médicales et un contrôle accru des accès aux données de santé sont donc deux autres bénéfices d'un dossier patient unique.

336. **Les risques.** Outre ces bénéfices qui ne sont plus à démontrer, quels sont les risques d'un tel projet ? Le premier risque identifié est l'insécurité potentielle des données de santé, qui sont, rappelons-le, des données sensibles. En comparant avec le dossier patient de l'Estonie, il est avéré que la sécurité est parfaitement gérée et est amenée à se développer et à se perfectionner dans le temps. Mais une sécurité optimale ne veut pas dire zéro risque. En effet, « *en 2017, une équipe de chercheurs internationaux découvre une brèche dans le système d'identification électronique : les cartes d'identité de 800 000 Estoniens, soit plus des trois quarts de la population, ont dû être refaites* »[861]. Une interconnexion aussi importante implique nécessairement de lourdes conséquences en cas de brèche de sécurité. De plus, la confiance n'est pas au rendez-vous en France puisqu'en 2021, sont dénombrés pas moins de 730 incidents au sein des établissements de santé, liés à de la cybercriminalité,[862] dont certains ont conduit à du vol de données.

Un autre risque est l'accès facilité aux données de santé concernant un patient, par tout professionnel. En effet, un seul dossier patient impliquerait que tous les professionnels auraient potentiellement accès à ce dossier ce qui pourrait entraîner des déviances. Mais, autant pour les risques de sécurité, que pour l'accès facilité aux données, c'est ce qui est actuellement le cas pour le DMP.

Ces risques sont dont déjà identifiés et encadrés, notamment avec les modalités d'accès fixés pour le DMP : d'une part, tous les professionnels ne peuvent pas forcément voir l'intégralité des documents. En effet, *« une matrice d'habilitation définit avec précision le type de documents auquel chaque professionnel de santé peut accéder en fonction des informations qui lui sont utiles pour* [la] *prise en charge* [du patient]. *Ainsi, par exemple, un pédicure podologue ne peut pas accéder à* [ses comptes rendus d'hospitalisation] *»*. D'autre part, l'accès au DMP n'est possible qu'avec la carte vitale du patient, sauf en mode « bris de glace » dans les cas d'urgence.

---

[860] Agathe VOILLEMET, *L'usage de la donnée médicale – Contribution à l'étude du droit des données,* Thèse dactylographiée, *op. cit.* pp. 91-92.
[861] Etienne LE VAN KY, « Protection des données : comment l'Estonie est devenue la référence de la cybersécurité », *Nice Matin*, 2021.
[862] Tom KERKOUR, « Les cyberattaques contre les établissements d santé ont doublé en 2021 », *Le Figaro,* 2022.

Conclusion du chapitre. Depuis quelques années, on assiste réellement à une volonté de dématérialiser complètement les documents contenant les données de santé, afin d'améliorer la prise en charge du patient, mais également notre système de santé. Cette volonté d'une dématérialisation totale, et notamment la création de dossiers régionaux mais également nationaux regroupant les données de santé du patient, laisse à penser qu'un dossier patient unique, à l'instar de l'Estonie, serait le bienvenu.

Ce dossier unique pourrait-il voir le jour prochainement ? La réponse est non. La France n'est pas encore mature pour mener un projet d'une telle envergure. Ne faudrait-il pas initialement travailler sur un mode d'identification et d'authentification extrêmement fiable pour les patients, à l'instar de l'Estonie ? Une des forces du dossier patient Estonien est bien cette fameuse carte d'identité électronique, que nous ne possédons pas (encore ?) en France.

De plus, le système de santé français met déjà en avant le développement de la e-santé, notamment avec la stratégie Ma santé 2022, dont les travaux sont encore en cours. Pour autant, avec la création automatique du DMP, on avance d'un pas vers ce projet.

Finalement, pour la réussite d'un tel projet, il est impératif de faire adhérer les principaux concernés : les patients et les professionnels de santé. Sans leur soutien, un tel projet ne peut pas voir le jour. Sans l'adhésion des patients, les dossiers dématérialisés ne seront pas créés, et pour les faire adhérer, il est nécessaire de leur en démontrer les bienfaits et assurer une sécurité optimale de leurs données. Sans adhésion des professionnels, le dossier ne sera pas alimenté et ne sera pas exhaustif. L'autre point important pour la réussite d'un tel projet est la mise en place d'un système d'information performant ; aujourd'hui, « *les systèmes d'information ont une utilité limitée. En théorie, ils permettent de faire ce qui est déjà fait, en mieux ou en plus vite »*[863]. Mais cela ne suffit pas toujours à faire adhérer les professionnels qui préfèrent « l'ancien système » au détriment de ce que peut apporter l'utilisation d'un système d'information. Il est impératif d'utiliser toutes les possibilités que les systèmes d'informations ont à offrir. « *Les meilleurs systèmes de santé partagent donc un certain nombre de caractéristiques, mais à la base, ce qui les relie tous, c'est une vision systématique de leur mission et de leur coopération. Si l'on résume à l'extrême, cette vision se conceptualise comme la recherche intégrée du triple objectif d'une meilleure expérience pour le patient, d'une meilleure santé pour la population, au meilleur coût pour la société. Cette intégration des objectifs pour chaque population, chaque prise en charge, débouche sur un*

[863] Antoine MALONE, « Innovations en santé publique, des données personnelles aux données massives (Big Data) », *Ethique biomédicale et normes juridiques*, Dalloz 2018, pp. 157-170.

rôle central pour les systèmes d'information, qui deviennent ensuite l'épine dorsale du fonctionnement clinique réel »[864]. La mise en place d'un dossier patient unique implique la création d'un système d'information qui soit performant, et surtout, qui puisse présenter de nombreux avantages pour les professionnels, pour les patients et pour les établissements de santé.

La mise en place d'un tel dossier n'est pas utopique ; prenons l'exemple du casier judiciaire unique automatisée fonctionnant depuis 1980. Depuis plus de quarante ans, chaque personne possède un seul et unique casier judiciaire informatisé comportant l'intégralité de ses condamnations, qui sont des données sensibles. S'il a été possible d'unifier et d'informatiser le casier judiciaire, il est tout à fait envisageable, quarante ans plus tard, de faire de même avec le dossier du patient.

Conclusion du titre. La dématérialisation permet de nombreuses avancées au sein des établissements de santé : la prise en charge des patients se voit transformée grâce à la e-santé, aussi bien avec les outils permettant la prise en charge tels que la télémédecine ou encore les outils de suivi patient, qu'avec les supports dématérialisés, nécessaires à la bonne prise en charge du patient, tels que les documents médicaux. On a pu constater tout au long des développements que le marché de la e-santé ou de la santé numérique ne fait que s'accroitre avec la création incessante de nouveaux dispositifs. « *Le développement massif de l'informatique en santé permet d'estimer, selon le cabinet Frost & Sullivan, à 234,5 Md$ la valeur du marché mondial de la santé numérique en 2023, soit une hausse de près de 160 % par rapport à 2019. Cette croissance s'explique essentiellement par les besoins liés au vieillissement de la population et à la forte augmentation des maladies chroniques, ainsi qu'au développement massif de l'informatique en santé, des technologies d'analyse de données et d'IA et de la prise en charge d'actes réalisés à distance avec la télémédecine et les objets connectés* »[865].

A ce rythme, à quoi ressemblera notre système de santé en 2030[866] au niveau numérique ? *« À l'horizon 2030, on peut prédire que la population française va continuer de croître, de vieillir et de s'urbaniser. […] L'espérance de vie à la naissance atteint 79,5 ans pour les hommes (67 ans en 1960) et 85,4 ans pour les femmes (73,6 ans en 1960) en 2018 en France métropolitaine. […] La population de la France s'élèvera à 70 millions en 2030, soit une*

[864] *Ibid.*
[865] Olivier BABINET, Corinne ISNARD BAGNIS, *La e-santé en question(s), op. cit.*, p. 21.
[866] Olivier BABINET, Corinne ISNARD BAGNIS, *La e-santé en question(s), op. cit.*, p. 7.

progression sur dix ans de 7 % »[867]. Ces données estimatives laissent à penser que les affections de longue durée seront également amenées à augmenter, que de plus en plus de patients auront besoin de soins réguliers, notamment au regard du vieillissement de la population. La santé numérique est une des clés essentielles pour assurer une bonne prise en charge de cette population.

De plus, le numérique est réellement vu comme novateur et révolutionnaire dans la manière de penser notre système de santé pour une prise en charge optimisée du patient : « *en 2030, la première porte d'entrée dans le système de santé sera dématérialisée. En amont, les patients auront accès à des dispositifs numériques de prévention en santé tout au long de leur vie qui seront accessibles depuis leur espace personnalisé. Surveillant eux-mêmes leur état de santé, les patients pourront également recourir à des plateformes d'orientation, tel le service d'accès aux soins, leur permettant d'accéder, à toute heure et à distance, à un professionnel de santé qui lui fournira un conseil, une téléconsultation, une orientation vers une structure ou l'envoi du SAMU selon son état de santé. […] L'hospitalisation à domicile « augmentée » par le numérique deviendra la norme. […] Les établissements de santé publics comme privés seront plus spécialisés, plus technologiques, davantage interconnectés entre eux et avec les structures médicales de ville. Ces établissements pourront se consacrer à la médecine d'urgence et la prise en charge des maladies aiguës qui nécessitent une intervention technique non réalisable en ambulatoire* »[868].

La dématérialisation en santé, présente véritablement un tournant dans la prise en charge du patient et devient un indispensable.

[867] *Ibid.*
[868] *Ibid.*

TITRE 2 : Les conséquences de la dématérialisation sur les droits du patient

337. **Le paternalisme médical**. Avant les années 2000, la relation médecin/patient était à sens unique, si bien que cette relation était considérée comme du paternalisme médical. Le patient était considéré comme malade, tandis que le médecin, lui, était le savant, l'expert, le « sachant », si bien que le médecin prenait seul les décisions médicales pour ses patients[869]. Le médecin était véritablement le chef d'orchestre de la prise en charge d'un patient, à l'instar du père à l'égard de sa famille.

Petit à petit, et surtout vers les années 2000, la vision de la prise en charge du patient a considérablement évolué en estimant que le patient ne devait plus être simple spectateur de sa santé, mais devait être en son centre et surtout d'en devenir l'acteur. Cela s'est notamment traduit par le développement de ses droits, jusqu'à aboutir à une Loi reconnaissant clairement les droits des patients en France.

338. **L'émergence des droits des patients.** Les droits du patient sont les prérogatives que détiennent les patients sur leur santé, certains parlent même de *« droits naturels inaliénables et sacrés de l'homme malade »*[870]. Mais cela va même plus loin puisque les droits des patients impliquent un devoir pour l'ensemble des professionnels de santé de respecter ces droits sous peine, en cas de non-respect, de voir leur responsabilité engagée.

Les droits des patients ont véritablement[871] été institués par la Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (1), dite également Loi « Kouchner »[872], reconnaissant ainsi au patient, le droit au secret de ses informations, à

[869] Alexandre JAUNAIT « Comment peut-on être paternaliste ? Confiance et consentement dans la relation médecin-patient », *Raisons politiques*, 2003/3, n°11, pp. 59-79. « La principale justification du paternalisme médical reste cependant d'ordre instrumental. Elle consiste, d'une part, à affirmer que le médecin est la personne la plus compétente pour réaliser le bien-être du patient et, d'autre part, que le patient est intrinsèquement dans un état le rendant inapte à prendre des décisions pour lui-même ».

[870] Patrick MISTRETTA, « La loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Réflexions critiques sur un droit en pleine mutation », *JCPG, op. cit.*

[871] Cela est confirmé par la doctrine en affirmant que *« l'architecture de ce texte et les principes qu'il a consacrés restent le socle incontesté des droits des personnes en matière de santé »*. Elle est même considérée comme *« recomposant en quelque sorte le « puzzle juridique » de la personne malade »*. (Dominique MARTIN et Didier TABUTEAU, « 18. Les droits des personnes malades », François Bourdillon éd., *Traité de santé publique.* Lavoisier, 2016, pp. 148-158).

[872] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (1), JORF, 5 mars 2002, texte n°1.

l'information et au consentement, mais également le droit au respect de sa dignité[873]. Ont suivi d'autres textes pour affiner, modifier ou créer des droits, tels que les droits des malades en fin de vie[874].

Les droits des patients sont nombreux et peuvent être découpés en six grandes rubriques[875] : i. le droit à l'accès aux soins et au choix du médecin. ii. le droit à l'information. iii. le droit à participer à la décision médicale et le droit au consentement. iv. le droit au respect de la personne soignée. v. le droit à la prise en charge de la douleur, soins palliatifs et fin de vie. vi. le droit de plainte, de contentieux et d'indemnisation. Face à cette multitude de droits, le patient se retrouve parfois perdu, ou n'en connaît même pas l'étendue.

Pour permettre aux personnes malades de connaître leurs droits essentiels concernant leur prise en charge dès lors qu'elles sont accueillies dans un établissement de santé, une charte a été créée (rédigée de manière vulgarisée afin que les droits soient aisément compréhensibles pour un profane)[876] : la charte de la personne hospitalisée[877], actualisée à la suite de la Loi Kouchner. Chaque établissement de santé a l'obligation « *d'intégrer le résumé de la charte dans* [son] *livret d'accueil »*[878] et d'en assurer la publicité, aux moyens de panneaux d'affichage par exemple[879].

---

[873] Marion GIRER, « Droits des patients et exercice en société », *RDSS*, 2014, p. 434. Marion GIRER fait état que cette Loi est occupe une place très importante dans tous les textes faisant état des droits du patient. En effet, *« l'étude de la genèse de la loi met clairement en exergue l'idée fondamentale selon laquelle les droits reconnus à toute personne qui recourt à des soins sont identiques quel que soit le statut juridique du professionnel de santé avec lequel il noue une relation, qu'il s'agisse d'un professionnel salarié, libéral, agent de la fonction publique, ou qu'il s'agisse d'un exercice individuel ou en société. Le texte a été construit de manière à placer le patient au centre du dispositif et à lui attribuer des droits liés à sa qualité de sujet de droit, indifférents à la qualification juridique de la relation de soins. Cette volonté peut être identifiée à travers la formulation symbolique des droits, énoncés comme de véritables droits des malades, donnant naissance à des obligations pour les professionnels, et non l'inverse ».*

[874] Loi n° 2005-370 du 22 avril 2005 relative aux droits des malades et à la fin de vie (1), JORF n°95, 23 avril 2005, texte n°1.

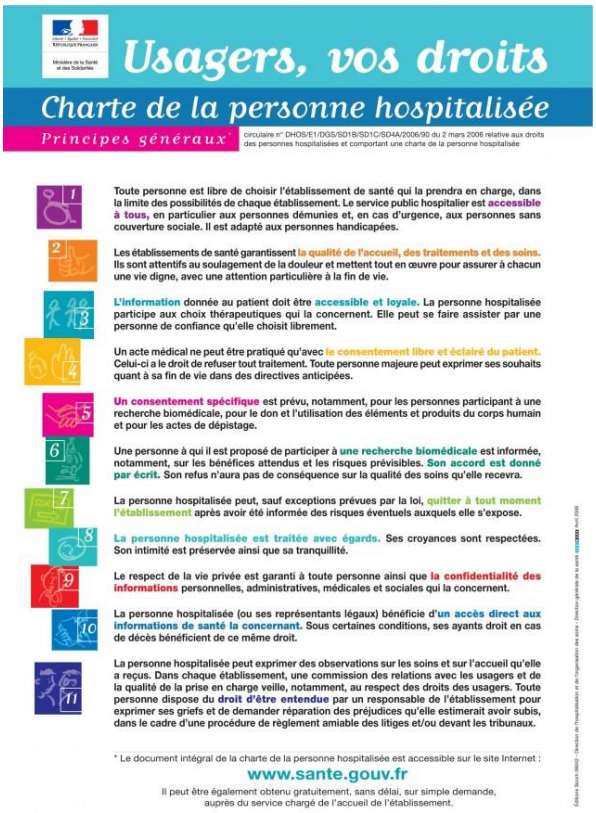
[875] HAS, *Droits des usagers : Information et orientation,* 2020.

[876] François VIALLA, « Brèves remarques sur la *nouvelle* charte de la personne hospitalisée », *RDS*, 2006, n°12, pp. 348-356.

[877] Circulaire DHOS/E1/DGS/SD1B/SD1C/SD4A/2006/90 du 2 mars 2006 relative aux droits des personnes hospitalisées et comportant une charte de la personne hospitalisée.

[878] *Ibid.*

[879] François VIALLA, « Brèves remarques sur la *nouvelle* charte de la personne hospitalisée », *op. cit.* Pour autant, *« les références opérées dans la loi à l'obligation de remettre les Chartes aux personnes accueillies ne leur confèrent assurément pas une valeur légale. Le mécanisme cependant n'est pas neutre sur le plan juridique en faisant de ces textes un outil indispensable et obligatoire de la prise en charge ».*



Usagers, vos droits

Charte de la personne hospitalisée

Principes généraux*

circulaire n° DHOS/E1/DGS/SD1B/SD1C/SD4A/2006/90 du 2 mars 2006 relative aux droits des personnes hospitalisées et comportant une charte de la personne hospitalisée

1 Toute personne est libre de choisir l'établissement de santé qui la prendra en charge, dans la limite des possibilités de chaque établissement. Le service public hospitalier est **accessible à tous,** en particulier aux personnes démunies et, en cas d'urgence, aux personnes sans couverture sociale. Il est adapté aux personnes handicapées.

2 Les établissements de santé garantissent **la qualité de l'accueil, des traitements et des soins.** Ils sont attentifs au soulagement de la douleur et mettent tout en œuvre pour assurer à chacun une vie digne, avec une attention particulière à la fin de vie.

3 **L'information** donnée au patient doit être **accessible et loyale.** La personne hospitalisée participe aux choix thérapeutiques qui la concernent. Elle peut se faire assister par une personne de confiance qu'elle choisit librement.

4 Un acte médical ne peut être pratiqué qu'avec **le consentement libre et éclairé du patient.** Celui-ci a le droit de refuser tout traitement. Toute personne majeure peut exprimer ses souhaits quant à sa fin de vie dans des directives anticipées.

5 **Un consentement spécifique** est prévu, notamment, pour les personnes participant à une recherche biomédicale, pour le don et l'utilisation des éléments et produits du corps humain et pour les actes de dépistage.

6 Une personne à qui il est proposé de participer à **une recherche biomédicale** est informée, notamment, sur les bénéfices attendus et les risques prévisibles. **Son accord est donné par écrit.** Son refus n'aura pas de conséquence sur la qualité des soins qu'elle recevra.

7 La personne hospitalisée peut, sauf exceptions prévues par la loi, **quitter à tout moment l'établissement** après avoir été informée des risques éventuels auxquels elle s'expose.

8 **La personne hospitalisée est traitée avec égards.** Ses croyances sont respectées. Son intimité est préservée ainsi que sa tranquillité.

9 Le respect de la vie privée est garanti à toute personne ainsi que **la confidentialité des informations** personnelles, administratives, médicales et sociales qui la concernent.

10 La personne hospitalisée (ou ses représentants légaux) bénéficie d'**un accès direct aux informations de santé la concernant.** Sous certaines conditions, ses ayants droit en cas de décès bénéficient de ce même droit.

11 La personne hospitalisée peut exprimer des observations sur les soins et sur l'accueil qu'elle a reçus. Dans chaque établissement, une commission des relations avec les usagers et de la qualité de la prise en charge veille, notamment, au respect des droits des usagers. Toute personne dispose du **droit d'être entendue** par un responsable de l'établissement pour exprimer ses griefs et de demander réparation des préjudices qu'elle estimerait avoir subis, dans le cadre d'une procédure de règlement amiable des litiges et/ou devant les tribunaux.

* Le document intégral de la charte de la personne hospitalisée est accessible sur le site Internet :

www.sante.gouv.fr

Il peut être également obtenu gratuitement, sans délai, sur simple demande, auprès du service chargé de l'accueil de l'établissement.

339. **La dématérialisation et les droits**. La dématérialisation de la prise en charge du patient, par l'utilisation de la e-santé, et notamment la dématérialisation des supports contenant les données de santé, conduit inévitablement à se demander ce que la dématérialisation implique pour les droits du patient.

Ces droits sont le ciment-même de la prise en charge actuelle. En effet, le patient, détenteur de droits, est au cœur de sa prise en charge, ce qui implique que cette dernière doit être réalisée dans le respect de ses droits. Aussi, l'objectif d'une dématérialisation totale d'un établissement de santé passe nécessairement par la dématérialisation des supports nécessaires au respect des droits du patient (chapitre 1).

Le respect des droits des patients ne se limite pour autant pas aux supports mais plutôt à leur application de manière générale. On peut se demander si la dématérialisation au sein d'un établissement de santé va respecter les droits du patient, les favoriser, ou au contraire les bafouer (chapitre 2) ?[880]

[880] Au regard de la multiplicité des droits détenus par un patient/usager, et au regard du sujet de thèse, le titre 2 de la partie 2 sera limitée aux droits présents dans la charte de la personne hospitalisée pour illustrer les propos bien que cette dernière n'ait aucune valeur normative. Or, elle fait état des droits principaux que détient un patient lors d'une hospitalisation.

Chapitre 1 : La dématérialisation matérielle d'un droit : le consentement du patient

340. **La dématérialisation matérielle d'un droit.** Les droits des patients sont des principes généraux qui ne se matérialisent pas physiquement en quelque chose que l'on peut toucher. Pour autant, afin de respecter ces droits, il est parfois possible d'utiliser des supports concrets tels que des écrits, qu'ils soient papier ou dématérialisés. Prenons l'exemple du droit pour le patient de quitter l'établissement de santé à tout moment. « *Une personne hospitalisée peut, à tout moment, quitter l'établissement. Lorsque la demande de sortie est jugée prématurée par le médecin et présente un danger pour la santé de la personne, celle-ci doit signer une attestation établissant qu'elle a eu connaissance des dangers que cette sortie présentait pour elle. A défaut de cette attestation un document interne est rédigé* »[881]. La signature par le patient d'une attestation de sortie est une transcription écrite du droit que le patient détient, soit, la possibilité de quitter l'établissement à tout moment. Cet écrit permet d'attester le respect du droit du patient mais montre également la validation de son choix par l'apposition de sa signature. Cette attestation est également un élément de preuve pour l'établissement en cas de contentieux, attestant l'absence de faute de l'établissement en cas de problème. Le document rédigé en interne par les professionnels, en cas d'absence de l'attestation signée du patient, permet également de démontrer que le droit du patient a été respecté et pourra être également utilisé comme moyen de preuve. En revanche, il manquera la validation du choix du patient par l'absence de sa signature.

341. **La dématérialisation du consentement.** Il apparaît donc que le respect et l'application des droits du patient peuvent se matérialiser par la production d'un support écrit, qui peut notamment être dématérialisé, en particulier lorsque le Droit n'impose pas d'écrit pour cette application, ou quand l'écrit est exigé et que la forme dématérialisée n'est pas explicitement interdite.

Pour autant, comment dématérialiser le support nécessaire au respect des droits du patient afin que celui-ci soit pertinent pour l'établissement et le patient, mais qu'il réponde également aux exigences imposées par le Droit ? Pour répondre à ces questions, nous allons nous baser sur un droit emblématique du patient, le droit au consentement (section 1) et sur sa dématérialisation, lorsque celui-ci est matérialisé sur support écrit dématérialisé (section 2).

[881] La Charte est disponible à l'adresse : https://solidarites-sante.gouv.fr/IMG/pdf/charte_a4_couleur.pdf

Section 1 : Les contours du droit au respect du consentement

342. **Le consentement, c'est quoi ?** Le consentement est défini comme l « *action de consentir ; résultat de cette action »*[882], c'est-à-dire, « *l'action de donner son accord à une action, à un projet ».*[883] Il s'agit d'un acquiescement, ou d'une approbation à quelque chose, notamment à un acte. En santé, le respect du consentement est un droit d'une importance primordiale pour la prise en charge du patient, et intervient dans absolument toutes les situations. Au même titre que les droits des patients, il existe pléthore de consentements parmi lesquels on peut retrouver : le consentement à l'acte médical, le consentement au partage d'informations entre différents professionnels de santé, le consentement à la prise d'un traitement ou encore le consentement du patient à la présence d'un étudiant en formation lors d'une consultation voire à la réalisation d'un acte par ce dernier. Le principe même est que, en tant qu'acteur de sa santé, le patient a le choix sur l'intégralité de sa prise en charge sauf exceptions prévues explicitement par les textes.

343. **Un acte, plusieurs consentements**. Il arrive parfois qu'un seul acte sur la santé nécessite le recueil de plusieurs consentements. Prenons l'exemple de la télémédecine[884] : pour la réalisation d'une téléconsultation, le patient doit consentir à l'acte médical, au partage de ses informations, au traitement de ses données à caractère personnel, à leur hébergement par un tiers le cas échéant, et avant 2021[885] à l'utilisation des TIC. Le recueil de ces cinq consentements pour la réalisation d'un seul acte peut sembler difficile à mettre en œuvre, cependant, la mise en œuvre de ce/ces consentements peut être réalisée de multiples manières et notamment de manière dématérialisée, facilitant son/leur recueil. Mais avant de pouvoir envisager la dématérialisation du consentement du patient, il est nécessaire d'en déterminer les principes (§1) ainsi que la forme imposée (ou non) par les textes (§2).

§1 Le principe du consentement

344. **Le même principe pour tous les consentements ?** Le respect du consentement du patient est un principe fondamental au titre du respect de l'intégrité humaine, notamment lorsqu'il se rapporte à un acte réalisé sur son corps. En effet, le Code

[882] TLFi, *V° « consentement »*, subst. masc.
[883] Larousse, *V° « consentement »*, nom masc.
[884] Stéphanie LANGARD, *Approche juridique de la télémédecine – entre Droit commun et règles spécifiques, op. cit.*
[885] Décret n° 2021-707 du 3 juin 2021 relatif à la télésanté, JORF n°0128, 4 juin 2021, texte n°15.

civil prévoit, qu' « *il ne peut être porté atteinte à l'intégrité du corps humain qu'en cas de nécessité médicale pour la personne ou à titre exceptionnel dans l'intérêt thérapeutique d'autrui. Le consentement de l'intéressé doit être recueilli préalablement hors le cas où son état rend nécessaire une intervention thérapeutique à laquelle il n'est pas à même de consentir »*[886]. Aussi, le consentement du patient est impératif et doit être recueilli chaque fois qu'un acte de santé sur son corps est réalisé, il s'agit d'un des droits les plus importants en matière de santé. Il est notamment prévu, qu'« *aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne* »[887], sauf exceptions[888]. Donc tout acte de santé ayant un impact sur le corps humain doit être réalisé avec le consentement libre et éclairé de la personne. Or tous les consentements en santé doivent-il revêtir les mêmes caractéristiques ? Pour certains consentements, la réponse est évidente puisqu'il est précisé textuellement que le consentement doit être libre et éclairé ; l'ancien article R. 6316-2 du Code de la santé publique prévoyait que « *les actes de télémédecine sont réalisés avec le consentement libre et éclairé de la personne »*[889]. Mais pour les autres ? « *Les caractères du consentement – libre et éclairé – semblent des caractères généraux, applicables pour l'assentiment de toute information délivrée au patient »*[890], même s'il n'est pas, pour la plupart des consentements, mentionné les conditions devant être remplies pour qu'ils soient valables. Une disparité sur leur teneur ne serait pas cohérente pour la prise en charge du patient, notamment au regard de la signification de ces deux critères.

345. **Un consentement libre et éclairé.** Aussi, que ce soit le consentement à l'acte de soin ou tout autre consentement, le principe est que la personne devant le donner doit le faire de manière libre (A) et éclairée (B) afin que celui-ci soit valable. En l'absence d'un de ces deux éléments, le consentement est nul, ce qui peut engager la responsabilité des professionnels de santé et/ou d'un établissement de santé puisqu'ils n'auront pas respecté leur obligation.

[886] C. civ., art. 16-3.
[887] C. santé publ., art. L. 1111-4.
[888] Les exceptions au principe du consentement ne sont pas étudiées, puisque le but de l'étude est la matérialisation du consentement par la dématérialisation.
[889] C. santé publ., art. R. 6216-2.
[890] Stéphanie LANGARD, *Approche juridique de la télémédecine – entre Droit commun et règles spécifiques, op. cit.* p-99.

A) Un consentement libre

346. **La définition de libre en général**. Le premier critère pour qu'un consentement soit valable est que celui-ci doit être libre. Le terme libre peut être défini de plusieurs manières différentes : « *qui a le pouvoir d'agir, de se déterminer à sa guise ; qui n'est soumis à aucune contrainte, à aucun contrôle, à aucune restriction* »[891] ou encore « *qui n'est pas soumis à une ou plusieurs contraintes externes ; qui n'est pas soumis à la puissance contraignante d'autrui* »[892]. Aussi, pour qu'un consentement soit libre, celui-ci doit être réalisé par la personne en fonction de ses convictions, et sans que celui-ci soit donné sous la contrainte d'autrui. L'assentiment de la personne doit venir d'elle-même en fonction de son désir à elle, sans que son choix soit forcé par un élément extérieur, tel qu'un tiers ou alors que son consentement ne reflète pas sa volonté, mais celle d'une tierce personne. Ainsi, le critère de liberté *« renvoie nécessairement à la question de la contrainte »*[893] ; pour qu'un consentement soit libre, celui-ci doit être dénué de contrainte. Aussi en l'absence de liberté de choisir pour la personne, on ne peut pas considérer que cette dernière ait consenti.

347. **La définition de libre en santé**. Bien qu'elle n'ait aucune valeur normative, la Charte de la personne hospitalisée va dans ce sens pour le consentement à l'acte médical, puisqu'il est précisé que « *le consentement de la personne doit être libre, c'est-à-dire ne pas avoir été obtenu sous la contrainte et renouvelé pour tout nouvel acte médical* »[894]. Le caractère non contraignant revient donc, mais un autre élément est ajouté pour caractériser la liberté du consentement : il doit être renouvelé pour tout nouvel acte médical. Ainsi, pour que le premier critère du consentement soit rempli, celui-ci doit :

i. être réalisé sans contrainte de la part de qui que ce soit, notamment d'un médecin.

ii. être réitéré à chaque nouvel acte médical. On constate donc qu'il ne s'agit pas d'un consentement global à la prise en charge du patient, mais bien d'un consentement ciblé, devant être donné pour chaque acte réalisé. La réalisation d'un acte, y compris l'administration d'un traitement sans l'accord du patient, même si ce dernier aurait donné son aval trente secondes auparavant pour un autre acte médical, est susceptible d'engager la responsabilité du professionnel, puisque le patient n'aurait pas consenti à tous les actes.

---

[891] Larousse, *V° « libre »*, adj.
[892] TLFi, *V° « libre »*, adj.
[893] Morgan LE GOUES, *Le consentement du patient en droit de la santé,* Thèse dactylographiée, Avignon, 2015, p. 447.
[894] Circulaire DHOS/E1/DGS/SD1B/SD1C/SD4A/2006/90 du 2 mars 2006 relative aux droits des personnes hospitalisées et comportant une charte de la personne hospitalisée.

Cette notion de réitération est présente dans l'article L. 1111-4 du Code de la santé publique : *« aucun acte ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne »*[895]. La formulation « aucun » signifie *a contrario* que chaque acte et chaque traitement doivent recevoir le consentement préalable du patient.

Gardons tout de même à l'esprit que certains actes médicaux peuvent être réalisés sans le consentement de la personne et de manière contraignante : l'administration d'un vaccin issue d'une obligation légale ou encore la réalisation de soins sur une personne hors d'état d'exprimer son consentement.

348. **Une définition en santé restrictive ?** Peut-on considérer que cette définition du caractère libre du consentement soit restrictive par rapport à la définition générale du terme libre ? Certes, la réitération de l'acte est un élément supplémentaire à la définition générale, mais il semblerait qu'il manque la notion de « libre arbitre ». En effet, il est bien précisé que le consentement doit être donné sans contrainte, mais cela englobe-t-il le consentement donné par une personne sans que celui-ci soit véritablement le reflet de son propre consentement et non celui d'une tierce personne ? En soi, la contrainte est une « *violence physique ou morale exercée contre une personne afin de l'obliger à agir contre sa volonté »*[896]. Le fait, pour une personne d'accepter quelque chose par des propos délivrés par une autre personne l'obligeant, même inconsciemment à donner son accord, est considéré comme de la contrainte morale, puisque la personne agit contre sa volonté, même sans s'en rendre compte.

349. **Les limites du critère de liberté**. La définition du consentement « libre » en santé, permet véritablement d'englober toutes les situations, même si l'on peut constater ses limites. En effet, le fait pour un professionnel de santé d'exercer une forme de contrainte à l'encontre d'un patient pour l'inciter à consentir à un acte engage sa responsabilité ; mais qu'en est-il des contraintes exercées par d'autres personnes, comme la famille ? Le patient, peut parfois donner son consentement, qui n'est pas le reflet de sa volonté, mais celle d'un proche, rendant son consentement caduc en l'absence du critère de liberté. Charge au professionnel de s'assurer que le consentement donné est bien le reflet de la volonté de son patient.

[895] C. santé. publ., art. L. 1111-4.
[896] TLFi, *V° « contrainte »*, subst. fém.

B) Un consentement éclairé

350. ***« Le consentement « éclairé », une histoire d'information »***[897]. En l'espèce, le terme éclairé renvoie indéniablement à la notion d'information, afin de permettre à la personne de décider, de donner son consentement, en toute connaissance de cause. *« Il ne fait nul doute que l'information due au patient par le professionnel de santé, prescrite par l'article L. 1111-2, constitue une obligation part du respect du consentement de la personne ».*[898]

Cette information nécessaire pour exprimer le consentement de la personne, est un droit à part entière pour les patients, et revenant systématiquement comme élément indispensable pour la prise en charge des patients en général. Ce devoir d'information par le médecin a été reconnu dès 1942 avec l'arrêt Teyssier[899] de 1942 comme étant un *« devoir particulièrement intense ! »*[900].

351. **L'information : le corollaire du consentement.** Le médecin, avant de pratiquer un acte médical sur la personne du patient, et avant de recueillir son consentement, doit l'informer sur « *les investigations, traitements ou actions de prévention proposés ainsi que sur leurs alternatives éventuelles »*[901] mais aussi sur les conséquences possibles, les risques fréquents et/ou graves d'un traitement ou encore les conséquences prévisibles en cas de refus d'un acte ou d'un traitement[902]. Un arrêt récent de la Cour de Cassation réaffirme que pour donner un consentement éclairé, le patient doit avoir reçu au préalable une information : *« l'obligation, pour le médecin, de donner des soins attentifs, consciencieux et conformes aux données acquises de la science comporte le devoir de renseigner avec précision sur son état de santé, afin d'évaluer les risques encourus et de lui permettre de donner un consentement éclairé ».*[903]

L'information délivrée doit revêtir trois critères[904], elle doit être : i. loyale c'est-à-dire une information « *qui est inspirée ou marquée par l'honneur, la probité ou la droiture »*[905] soit, une information honnête et complète, reflétant les faits à un moment donné, sans tricherie ; ii.

---

[897] Morgan LE GOUES, *Le consentement du patient en droit de la santé,* Thèse dactylographiée, Avignon, 2015, p. 450.
[898] *Ibid.*
[899] Cass., req., 28 janv. 1942, Gaz. Pal. 1942. 1. 177 ; D. 1942. 63 ; F. Vialla et *alii*, préc., p. 147 s.
[900] François VIALLA, « Bref retour sur le consentement éclairé », *Recueil Dalloz,* 2011, p. 292.
[901] *Ibid.*
[902] C. santé publ., art. L. 1111-2.
[903] Cass, 1ère, 05 mars 2015, 14-12.292.
[904] *Ibid.*
[905] Larousse, *V°* « *loyal* », adj.

accessible et intelligible, c'est-à-dire une information claire et compréhensible pour les profanes, qui n'ont pas les compétences médicales requises pour comprendre le jargon médical ; iii. appropriée : en effet, pour qu'une information soit loyale, accessible et intelligible, elle doit également être appropriée. « *Si le devoir de loyauté renvoie à la vérité, celui de clarté permet de bannir le discours abscons scientifique et technique, le caractère approprié infuse cette dose d'individualisation en tendant à l'adaptation du discours à chaque personne* »[906]. Dans le cadre d'un acte médical, l'information donnée à un patient ne peut pas être la même pour tous les patients. « *Toute personne a le droit de connaître l'ensemble des éléments concernant sa prise en charge, néanmoins le médecin doit adapter cette information selon le discernement de la personne qu'il a en face de lui, selon sa capacité de compréhension* »[907]. Aussi, pour garantir la validité du consentement[908], l'information délivrée au patient doit être personnalisée afin qu'il puisse donner son accord en toute connaissance de cause. *« L'information doit donc être consciencieuse afin que le patient, profane, puisse appréhender correctement les dires du technicien, du professionnel »*[909] et ainsi permettre au patient de donner un *« juste consentement »*[910].

352. **La preuve de l'information.** L'information donnée au patient pour la réalisation d'un acte médical doit être réalisée lors d'un entretien individuel. Pendant cet entretien, le médecin devra répondre aux différentes questions du patient. Il est de sa responsabilité de s'assurer de la bonne compréhension de l'information par le patient. Pour cela, il peut reformuler dans d'autres termes ses propos, poser des questions au patient l'incitant à répéter avec ses propres mots l'information ou encore remettre un document écrit

---

[906] François VIALLA, « Bref retour sur le consentement éclairé », *op. cit.*

[907] Stéphanie LANGARD, *Approche juridique de la télémédecine – entre Droit commun et règles spécifiques, op. cit.*, p-90.

[908] Jacques LUCAS (Dr), « Le partage des données personnelles de santé dans les usages du numérique en santé à l'épreuve du consentement exprès de la personne », *Ethics, Medicine and Public Health,* 2017, vol 1, pp. 10-18. *« L'information est la source du consentement et de sa validité ».*

[909] Morgan LE GOUES, *Le consentement du patient en droit de la santé, op. cit.*, p. 451

[910] Marion GIRER, « A la recherche du juste consentement en matière de soins », *Les cahiers de la justice,* 2021/4, n°4, pp. 635-646. *« L'article L. 1111-4 al. 1er du code de la santé publique, issu de la loi du 4 mars 2002, dispose que « Toute personne prend, avec le professionnel de santé et compte tenu des informations et des préconisations qu'il lui fournit, les décisions concernant sa santé ». C'est désormais le modèle de la décision partagée qui domine la relation de soins. Le choix des mots n'est pas laissé au hasard : la personne prend les décisions concernant les actes de soins et traitements à réaliser, mais elle ne le fait pas seule. Elle doit être non seulement informée, mais également conseillée, guidée dans ses choix par le professionnel de santé. C'est bien le patient qui décide, au final, car « Aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne et ce consentement peut être retiré à tout moment », mais il ne doit pas être abandonné dans la prise de décision. C'est à ce prix qu'un « juste consentement » pourra être consacré. La volonté ne doit pas être contrainte, mais accompagnée et guidée, éclairée par une information loyale, claire et appropriée.*

reprenant les éléments d'information[911]. C'est à la charge du professionnel, en cas de contentieux, d'apporter la preuve que l'information a bien été donnée et surtout comprise[912].

353. **L'information nécessaire pour tous les consentements ?** L'information étant un des deux critères permettant au consentement d'être valable, elle est impérative avant tout recueil de consentement. Mais doit-elle prendre la même forme que pour l'information préalable à la réalisation d'un acte médical, c'est-à-dire, doit-elle être loyale, accessible, intelligible et adaptée ? Il semble difficile d'imaginer le contraire, d'autant plus qu'une information non comprise ou viciée, implique nécessairement l'invalidité du consentement.

En revanche, l'information peut prendre des formes différentes selon le contexte, la pertinence, et la personne en face de lui. Pour certains patients, il sera pertinent de donner l'information en s'appuyant sur des schémas réalisés sur papier, tandis que pour d'autres, s'appuyer sur un document écrit pourrait suffire. A la suite de l'entretien réalisé par le médecin, l'information peut être notamment réitérée par un autre professionnel, tel qu'une infirmière.

354. **L'information implique-t-elle le recueil systématique d'un consentement ?** On l'a vu, le consentement ne peut avoir lieu sans l'information, mais l'information peut-elle être requise sans aboutir à un consentement ? La réponse est oui. Le Droit peut exiger la fourniture d'une information au patient, sans pour autant nécessiter le recueil d'un consentement. Un exemple concret est l'information concernant la tarification des prestations : en effet, « *toute personne a droit à une information sur les frais auxquels elle pourrait être exposée à l'occasion d'activités de prévention, de diagnostic et de soins et, le cas échéant, sur les conditions de leur prise en charge et de dispense d'avance des frais. Cette information est gratuite* »[913] et doit être délivrée, pour « *les professionnels de santé exerçant à titre libéral et par les centres de santé, par affichage dans les lieux de réception des patients*

---

[911] En revanche, il apparaît qu'une attestation d'un supérieur hiérarchique, rédigée plusieurs années après les faits, attestant la bonne information d'un patient, n'est un élément de preuve pris en compte par les juridictions. Magali BOUTEILLE, « La preuve de l'information », *RDS*, 2007, n°19, pp. 633-634. *« S'il est admis que la preuve de l'information peut être apportée par tous moyens […], la Cour de cassation a, jusqu'à présent, fait preuve d'une grande souplesse quant à l'administration de la preuve, en admettant très largement les présomptions […]. Il est intéressant de constater que, pour la Cour administrative d'appel de bordeaux, les moyens de preuve apportés par le Centre Hospitalier n'ont, semble t-il, pas emporter leur intime conviction. […] Il en aurait été différemment si l'attestation avait été produite dans les jours suivant le geste thérapeutique, mais trois ans après les faits, et sans document écrit pour la conforter, on peut douter du caractère infaillible de la mémoire humaine ».* CAA Bordeaux, 22 mai 2007, n°04BX01203.

[912] Initialement, c'était au patient d'apporter la preuve que le médecin avait failli à son devoir d'information (Cass. civ. 1ère, 29 mai 1951). Un revirement de jurisprudence a eu lieu dès 1997 (Cass. civ. 1ère, 25 fév. 1997, pourvoi n° 94-19685 ; Bull. 1997, I, n° 75, p. 49). Cette position a ensuite été conformée par la Loi du 4 mars 2002.

[913] C. santé publ., art. L. 1111-3.

et par devis préalable au-delà d'un certain montant [et] *s'agissant des établissements de santé, […] par affichage dans les lieux de réception des patients ainsi que sur les sites internet de communication au public* »[914]. Cette information est à sens unique, dans le sens où le patient, ne doit pas, à la suite de cette information, donner son consentement. Pour autant, cette information doit tout de même être loyale, accessible, intelligible et appropriée, dans la mesure du possible.

§2 La matérialisation du consentement

355. **La matérialisation du consentement**. La question de la forme du consentement est très importante et absolument pertinente puisqu'elle permet de déterminer de quelle manière, le consentement doit être matérialisé, c'est-à-dire de quelle manière il doit être produit. En effet, pourquoi matérialiser tous les consentements de la même manière (A), rendant parfois la tâche fastidieuse, alors même que le Droit ne l'impose pas (B).

A) La forme du consentement

356. **La dématérialisation du consentement**. La question que l'on se pose est comment dématérialiser le consentement du patient pour attendre l'objectif du « zéro papier » en établissement de santé ? Mais pour répondre à cette question, il est nécessaire de se demander, quelle forme doit avoir le consentement afin de déterminer s'il est pertinent de le dématérialiser et si oui, de quelle manière.

357. **Les différentes formes du consentement**. Les textes de Droit indiquent la forme que doit revêtir le consentement, il peut être soit exprès ou sauf opposition, soit écrit ou matérialisé sous une autre forme.

Le consentement ou consentement exprès, est un consentement donné par le patient avec un acte positif. Il doit exprimer clairement son accord, et non pas « ne pas s'y opposer ». Un exemple de consentement exprès est le consentement à la réalisation d'un acte médical. En effet, il est bien indiqué qu'« *aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne* »[915] qui doit prendre la forme d'un acte positif de la part du patient, qui doit dire clairement et sans ambiguïté qu'il est d'accord pour la réalisation de tel acte ou traitement.

[914] C. santé publ., art. L. 1111-3-2.
[915] C. santé publ., art. L. 1111-4.

A contrario, certains consentements sont des consentements « sauf opposition » ou encore des consentements tacites. Le patient va recevoir une information (puisque sans une information, il ne peut pas consentir), et sans opposition de sa part, des effets seront produits. Il s'agit là bien d'un consentement même si ce dernier n'est pas donné expressément. Un exemple de consentement sauf opposition est le consentement à l'hébergement des données de santé réalisé par un tiers. En effet, cet hébergement, « *quel qu'en soit le support, papier ou numérique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime* »[916]. Le consentement à l'hébergement de données de santé par un tiers est donc un consentement donné de manière tacite puisqu'il est considéré comme recueilli sans opposition de la part du patient. Avant la Loi de modernisation de notre système de santé (1), ce consentement était exprès.

En outre, le consentement exprès suppose également de se poser la question du format du consentement ; doit-il être écrit ou non ? Par principe, en l'absence d'indication expresse, le consentement peut être réalisé par écrit, par oral ou par toute autre forme. En santé, seuls quelques consentements ont l'obligation d'être écrit notamment[917] : l'interruption volontaire de grossesse[918], la stérilisation à visée contraceptive[919], le prélèvement d'organes, tissus, cellules et produits du corps humain sur une personne vivante[920], la recherche interventionnelle qui comporte une intervention sur la personne[921], l'examen des caractéristiques géniques d'une personne et identification d'une personne par ses empreintes génétiques[922], le don et utilisation de gamètes[923]. En dehors des cas prévus par la Loi, le consentement exprès n'a pas l'obligation d'être écrit.

358. **Le retrait et le refus**. Deux autres cas sont à étudier dans le cadre de la forme du consentement afin de déterminer la pertinence de sa dématérialisation : le retrait du consentement et le refus. Toute personne ayant préalablement donné son consentement peut le retirer à tout moment. Cette possibilité est très souvent indiquée au sein des textes. En cas de consentement écrit, est-ce que le retrait du consentement nécessite un retrait également écrit ? Le droit public est caractérisé par le parallélisme des formes impliquant qu'un acte réalisé par

[916] C. santé publ., art. L. 1111-8.
[917] CNOM, *Recueillir le consentement de mon patient*, 2019. Disponible à l'adresse : https://www.conseil-national.medecin.fr/ (consulté le 21/07/2022).
[918] C. santé publ., art. L. 2212-5.
[919] C. santé publ., art. L. 2123-1.
[920] C. santé publ., art. L. 1241-1.
[921] C. santé publ., art. L. 1122-1-1.
[922] C. santé publ., art. R. 1131-4.
[923] C. santé publ., art. L. 1244-2.

une certaine procédure ne peut être défait que par la même procédure comme cela a été consacré par le Conseil d'Etat en 1994 par l'arrêt Allamigeon et Pagneaux[924]. Il n'est pas mentionné que le retrait du consentement doive être matérialisé sous la même forme qu'initialement, lorsqu'il a été donné, même si ce dernier devait être recueilli par écrit. Ainsi, contrairement au droit administratif, le retrait du consentement peut être réalisé, y compris par oral.

Quant au refus, doit-il être matérialisé ? Aucune disposition au sein des textes n'impose un écrit pour matérialiser le refus d'un patient.

B) La valeur juridique et probante du consentement

359. **L'écrit**. Le consentement exprès écrit apparaît donc comme l'exception au principe du consentement. Il n'est obligatoire que dans très peu de cas prévus expressément par la Loi, privilégiant plutôt un recueil du consentement plus facile. Pour autant, la pratique veut que des consentements, même non obligatoires, soient recueillis par écrit. La raison ? Une question de preuve. Mais un consentement écrit est-il suffisant pour apporter la preuve du consentement du patient ?

360. **La preuve de l'information et du consentement**. Comme vu précédemment, pour qu'un consentement soit valable, le patient doit obligatoirement avoir obtenu une information lui donnant toutes les données, tous les éléments nécessaires pour sa prise de décision. Le Code de la santé publique prévoit qu' « *en cas de litige, il appartient au professionnel ou à l'établissement de santé d'apporter la preuve que l'information a été délivrée à l'intéressé […]. Cette preuve peut être apportée par tout moyen* »[925]. Aussi, « *prétendant avoir correctement rempli ses devoirs d'information et de préconisation, le praticien doit encore administrer la preuve de ses allégations* »[926]. Le réflexe des professionnels est de fournir un document écrit et tangible[927], pour autant ce simple écrit ne suffit pas toujours à démontrer la bonne information du patient.

[924] CE, 10/ 7 SSR, 27 avril 1994, 147203 148545, publié au recueil Lebon.
[925] C. santé publ., art. L. 1111-2.
[926] François VIALLA, « Bref retour sur le consentement éclairé », *op. cit.*
[927] Pierre-Laurent VIDAL, « la signature d'un consentement éclairé n'est ni nécessaire ni suffisant pour apporter la preuve du respect de l'obligation d'information du patient », *RDS*, 2014, n°60, pp. 1378-1379. En effet, *« bon nombre de médecins pensent se ménager la preuve du respect de cette obligation en faisant signer ce document à leurs patients préalablement à toute intervention »*, ce qui n'est pas le cas.

A titre d'exemple, une décision de la Cour d'appel de Toulouse rendue en 2010[928] est venue affirmer qu'un document intitulé « consentement éclairé mutuel – autorisation d'opérer » signé par une patiente, ne suffit pas à valider le consentement de la personne en prouvant notamment que l'information a été donnée. En effet, ce document manquait d'informations, et bien qu'il soit signé, le juge a considéré que le médecin avait manqué à son devoir d'information, rendant le consentement caduc.

La Haute Autorité de Santé (HAS) a publié des recommandations de bonnes pratiques comme cela est prévu par l'article L. 1111-2 du Code de la santé publique. Elle réaffirme que « *le document d'information est exclusivement destiné à donner à la personne des renseignements par écrit. Ce document n'a pas à être signé par la personne et ne contient aucune formule l'invitant à y apposer une signature* »[929]. Le document d'information, et/ou le document de consentement signé à lui seul ne permet pas de démontrer que l'information a correctement été donnée et que le consentement est valable. En revanche, elle préconise davantage l'utilisation du dossier patient comme outil permettant de prouver, en cas de litige, que l'information a correctement été donnée. Une traçabilité des éléments d'information donnés au patient au sein du dossier patient suffit « *à servir de moyen de preuve en cas de litige, il n'y a pas lieu de demander à la personne une confirmation signée de la délivrance de l'information* »[930].

Cela a été réaffirmé dans un arrêt de la Cour d'appel de Marseille en 2014 : *« la production par un établissement hospitalier d'un document écrit signé par un patient n'est ni nécessaire, ni suffisante pour que puisse être considérée comme rapportée la preuve, qui lui incombe, de la délivrance de l'information »*[931]. En revanche, il est précisé que ce document apporté à l'appui d'un entretien préalable permet au patient « *de donner en connaissance de cause un consentement éclairé à l'acte de soins auquel il s'est ainsi volontairement soumis* »[932].

Puis récemment dans un jugement du 22 février 2016, celui-ci est venu confirmer la bonne information délivrée au patient alors même que le formulaire de consentement que l'ophtalmologiste avait fait signer au patient avait été égaré[933]. En l'espèce, un faisceau d'indices (remise obligatoire d'un document d'information, témoignage d'une hôtesse

[928] CA Toulouse, 1ère ch. sect., 25 octobre 2010, 10/01705., F. VIALLA, « Bref retour sur le consentement éclairé », D., 2011, p. 292.
[929] HAS, « *Délivrance de l'information à la personne sur son état de santé* », Recommandation de bonne pratique, 2012.
[930] *Ibid.*
[931] CAA Marseille, 2ème, 13 février 2014, n°11MA02696, Inédit au recueil Lebon.
[932] *Ibid.*
[933] Sophie LORIEAU, « Consentement écrit du patient égaré tout n'est pas perdu ! », *MACSF*, 2020.

d'accueil, le patient ne nie pas avoir reçu ce document) a permis d'établir que l'information avait été correctement donnée.

Les juges vont davantage apprécier la réelle délivrance de l'information grâce à un faisceau d'indices tels que la réalisation d'entretiens individuels avec le patient, les informations consignées dans le dossier du patient (les questions posées par le patient et les réponses apportées par le médecin), une fiche d'information générale remise au patient, etc.

Un formulaire de consentement signé ne permet pas à lui seul d'exonérer le professionnel et/ou l'établissement de sa responsabilité[934]. Rappelons-le, un document écrit n'est ni nécessaire, ni suffisant.

361. **Un consentement non écrit mais une information écrite**. Pour autant, même si l'écrit n'est pas toujours suffisant seul, il est parfois nécessaire et imposé par les textes. Prenons l'exemple du partage d'informations de santé concernant un patient, lorsqu'il a lieu entre des professionnels de santé et des non professionnels de santé[935] (ostéopathes, assistants de service social etc.). Lorsqu'un partage d'informations a lieu entre ces deux catégories de professionnels, le consentement de la personne doit être recueilli. En revanche, il est prévu que « *l'information préalable de la personne est attestée par la remise à celle-ci, par le professionnel qui a recueilli le consentement, d'un support écrit, qui peut être un écrit sous forme électronique, reprenant cette information. Ce support indique les modalités effectives d'exercice de ses droits par la personne 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* »[936]. Dans ce cas précis, la remise d'un document écrit est une obligation légale, et non plus un document servant d'indice. Pour autant, ce document ne doit pas revêtir de signature.

---

[934] François VIALLA, « Explication de texte : qu'est-ce que le consentement éclairé ? – CA Toulouse, 25 octobre 2010, n°508, 10/01705 », *RDS*, 2011, n°39, pp. 33-36. François VIALLA affirme à juste titre que la signature d'un formulaire ne permet pas au praticien de prouver indéniablement l'information du patient. *« Il s'agit d'une véritable méprise sur le sens de l'information requise et sur le but poursuivi par le texte (L. 1111-2). Obnubilés par la responsabilité, les praticiens semblent parfois se contenter du minimum en matière d'information se croyant « couverts » par le document « générique » qu'ils font signer au patient. […] L'erreur nous semble grande d'accorder foi au document « générique » si répandu. Pour avoir une quelconque valeur, il devrait répondre non seulement sur le fond mais encore sur la forme aux exigences légales et réglementaires ! Sur le fond, l'information frise aujourd'hui l'exhaustivité, l'arsenal des possibles devant être présenté au patient. Une grande précision sur les risques encourus est encore exigée. Sur la forme, dans la mesure où le sens de l'écrit, improprement qualifié de « consentement éclairé », est censé être maîtrisé par le patient, c'est dans la langue du malade et non celle du médecin qu'il faut décrire ce qui a été dit au cours de l'entretien ».*

[935] C. santé publ., art. R. 1110-2.

[936] C. santé publ., art. D. 1110-3-2.

362. **La signature d'un document comme preuve rassurante**. Bien que la signature d'un document, lorsque cela n'est pas obligatoire, ne permet pas à elle seule de prouver que le patient a reçu l'information et a consenti, on voit encore « *se multiplier les écrits, les praticiens développant nombres de documents de « consentement éclairé », de « permis d'opérer »… On se doit même de remarquer que pour bien des professionnels de santé la formule « consentement éclairé » est devenue synonyme d'écrit !* »[937] alors même que les recommandations des institutions et la jurisprudence affirme que la signature n'est ni nécessaire ni suffisante. Pour autant ces documents ne sont pas inutiles puisqu'ils constituent un élément de preuve et servent à « rassurer » les professionnels et les établissements de santé. Ces derniers doivent garder en tête que ces documents signés ne constituent pas une preuve irrévocable mais doivent être complétés par d'autres preuves. Est-il donc bien utile de se compliquer la tâche en recueillant une signature, la réponse est non. Est-ce que cela va rester la pratique ? La réponse est oui, pour l'instant.

[937] François VIALLA, « La défaillance dans l'information : une faute d'humanisme », *RJOI*, n°16, 2013.

Section 2 : la matérialisation du e-consentement

363. **Le consentement signé comme élément rassurant**[938]. Le consentement écrit signé, apparaît véritablement comme un document rassurant les établissements et les professionnels, estimant que grâce à ce document, ils sauront prouver que le patient a consenti conformément à leurs obligations légales. Or comme on a pu le voir, seuls quelques consentements doivent nécessairement être écrits et signés, et que ce document seul ne permet pas de les exonérer de leur responsabilité. Pour autant, ils constituent tout de même un élément de preuve même si les professionnels et établissements s'ajoutent des difficultés non-nécessaires dans la plupart des cas.

En revanche, pour faciliter leur pratique et/ou leurs obligations légales, et pour atteindre l'objectif du « zéro papier » au sein d'un établissement, il est possible de procéder à un e-consentement.

364. **Le e-consentement comme réponse aux besoins**. Le e-consentement est à distinguer du consentement dématérialisé par copie numérique, à l'instar de la prescription. Le consentement dématérialisé par copie numérique est la réalisation d'un consentement papier, éventuellement signé de manière manuscrite puis ensuite dématérialisé. Le e-consentement est la production d'un consentement de manière native numérique, avec éventuellement, l'apposition d'une signature électronique. L'utilisation de ce e-consentement plutôt qu'un autre permet de faciliter les échanges entre les professionnels et le patient et de tracer informatiquement les actions réalisées mais également les éléments communiqués au patient. Ce consentement peut être accompagné d'une information détaillée ; ces traces pourront être utilisées en tant que preuve lors d'un contentieux. Ce e-consentement permettra également de ne pas « égarer » les documents et donc de ne pas perdre des indices permettant de prouver la réalisation des obligations des professionnels. Or, pour que ce e-consentement soit utilisé comme preuve, celui-ci doit, à l'instar des documents contenant des données de santé,[939] bénéficier d'une valeur probante afin que son authenticité et sa fiabilité ne puissent être remises en cause (§1). Ce e-consentement bénéfique pour les professionnels et les établissements est possible grâce à la e-santé et l'utilisation de services numériques en santé (§2).

[938] Claude BERGOIGNAN-ESPER, « Le consentement médical en droit français », *Laennec*, 2011/4, tome 59, pp. 15-23. *« Il n'est pas nécessaire que le consentement soit écrit ou signé. Même si la pratique s'est passablement développée en ce sens, cette exigence ne figure pas dans les textes ».*
[939] Cf partie 1.

§1 La valeur probante du e-consentement

365. **Un document de consentement à valeur probante**. Indépendamment de l'intérêt juridique d'avoir un consentement écrit et signé, la question qui se pose en l'espèce est la valeur juridique et probante que doit revêtir un document matérialisant le consentement du patient. Même si, comme cela a pu être démontré précédemment, le consentement écrit et signé ne suffit pas à lui seul à démontrer son recueil, et que ce document écrit, n'est dans la plupart des cas, pas obligatoire, se pose tout de même la question de sa valeur probante. En effet, bien que cette forme ne soit pas nécessairement utile, elle est tout de même très utilisée et répandue, elle doit donc bénéficier d'une valeur probante pour être utilisée comme preuve, le cas échéant.

A l'instar de tous les documents natifs numériques[940] contenant des données de santé, des exigences en termes de sécurité et d'archivage doivent être respectées afin de garantir la fiabilité et l'intégrité du document dématérialisé nativement (A). Il doit également revêtir la signature électronique du patient afin de garantir son identité (B). C'est par le respect de ces exigences que le e-consentement aura la même valeur probante qu'un consentement écrit papier.

A) Le niveau de fiabilité exigé

366. **Rappel de la valeur probante des écrits nativement numériques contenant des données de santé**. Rappelons-le, un document, produit par un professionnel de santé qu'il exerce sa profession en établissement de santé ou en libéral, contenant des données de santé d'un patient, peut être créé sous forme numérique et possède « *la même force probante qu'un document sur support papier lorsqu'il a été établi et conservé dans les conditions prévues à l'article 1366 du code civil »*[941]. A ce titre, « *l'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »*[942]. Un e-consentement peut donc tout à fait avoir la même force probante qu'un consentement écrit papier sous réserve de pouvoir identifier le patient et garantir l'intégrité du document au moment de sa création et pendant toute sa conservation.

[940] Cf partie 1
[941] C. santé publ., art. L. 1111-27.
[942] C. civ. 1366.

367. **Le niveau d'exigence pour le e-consentement**. Le référentiel « force probante des documents de santé » produit par l'ANS, précisant les conditions d'application des dispositions relatives à la force probante des documents comportant des données de santé est pleinement applicable aux documents de consentement[943]. A ce titre, les exigences décrites précédemment s'appliquent pour le e-consentement[944]. Il est notamment précisé que « *les documents créés nativement numérique doivent ainsi disposer des propriétés permettant de répondre aux enjeux suivants : identification de l'émetteur ; intégrité et non répudiation ; pérennité dans le temps ; portabilité ; traçabilité* »[945] : tous ces éléments permettent de garantir la même valeur probante entre un consentement papier et un consentement natif numérique.

Or, le niveau d'exigences à respecter notamment concernant la sécurité, la traçabilité, les modalités d'authentification ou encore les mesures d'archivage vont dépendre de l'importance du document. Le référentiel de l'ANS a déterminé par type de document, le niveau minimal d'exigences à respecter[946] :

Type de document	Palier minimum à mettre en œuvre		
	Palier 1	Palier 2	Palier3
Expression de la volonté du patient			X
Information communiquée par la personne prise en charge	X		
Autre document du périmètre (traitement par défaut)		X	

En l'espèce, le document qui nous intéresse est celui qui permet de recueillir l' « expression de la volonté du patient », qui correspond au palier 3, c'est-à-dire au plus haut niveau d'exigence car ce document aura « *des conséquences sur sa prise en charge* »[947]. Les documents envisagés par l'ANS relevant de cette catégorie sont, bien que la liste ne soit pas exhaustive[948] : les directives anticipées, le refus de don d'organe, la décharge pour sortie contre avis médical, ou encore le don du corps à la science.

368. **Un niveau d'exigence adapté ?** Il apparaît que sont concernés, les documents devant faire l'objet d'un consentement écrit et signé, de manière obligatoire. Pour ces

[943] ANS, *Référentiel force probante des documents de santé – Document introductif, op. cit.*
[944] L'intégralité des obligations pour garantir l'intégrité du document ont été vues au sein de la partie 1 et s'appliquent dans les mêmes conditions. Ne seront présentés dans cette partie que les spécificités du e-consentement.
[945] ANS, *Référentiel force probante des documents de santé – Document introductif, op. cit.*
[946] ANS, *Référentiel force probante des documents de santé – Annexe 6 – Classification des documents de santé, op. cit.*
[947] *Ibid.*
[948] *Ibid.*

derniers, il apparaît évident que le plus haut niveau de sécurité et d'exigences doit être respecté puisque la volonté du patient et/ou son consentement, quand il est nécessaire, peut ou va entraîner des conséquences importantes sur sa personne, sur son corps.

Ce qui, semble-t-il reste très étonnant, est la nécessité d'avoir le même niveau d'exigence pour les consentements qui peuvent être recueillis par tout moyen, donc y compris par oral. En effet, il est prévu que le palier 3 couvre les documents exprimant la volonté du patient « *ou son consentement avec des conséquences sur sa prise en charge »*[949], et il est expressément écrit que la liste des documents n'est pas exhaustive ; cette formulation laisse à penser que tous les consentements, y compris ceux non obligatoires, doivent respecter le palier 3. Or un tel niveau d'exigence pour un consentement qui, de prime abord, peut être recueilli de manière orale semble disproportionné. Pour autant, si on regarde la formulation « consentement avec des conséquences sur sa prise en charge », tous les consentements entrent dans cette définition. A titre d'exemple, le refus ou le consentement à l'acte médical ou à un traitement entraînent inévitablement des conséquences sur la prise en charge du patient.

Cette position est-elle une manière d'essayer d'endiguer la pratique de faire signer au patient de multiples consentements, obligeant les professionnels à mettre en place le plus haut niveau de sécurité concernant la signature de tels documents ou de revenir aux bases et de ne faire signer que des formulaires de consentement, seulement lorsque le Droit l'exige ? Ou alors, est-il possible de baisser le niveau d'exigence pour les consentements non obligatoires, sachant que de toute façon, il ne s'agit que d'une preuve parmi d'autres, pour prouver le consentement du patient ? Le risque potentiel pourrait être de voir cette preuve écartée ou sa valeur amoindrie. Pour autant, la preuve pouvant être apportée par tout moyen, il est difficile d'imaginer qu'on puisse l'écarter, au seul motif qu'elle ne réponde pas au palier 3 du référentiel de l'ANS. Il sera donc nécessaire de pouvoir établir l'intégrité du document et posséder d'autres preuves.

369. **Une convention de preuve**. Pourrait-on utiliser une convention de preuve pour autoriser l'utilisation d'un palier inférieur, notamment pour les consentements écrits non obligatoires ?

Par principe, des professionnels peuvent conclure entre eux une convention de preuve, soit *via* un contrat ou encore des conditions générales d'utilisation, afin « *de permettre aux parties*

[949] *Ibid.*

d'aménager la manière dont elles vont démontrer les droits qu'elles peuvent être amenées à invoquer l'une contre l'autre lors d'une procédure contentieuse »[950]. En revanche, le juge n'est pas lié par cette convention de preuve, notamment s'il constate que les clauses de cette convention sont abusives et desservent davantage l'une ou l'autre des parties. Mais pourrait-on envisager cette solution entre un professionnel et un patient ? Le lien entre un professionnel de santé et un patient suppose déjà, rien que par la nature de leur relation, une position de force pour le professionnel. Aussi, il y a fort à parier qu'une convention de preuve, indiquant que le professionnel de santé peut baisser le niveau d'exigence imposé par l'ANS pour se constituer une preuve présumée fiable, serait considérée comme abusive par les juges, en cas de contestation de la part du patient.

Pour autant, hors les cas où la volonté du patient ou son consentement doivent être recueillis obligatoirement par écrit, il serait tout de même envisageable de baisser le niveau de fiabilité demandé, au regard des autres preuves que les professionnels doivent se constituer. Ce consentement écrit n'est qu'une preuve parmi d'autres.

B) La signature électronique du patient

370. **L'effet de la signature électronique**. Pour qu'un document puisse avoir une force probante équivalente à l'écrit papier, la personne dont il émane doit être identifiée. Dans le cadre du e-consentement, cette identification est notamment réalisée *via* sa signature, qui sera électronique mais cette dernière aura également d'autres fonctionnalités. En effet, la signature d'un document contenant des données de santé, réalisée par la personne prise en charge signifie qu'elle « *a pris acte du contenu du document et, le cas échéant, y consent* ».[951] La signature est donc obligatoire pour l'établissement d'un consentement, et plus particulièrement, une signature électronique dans le cadre du e-consentement.

371. **Les paliers de signature électronique**. A l'instar de la signature électronique pour les professionnels de santé, il existe des paliers de signature électronique pour les personnes prises en charge, allant du palier 1 à 3 : le palier 1 correspond à la signature électronique dite simple ; elle peut consister « *à apposer un cartouche graphique sur le document* »[952] après accord de la personne de manière orale. Le palier 2 correspond à la signature électronique simple mais pour laquelle l'acteur de santé vient sceller avec le

[950] ANS, *Référentiel force probante des documents de santé – Document introductif, op. cit.*
[951] C. santé publ., art. L. 1111-28.
[952] ANS, *Référentiel force probante des documents de santé – Annexe 3 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques, op. cit*.

certificat de l'établissement de santé, le consentement du patient, attestant davantage son intégrité. Le palier 3 est le plus haut niveau de signature électronique, il s'agit de la signature électronique avancée. « *Elle est réalisée par la personne prise en charge préalablement identifiée par un acteur de santé et après authentification de la personne prise en charge* »[953]. Ainsi, l'identification de la personne est réalisée par un acteur de santé, qui vérifie l'identité de la personne grâce à sa carte d'identité. Puis, « *l'acteur de santé saisit le nom le prénom et numéro de téléphone portable de la personne prise en charge dans l'application de signature. L'application affiche le document à signer. Elle est garante de la bonne représentation du document, et doit interdire la signature d'un document qui ne serait pas complètement visualisable* »[954]. Un OTP sms est ensuite envoyé sur le portable de la personne prise en charge. Il s'agit d'un mot de passe à usage unique, que la personne saisit dans l'application de signature, et qui permet d'une part de l'authentifier et d'autre part de valider la signature.

Aujourd'hui, le palier 3 est le plus haut niveau de signature pour les patients. Pour autant, ce mode d'authentification ne sera peut-être plus suffisant à terme, au regard de l'évolution législative concernant l'identification électronique[955].

372. **Quel palier choisir pour le e-consentement ?** La question qui se pose est : quel palier de signature choisir pour les e-consentements ? Au regard du document de classification des documents de santé, le palier 3 de signature serait celui qui est nécessaire pour la signature d'un e-consentement. Pour autant et comme vu précédemment, ne pourrait-on pas envisager des signatures électroniques plus faibles pour les consentements dont le formalisme écrit n'est pas imposé ? Par exemple une signature par tablette après la vérification de l'identité du patient par un acteur de santé, puis scellement de cette signature par le cachet de l'établissement. Cette signature ne serait pas avancée, elle serait un peu moins « fiable » mais avec pour autant une valeur juridique réelle. L'établissement de santé devra, en cas de litige, prouver qu'il s'agit bien de la personne prise en charge qui a signé et que ce e-consentement est intègre, de sa création jusqu'à sa production. Comme pour n'importe quel autre document contenant des données de santé, la production des métadonnées et des processus mis en place au sein de l'établissement de santé permettront de prouver l'intégrité du document et notamment du moyen de signature mis en place afin d'emporter la conviction du juge en cas de contentieux.

---

953 *Ibid.*
954 *Ibid.*
955 Voir le paragraphe B du paragraphe 2 de la section 1 du chapitre 2 du titre 2 de la partie 2 : l'identification et l'authentification du patient pour l'utilisation d'un service numérique en santé.

L'utilisation d'une signature avancée permet davantage de sécurité et de garantie en termes de valeur probante du e-consentement et il sera plus aisé d'emporter la conviction du juge, même si la production d'un consentement écrit n'est pas obligatoire. Pour autant, comme le consentement ne permet pas à lui seul de prouver le consentement du patient, et qu'il devra obligatoirement être complété par d'autres preuves, il apparaît envisageable d'utiliser une signature plus faible qu'une signature avancée.

En revanche, les consentements devant prendre la forme d'un écrit peuvent être réalisés sous forme dématérialisée, mais l'utilisation d'une signature avancée est alors obligatoire.

§2 Les services numériques comme réponse au recueil du e-consentement

373. **Les outils du numérique**. Partons du principe que les consentements dématérialisés peuvent prendre plusieurs formes et répondent à des règles différentes, comme l'utilisation d'une signature simple avec scellement ou d'une signature avancée. Est-il vraiment dans l'intérêt de l'établissement de santé de mettre en place des processus différents selon le consentement, alors même que le e-consentement a pour but de simplifier les choses ? Tout dépend du processus mis en place. Si l'établissement de santé ne fait pas signer systématiquement des consentements, différencier les processus a un réel intérêt. En revanche, pour tous les e-consentements, une homogénéisation des pratiques est souhaitable afin de mettre en place un seul processus bénéficiant du plus haut niveau de sécurité exigé afin de répondre à toutes les obligations légales pesant sur les professionnels et établissements de santé, peu importe le consentement dématérialisé réalisé. Dans cette optique, des services numériques ont vu le jour afin de recueillir et conserver les e-consentements des patients (A). Ces services spécialisés dans le recueil du e-consentement permettent d'en garantir l'intégrité et la fiabilité et assurent également l'identité du signataire (B).

A) Un outil de recueil et de centralisation des e-consentements

374. **Un service de e-consentement**. Depuis quelques années, des services de recueil dématérialisé du consentement ont émergé[956]. Bien plus qu'un service permettant la seule signature d'un consentement, qui peut être réalisé juste avec la mise en place d'une application de signature électronique, un service de e-consentement fournit davantage de

[956] Laure MARTIN, « e-consentement : pour une meilleure information du patient », *Mind Health,* 2021. *« Depuis quelques années, une nouvelle solution émerge au sein des établissements de santé : le recueil dématérialisé du consentement des patients. Ce dispositif, précis dans sa mise en œuvre, se situe à la croisée de l'information du patient et de la sécurisation de sa signature afin de garantir son identité ».*

fonctionnalités utiles pour les professionnels de santé, les établissements de santé mais également pour le patient. Ce simple service pourrait fournir la preuve de la bonne réception de l'information par le patient et donc de son consentement libre et éclairé.

375. **L'exemple d'un service existant** : **easy-consent**[957]. Prenons l'exemple d'un service de recueil de consentement dématérialisé pour les actes chirurgicaux, le service easy-consent. Ce service permet au patient de donner un consentement libre et éclairé lors d'une prise en charge médicale. Pourquoi libre ? Le patient n'est pas pressé par le temps puisque le recueil du consentement n'est pas instantané, au moment de la consultation avec le professionnel de santé. Le patient devra se connecter à la plateforme ultérieurement pour signer ou non son consentement. Cela lui laisse le temps de réfléchir et de poser les questions qu'il souhaite, le cas échéant. Pourquoi éclairé ? Le service ne permet pas que de signer un consentement, une information est fournie au préalable. Rappelons-le, un consentement éclairé signifie que le patient a obtenu une information de la part du professionnel qui soit loyale, accessible et appropriée[958]. Avant la mise en signature du consentement du patient, le service propose une information à destination de ce patient, information dont le contenu est vulgarisé, illustré, adapté et adaptable. En effet, l'information donnée est adaptée en fonction de l'acte pour lequel le patient doit consentir. Le professionnel a la possibilité de personnaliser lui-même les formulaires d'information et de consentement en fonction des besoins, notamment afin qu'ils soient totalement personnalisés pour le patient. Pour s'assurer de la bonne compréhension de l'information par le patient, ce qui est une obligation pour le professionnel, un questionnaire interactif personnalisable est mis en place[959] et le patient peut poser des questions ; les réponses lui sont fournies par un algorithme. A la suite de cette information, le patient est invité à signer électroniquement[960] son consentement, qui sera conservé au sein du service, pendant toute la durée des liens contractuels ou pendant la durée légale de conservation du consentement.

Le service de e-consentement est un réel outil pour le patient, lui permettant de comprendre pleinement les risques ainsi que les enjeux de sa prise en charge, mais également pour les

[957] Easy-consent, « Améliorez l'information du patient tout en vous protégeant juridiquement ». Disponible à l'adresse : https://www.calimed-sante.fr/ (consulté le 10/07/2022).
[958] Cass, 1ère, 05 mars 2015, 14-12.292.
[959] Easy-consent, « Améliorez l'information du patient tout en vous protégeant juridiquement ». Disponible à l'adresse : https://www.calimed-sante.fr/ (consulté le 10/07/2022).
[960] La plupart du temps, les services de recueil du consentement ont un partenariat avec des experts de la signature électronique tels que Yousign ou encore Docusign, afin de garantir la valeur probante de la signature électronique apposée.

professionnels et les établissements de santé, car ce service permet d'apporter les preuves nécessaires pour assurer que le consentement du patient est bien libre et éclairé.

376. **Les limites de ces outils**. En revanche, l'utilisation de tels services présente tout de même des limites à ce qu'il est possible de faire :

i. Ces outils ne dispensent pas les professionnels de santé de délivrer une information orale au patient lors d'un entretien individuel[961].

ii. Au regard du nombre de consentements et de leurs particularités, il est difficilement envisageable de créer un seul service pour le recueil de tous les consentements, bénéficiant d'une information aussi personnalisée. Un service moins performant, donnant une information et un consentement standardisés pourrait être envisageable mais présente moins d'avantages puisqu'il sera plus difficile, par le biais de ce seul service, de prouver que le patient a eu une information personnalisée et qu'elle a été comprise. Le professionnel devra tout de même consigner des éléments au sein du dossier patient.

iii. La réception de l'information et le recueil du consentement supposent que le patient se connecte ultérieurement sur le service de e-consentement. Or certains patients, notamment les personnes âgées, n'auront pas la possibilité et/ou pourront oublier de se connecter sur ce service. Il sera nécessaire d'effectuer des rappels automatisés mais aussi par téléphone pour rappeler au patient de se connecter. Les patients français ne sont pas encore suffisamment aculturés aux services d'e-santé pour garantir leur connexion systématique.

Malgré les limites des services de e-consentement, on voit ces outils se multiplier de plus en plus pour faciliter la pratique des professionnels et garantir un consentement libre mais surtout éclairé des patients. Ces services sont autant bénéfiques pour les professionnels et les établissements de santé que pour les patients.

B) L'identification et l'authentification du patient pour l'utilisation d'un service numérique en santé

377. **Un service numérique en santé**. Ces services de e-consentement sont des services numériques de santé au sens de l'article L. 1470-1 du Code de la santé publique : « *Les services numériques en santé […] sont les systèmes d'information ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique,*

[961] C. santé publ., art. L. 1111-2.

qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités »[962]. En effet, ces services électroniques concourent à la prise en charge du patient, en répondant notamment à des obligations légales d'information et de recueil du consentement du patient. A ce titre, ces services doivent respecter la PGSSI-S qui fixe « *les exigences relatives aux différents aspects de la sécurité des systèmes d'information en santé »*[963] et notamment de nouvelles exigences concernant l'identification et l'authentification des acteurs de santé et des usagers nécessaires pour l'accès à ces services numériques.

378. **Identification et authentification**. Dans le cadre de l'utilisation d'un service numérique pour le recueil du e-consentement, l'identification de la personne ainsi que son authentification sont primordiales d'une part, pour garantir la fiabilité du consentement, répondant aux exigences de la valeur probante du document, et d'autre part, pour pouvoir accéder au service grâce à l'identification électronique. Ces deux termes ne sont pas à confondre puisque l'un, l'identification, permet à une personne de communiquer son identité, tandis que l'autre, l'authentification, permet de prouver son identité. L'un et l'autre permettent l'identification électronique d'une personne, nécessaire pour utiliser un service numérique tel qu'un service permettant le recueil du e-consentement[964].

A l'instar du référentiel force probante, l'ANS a été chargée d'établir[965] un référentiel d'identification électronique pour les utilisateurs des services numériques, tels qu'un portail patient ou encore un site de prise de rendez-vous médical en ligne, notamment pour les usagers de ces services soit les patients, afin de « *préciser notamment les identifiants et dispositifs d'authentification utilisables pour ces personnes, en fonction du cadre d'usage »*[966]. Ce référentiel divisé en trois volets (personnes physiques acteurs de santé et du médico-social, personnes morales acteurs de santé et du médico-social et usagers) est applicable à compter du 1er juin 2022 bien qu'une période transitoire jusqu'au 31 décembre 2025 ait été mise en place afin de permettre la mise en conformité des services numériques. Ce référentiel est juridiquement opposable impliquant que son application est obligatoire, sous peine de voir la responsabilité des responsables de traitement des services numériques engagée.

---

962 C. santé publ., art. L. 1470-1.
963 ANS, *PGSSI-S.* Disponible à l'adresse : http://esante.gouv.fr/ (consulté le 17/07/2022).
964 Margo BERNELIN, « Le référentiel d'identification électronique en santé approuvé », *op. cit.*
965 C. santé publ., art. L. 1470-2 et L. 1470-5.
966 ANS, *Référentiel d'identification électronique – usagers »*, PGSSI-S, 2022.

379. **L'identification du patient en santé**. L'identification électronique d'une personne repose donc sur deux facteurs, l'identification de la personne et son authentification. Au quotidien, chaque personne s'identifie par son prénom, voire son nom, ce qui suffit à l'identifier par tout un chacun. Pour autant, dans le cadre de traitement de données plus important, ces simples informations ne permettent pas d'identifier clairement la personne au regard du risque d'homonymie. L'identification de la personne doit donc être réalisée avec plusieurs facteurs tels que son nom, son/ses prénom(s), son genre, sa date de naissance etc. pour ensuite lui attribuer un identifiant propre sous la forme par exemple d'un numéro. Cet identifiant permettra notamment d'éviter la collision avec une autre personne ou encore d'éviter la création d'un second identifiant à une personne en possédant déjà un. Cela contribue à l'identitovigilance. En effet, *« l'identitovigilance est l'ensemble des mesures mises en œuvre pour fiabiliser l'identification de l'usager afin de sécuriser ses données de santé, à toutes les étapes de sa prise en charge. La bonne identification du patient constitue le premier acte d'un processus qui se prolonge tout au long de sa prise en charge par les différents professionnels de santé impliqués, quels que soient la spécialité, le secteur d'activité et les modalités d'accompagnement »*[967].

En cas de mauvaise identification, ce dernier encourt de nombreux risques : administration de soins au mauvais patient, *« […] retard de prise en charge, […] erreur diagnostique, […] erreur thérapeutique, […] échange d'informations erronées entre professionnels (imagerie, examens de biologie), […] enregistrement de données de santé dans le dossier d'un autre usager (collision), […] création de plusieurs dossiers pour un même usager (doublons), […] erreur de facturation… »*[968].

Depuis le 1er janvier 2021, l'identification du patient pour référencer ses données de santé est l'INS, l'Identité Nationale de Santé[969], qui est propre à chaque patient, afin de fiabiliser son identification et ainsi lutter contre les risques liés à une mauvaise identification. Cet INS correspond au « *numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) »*[970] ou par le numéro d'identification d'attente lorsque la personne est en instance d'attribution du NIR.

[967] Ministère de la santé et de la prévention, « Identitovigilance – les bons soins au bon patient et au bon endroit », 2022. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 15/09/2022).
[968] *Ibid.*
[969] C. santé publ., art. L. 1111-8-1.
[970] *Ibid.*

Des exceptions à l'utilisation de l'INS est possible, permettant l'utilisation d'un identifiant « privé », propre à chaque fournisseur de service qu'il aura établi lui-même. Ces exceptions sont notamment les suivantes :

i. L'INS n'est pas connu : il peut s'agir du cas où la personne est prise en charge en urgence et que les professionnels ne connaissent pas l'identité de la personne ;

ii. La personne prise en charge est étrangère : dans ce cas, elle n'a pas de NIR ;

iii. L'impossibilité d'accéder à l'identifiant national de santé[971] : notamment dans le cas où le téléservice INSi, en charge de vérifier ou d'obtenir les numéros NIR est indisponible.

Cet INS est donc utilisé comme numéro identifiant le patient lors d'une prise en charge, contribuant ainsi à renforcer l'identitovigilance.

380. **L'authentification du patient par un moyen d'identification électronique**. Outre l'identité de la personne, l'identification électronique d'une personne *« repose sur un moyen matériel ou immatériel, qui garantit un niveau adapté de sécurité et de protection des données à caractère personnel traitées par le service numérique en santé concerné »*[972]. Actuellement, les moyens d'identification varient selon le type de service numérique en santé utilisé et sont associés « *à un niveau de garantie faible, substantiel ou élevé selon le niveau de sécurité qu'il*[s] *offre*[nt]»[973]. Le type d'authentification choisi par les fournisseurs de services doit fournir des garanties suffisantes de sécurité en fonction du type et de la quantité de données traitées. « *Ces choix doivent être pris en regard d'une analyse de risque concernant le service proposé, et prenant en compte la protection des données de santé à caractère personnel qui y sont traitées. Ceci comprend en particulier la garantie de confidentialité des données (que ce soit un vol massif de données par un attaquant externe, ou la consultation plus ou moins étendue de données par un professionnel, un usage ou un autre type d'intervenant) ainsi que d'intégrité de ces données (modification non autorisée ou accidentelle des données) »*[974]. L'analyse de risque doit également évaluer les risques d'accès éventuels aux données. Il est de la responsabilité du fournisseur de service de choisir un mode d'authentification adapté à son service au regard des retours de l'analyse de risque, reposant notamment sur deux facteurs[975] d'authentification de types différents parmi les trois suivants :

[971] C. santé publ., art. R. 1111-8-1.
[972] C. santé publ., art. L. 1470-2.
[973] ANS, *Référentiel d'identification électronique – usagers », op. cit.*
[974] *Ibid.*
[975] Jeanne BOSSI MALAFOSSE, « Publication du référentiel de sécurité relatif à l'identification électronique des acteurs de santé », *Delsol Avocats,* 2022.

connaissance, possession et biométrie. L'alliance de deux types de facteurs différents, par exemple mot de passe + OTP sms ou encore mot de passe + biométrie, permet de garantir l'identification électronique de la personne[976].

A terme, seuls les moyens d'authentification substantiels ou élevés, selon le Règlement eIDAS seront acceptés[977].

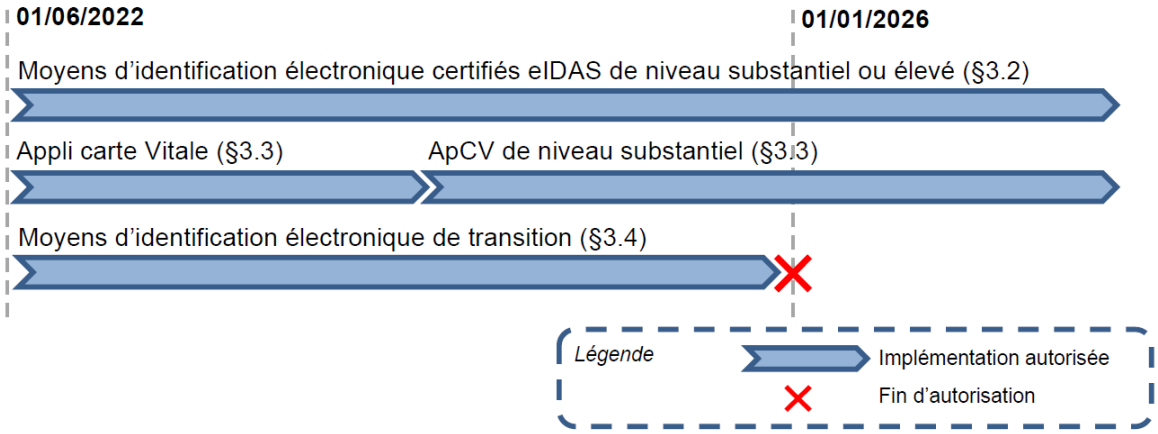
381. **L'identification électronique : comment ça marche[978]**. Pour créer l'identification électronique d'un usager, ce dernier va se faire enregistrer auprès d'un fournisseur d'identité. Ce fournisseur d'identité va enregistrer l'usager au sein de son répertoire, en vérifier l'identité grâce à la collecte de ses traits d'identité (exemples : nom de naissance, prénom(s), date de naissance, lieu de naissance etc.) et va ainsi pouvoir lui créer une identité électronique fiable et lui délivrer un moyen d'identification électronique lui permettant de s'authentifier. C'est le cas par exemple pour l'application ApCV, qui est la version dématérialisée de la carte vitale, actuellement en cours d'expérimentation jusqu'au 31 décembre 2022[979]. L'usager s'enregistre auprès du service gérant l'ApCV en fournissant ses traits d'identité et obtient une application installée sur l'appareil ayant servi pour l'enregistrement, permettant de s'identifier électroniquement. L'ApCV intervient comme fournisseur d'identité électronique de confiance. A terme, l'application ApCV sera « *le fournisseur d'identité de niveau substantiel eIDAS de référence pour le secteur santé/social* »[980] et pourra être utilisée comme identification électronique pour l'utilisation des services numériques en santé sur tout le territoire. Pendant la période transitoire, des identifications électroniques de niveau plus faibles peuvent être utilisées de telle sorte qu'un fournisseur de service numérique peut lui-même être fournisseur d'identité pour l'usager. Dans ce cas, en s'inscrivant sur le service numérique, l'usager communique ses données personnelles, choisit un login et un mot de passe pour l'utilisation du service et reçoit par exemple, un OTP sms pour garantir la fiabilité de son identité grâce à l'utilisation d'un double moyen d'authentification (mot de passe + OTP sms) à chaque connexion au service

[976] ANS, *Référentiel d'identification électronique – usagers », op. cit.*
[977] Margo BERNELIN, « Le référentiel d'identification électronique en santé approuvé », *op. cit. « Du côté des usagers, le référentiel impose à partir du 31 janvier 2025, et encourage vivement avant cette date, de recourir soit à des moyens d'identification électronique certifiés eIDAS dont le niveau de sécurité est substantiel ou élevé (à l'image de l'application FranceConnect), soit d'identifier les usagers grâce à l'application mobile carte Vitale. Dans ce cadre, l'identifiant utilisé pour que l'usager se connecte à un service numérique devra être de préférence son matricule « Identité nationale de santé ».*
[978] ANS, *Référentiel d'identification électronique – usagers », op. cit.*
[979] Décret n° 2019-528 du 27 mai 2019 relatif à l'expérimentation d'une « e-carte d'assurance maladie », JORF n°0124, 29 mai 2019, texte n°7.
[980] Bruno NOURY, « ApCV », *G.NIUS,* 2021.

numérique de santé. Les fournisseurs de services numériques sont libres de choisir le service d'identification qu'ils souhaitent.

Ce fournisseur de service intervient également au moment de l'authentification de l'usager pour sa connexion au service numérique, puisqu'il garantit l'identité de la personne. Ainsi, pour accéder au service numérique, que le fournisseur d'identité soit le fournisseur de service lui-même, ou un autre fournisseur, il intervient pour garantir l'identité de la personne. Au moment de l'authentification, un appel contextuel est également réalisé auprès du téléservice INSi pour obtenir ou vérifier l'identité INS du patient.

382. **Le calendrier**. L'offre actuelle concernant les moyens d'identification de niveau substantiel étant faible, des mesures transitoires ont été mises en place pour accorder du temps aux fournisseurs d'identité et aux fournisseurs de service de se mettre en conformité[981] :



En 2026, il ne sera plus possible d'utiliser n'importe quel fournisseur d'identité ; il sera nécessaire d'utiliser des moyens d'identification électroniques certifiés de niveau substantiel eIDAS ou élevés afin de garantir une fiabilité maximale concernant l'identité électronique du patient. Il s'agira notamment de l'application ApCV de niveau substantiel. Actuellement en France, seule l'identité numérique de la Poste possède un niveau substantiel accessible *via* FranceConnect+. Les moyens d'identification électronique de niveau substantiel et élevé sont disponibles sur le site institutionnel de l'ANSSI[982].

L'Etat travaille également sur le projet, à l'instar de la Belgique ou encore de l'Estonie, d'une carte d'identité numérique française[983] ou encore d'un passeport numérique qui seront des

[981] ANS, *Référentiel d'identification électronique – usagers », op. cit.*
[982] La liste des produits et services qualifiés est disponible à cette adresse : https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
[983] CASSAR Bertrand, *La transformation numérique du monde du droit*, Thèse dactylographiée, Strasbourg, 2020, p. 77. Bertrand Cassar a soulevé deux obstacles à une carte d'identité électronique ; 1. Le Conseil

moyens d'identification électronique de niveau substantiel et pourront servir également de signature électronique : un outil « deux en un ».

constitutionnel a considéré qu'intégrer un certificat de signature électronique était contraire à la Constitution. (cons. const. 22 mars 2012 n°2012-652 DC) 2. Il existe des limites techniques : Un certificat n'est valable que trois ans, alors que la carte d'identité l'est pour 10 ans. *« En outre, l'usage d'un CSE nécessiterai probablement l'achet d'un dispositif de création de signature électronique. De plus certaines techniques – telles que le RFID ou le NFC – ne remplissent pas nécessairement les exigences pour qualifier le dispositif ».*

Conclusion du chapitre. La dématérialisation de l'information et du consentement du patient présente de nombreux avantages pour les professionnels, les établissements de santé, mais également pour le patient.

Même si le recueil du consentement écrit n'est pour la plupart des cas pas obligatoire, la pratique actuelle veut que les consentements soient très régulièrement écrits. La dématérialisation de l'information et du consentement présente les mêmes avantages qu'une information et un consentement écrit ; cela permet de les utiliser comme preuve par les professionnels et les établissements en cas de contentieux. L'avantage de la dématérialisation est la possibilité d'automatiser l'information et le consentement, tout en les personnalisant quand même, grâce à l'utilisation de l'intelligence artificielle ou des algorithmes, comme la réponse automatique aux patients lorsqu'il pose des questions. Cette automatisation fait gagner du temps au professionnel, et permet de prouver grâce aux données informatisées, que le patient a pu poser des questions et a reçu une information complète ; mais elle permet également au patient d'être mieux informé sur sa prise en charge.

Quant au patient, cette dématérialisation, et notamment l'utilisation de service d'e-consentement lui permet de mieux appréhender sa prise en charge et de prendre le temps nécessaire à la réflexion, sans subir de pression même indirecte, telle la décision rapide devant être prise avant la fin d'un rendez-vous médical.

La dématérialisation permet un consentement plus libre et plus éclairé.

Chapitre 2 : L'évolution des droits des patients : une nécessité ?

383. **Les droits du patient impactés par la dématérialisation.** Comme vu précédemment, le patient bénéficie de nombreux droits entourant sa prise en charge médicale. Ces droits ont principalement été institués par la Loi Kouchner de 2002, qui a fêté cette année ses 20 ans[984] permettant un rééquilibre de la relation patient-médecin en plaçant véritablement le patient au cœur de sa prise en charge. Les droits du patient ont été renforcés par la suite avec d'autres Lois telles que la Loi HPST ou encore la Loi de modernisation de notre système de santé en 2016.

Lors de ces deux décennies, l'essence même des droits du patient n'a pas profondément été modifiée, même si des modifications successives ou des ajouts ont été réalisés. En soi, le patient bénéficie des mêmes droits aujourd'hui, qu'il y a 20 ans[985]. Pour autant, le système de santé et la prise en charge des patients ont bien évolués au cours de ces années et recourent de plus en plus, comme cela a pu être constaté au cours des développements, à l'utilisation du numérique en santé. Ces évolutions, notamment engendrées par le numérique, par la dématérialisation, impliquent inévitablement des conséquences sur les droits des patients. L'exemple du e-consentement étudié précédemment est un exemple tout à fait parlant et marquant puisque le droit au consentement du patient peut se matérialiser aujourd'hui de manière dématérialisée, tandis que vingt ans auparavant, la dématérialisation du consentement n'était pas envisagée, ni envisageable au regard de l'absence de valeur et de force probante de l'écrit dématérialisé.

384. **Les droits du patient appropriés ou inappropriés**. L'arrivée des nouvelles technologies dans le domaine de la santé a créé de nouvelles opportunités en matière de prise en charge du patient, tant au niveau des outils que des supports utilisés. Bien que le numérique et la dématérialisation ne soient pas des concepts nouveaux et ont pu être utilisés avant les années 2000, l'institution des droits du patient n'a pas pris en compte de prime abord le numérique. A l'heure actuelle, il n'est plus possible d'en faire l'impasse au regard de son développement croissant et inévitable. La question est de savoir si la dématérialisation de notre système de santé permet de garantir le respect des droits des patients à l'heure actuelle (section 1), ou s'il est nécessaire de l'adapter avec l'avènement du numérique (section 2).

[984] Vie publique, « Loi Kouchner sur les droits des malades : 20 ans après la loi, quel bilan ? », *Eclairage*, 2022.
[985] Sandrine CABUT, et Pascale SANTI, « Droit des malades : les vingt ans d'une révolution inachevée », *Le Monde*, 2022.

Section 1 : Dématérialisation VS droits des patients

385. **L'impact inévitable de la dématérialisation sur les droits**. La dématérialisation de la prise en charge du patient et l'utilisation de supports dématérialisés entraînent inévitablement un questionnement sur l'application des droits du patient à l'ère de la dématérialisation de la santé et du développement du numérique en santé. La plupart des droits du patient vont en effet être impactés, soit par leur dématérialisation matérielle à l'instar du consentement[986], soit par la dématérialisation des outils de prise en charge, ayant un impact sur un droit, comme l'accès aux soins.

386. **Un coup de pouce pour le droit des patients ?** Afin d'établir si les grands principes des droits du patient doivent être modifiés, ou encore adaptés au monde du numérique, il est nécessaire de se demander si ces droits sont ou ne sont pas respectés, lors d'une prise en charge d'un patient utilisant les outils du numérique et donc la dématérialisation. Il apparaît que certains de ces droits vont être favorisés par leur utilisation (§1), tandis que d'autres, vont plutôt voir leur application réduite (§2).

§1 Le respect des droits des patients favorisés par la dématérialisation

387. **Le numérique synonyme de danger**. Dans l'esprit de tout un chacun, dès lors que l'on parle de numérique, on pense inévitablement à la technologie et à ses bienfaits dans la vie de tous les jours, lui donnant un aspect très positif. Dès lors que l'on parle de numérique associé à des données plus personnelles et plus sensibles, telles que les données de santé, les personnes sont davantage mitigées et pensent tout de suite au mot « danger ». En effet, la dématérialisation des données renvoie à l'absence pour le patient de maîtrise de ses informations, de ses données, et l'éventualité qu'elles soient perdues dans le monde vaste de l'Internet ou réutilisées à d'autres fins. Pour autant, les bienfaits de la dématérialisation ne sont plus à démontrer, notamment pour le respect des droits du patient dans sa prise en charge.

388. **La dématérialisation : un service**. La dématérialisation et l'utilisation des services numériques en santé sont au service du patient (A) mais aussi au service du professionnel de santé et de l'établissement de santé (B) pour garantir le respect des droits du

[986] Laure MARTIN, « e-consentement : pour une meilleure information du patient », *op. cit.*

patient tout au long de sa prise en charge. Ils permettent même, dans certains cas, d'en favoriser le respect.

A) La dématérialisation au service des droits du patient

389. **Le droit des patients favorisé**. L'utilisation du numérique, des TIC ou la dématérialisation dans le cadre de la santé n'est pas un obstacle au respect des droits du patient, bien au contraire ; elle les favorise. Prenons l'exemple d'un des droits fondamentaux du patient, l'accès aux soins pour tous, et notamment l'égal accès aux soins[987]. Au regard de l'offre de soins sur le territoire national, des inégalités sont présentes et persistantes au regard de certaines zones isolées entraînant des déserts médicaux[988] et donc une absence d'offre de soins de proximité[989]. Cette disparité sur le territoire implique le non-respect d'un des droits fondamentaux du patient. En réponse à cette inégalité, des dispositifs sont mis en place comme la création de CPTS[990] rassemblant des acteurs de santé afin qu'ils puissent se coordonner en vue d'améliorer la prise en charge des patients sur un territoire donné. Au-delà de ces CPTS qui s'appuient notamment sur des services numériques en santé pour se coordonner, des outils de prise en charge à distance tels que les outils de télémédecine ou de télésoin, permettent de garantir aux patients l'accès à des professionnels de santé, même s'ils ne se trouvent pas à proximité. L'accès à des professionnels de santé sur toute la France permet d'offrir au patient un accès aux soins, peu importe son lieu de vie, même si celui-ci se trouve éloigné des praticiens. Le numérique et la dématérialisation de la prise en charge du patient permettent de mieux garantir le respect du droit à l'accès au soin ainsi que l'égal accès au soin.

390. **Les TIC garantissant le respect de plusieurs droits**. Les technologies de l'information et de la communication et les outils numériques permettent également de voir émerger des projets favorisant le respect des droits du patient grâce à la dématérialisation de certaines données, ce qui serait impossible à mettre en œuvre sans ces nouvelles technologies. L'Etablissement Hospitalier Sainte-Marie de soins de suite oncologique de Villepinte a mis en

---

[987] C. santé publ., art. L. 1110-1 et L. 1110-3.

[988] La Loi Kouchner de 2002 a posé le principe de non-discrimination dans l'accès aux soins, pour autant des inégalités continuent de persister, même vingt ans après : (Marion GIRER, « La loi n°2002-303 du 4 mars 2002 et les droits individuels des patients, vingt ans après », 2022, n°107, pp. 262-276) *« les difficultés demeurent et constituent pour l'avenir un enjeu fort de l'organisation de notre système de santé »*. Pour essayer de pallier en partie cette inégalité qui entrave un droit du patient, le système de santé s'appuie sur le numérique, comme cela va être détaillé dans le cadre de cette thèse.

[989] Delphine BAGARRY, « *Maillage territorial et accès aux soins* », Compte-rendu de la concertation du 20 juin 2020, 2020.

[990] Mise en place par la Loi de modernisation de notre système de santé de 2016.

place un projet de tablettes numériques mises aux lits des patients. Opérationnel depuis janvier 2021, ce projet a pour objectifs de : « *développer les informations données aux patients sur leur séjour et leurs droits ; permettre aux patients de rompre l'isolement et l'ennui et de garder le lien avec leurs proches ; proposer un outil de divertissement, permettant au patient un instant d'oublier sa maladie* »[991]. Cette tablette, outre l'utilité de divertissement et de lien avec les proches, est un véritable outil permettant au patient de s'informer sur ses droits mais également de répondre à certains d'entre eux. En effet, la tablette « *permet aux patients d'accéder à toutes les informations concernant leur séjour (livret d'accueil, charte de la personne hospitalisée, liste des ministres des cultes et des interprètes, documents de prévention sur la nutrition, la douleur, l'hygiène, …, le questionnaire de sortie, …), et ainsi renforcer leur droit à l'information* »[992]. De plus, elle est dotée d'« *un module "Aide à la communication"* [qui] *permet aux patients en difficulté de mieux communiquer avec l'équipe soignante* »[993].

Ces éléments d'information dématérialisés permettent au patient d'avoir une information claire loyale et accessible à toute heure, notamment concernant des informations sur sa prise en charge ou encore des éléments pour faciliter la pratique de sa religion, qui est un droit pour le patient. Cette tablette permet également au patient d'être réellement acteur de sa santé en lui permettant de « mieux » communiquer avec le personnel soignant, notamment concernant sa prise en charge.

Un retour d'expérience a été mené par l'établissement de santé au cours du premier trimestre 2021, « *86% des patients sont satisfaits des tablettes numériques* »[994]. Ce nombre montre l'importance de continuer sur cette lancée et les bienfaits de l'utilisation des nouvelles technologies au service de la santé et notamment des droits du patient.

391. **La technologie au service des droits du patient**. L'utilisation des nouvelles technologies est un réel avantage pour garantir le respect des droits du patient ; leurs possibilités sont multiples. Prenons cette fameuse tablette qui ne fait « que » informer le patient sur ses droits et lui donner quelques informations sur sa santé. Ne pourrait-on pas la coupler avec un service numérique permettant de dématérialiser les consentements du patient lors de sa prise en charge ? Ou encore implémenter des services permettant la réalisation

[991] Ministère de la santé et de la prévention, « La mise en place de tablettes numériques au lit des patients », 2021.
[992] *Ibid.*
[993] *Ibid.*
[994] *Ibid.*

d'actes de télémédecine ? Le numérique allié à la dématérialisation des données permet de garantir amplement le respect des droits des patients.

B) La dématérialisation des droits du patient au service du professionnel de santé et de l'établissement de santé

392. **L'écho des droits : les obligations**. Les droits des patients font écho inévitablement aux obligations à la charge des professionnels de santé et des établissements de santé. Le droit pour le patient d'être informé sur son état de santé fait écho à l'obligation pour le professionnel de santé d'informer ledit patient. Le droit au respect de la vie privée du patient implique l'obligation de secret professionnel pour les professionnels de santé et l'obligation pour les établissements de santé, de garantir ce secret. Aussi, il est dans l'intérêt des professionnels et des établissements de garantir le respect des droits du patient, pour ne pas voir leur responsabilité engagée. Ainsi, le simple respect du droit du patient ne suffit pas, il faut pouvoir prouver qu'il a été respecté, en cas de contentieux. Comme vu précédemment avec le e-consentement, l'utilisation d'un service numérique en santé et la dématérialisation des données permet non seulement d'informer le patient et de recueillir son consentement, mais également de se constituer des éléments de preuve en cas de contentieux pour le professionnel de santé, grâce aux informations contenues dans le service, les métadonnées créées ou encore les éléments de traçabilité, à condition bien sûr, d'utiliser un service fiable et complet.

393. **Une meilleure prise en charge du patient**. Outre la réponse à une obligation légale, le respect des droits des patients permet aux professionnels de santé de mieux prendre en charge leurs patients grâce à l'utilisation de services numériques. En effet, le patient a droit à la continuité des soins[995] mais comme on a pu le constater, la barrière séparant l'hôpital de la ville ne permet pas une continuité des soins pour le patient de manière optimale. La dématérialisation des échanges et la prolifération d'outils d'e-santé permettent d'inverser la tendance ainsi qu'une meilleure communication ville/hôpital comme ville/ville[996], favorisant la coordination des soins, ainsi que le parcours patient. La prise en charge du patient en est ainsi améliorée[997].

---

[995] C. santé publ., art. L. 1110-1 et L. 1110-3.
[996] On peut nommer les services d'e-parcours.
[997] A l'instar du DMP. Hubert BALIQUE, Gaëtan GENTILE, Stéphanie GENTILE, Bernard GIUSIANO, Maeva JEGO, Roland SAMBUC, « Prise en charge des personnes sans chez-soi : intérêt du dossier médical partagé ? », *op. cit.*

394. **Un gain de temps au profit de la prise en charge**. Ces outils permettent également un gain de temps pour les professionnels, laissant de côté une partie des tâches administratives pour se concentrer sur la prise en charge effective des patients. Un des outils les plus évidents est celui permettant la prise de rendez-vous en ligne : « *parfois laborieuse, tributaire de la disponibilité des praticiens demandés, elle se fait désormais d'un simple clic. Elle libère aussi les professionnels à la fois d'une charge financière appréciable et d'une tâche chronophage (30 à 40 % du temps de travail des praticiens est consacré à l'administratif)* »[998].

Pour autant, l'avis n'est pas unanime quant au gain de temps que procure l'utilisation de certains services numériques ; la redondance des informations à fournir au sein du service, sa complexité d'utilisation par les professionnels de santé, ou encore la multiplication des outils à utiliser peut entraîner un manque d'adhésion des professionnels, préférant revenir à la bonne vieille méthode. Là où l'outil de prise de rendez-vous en ligne fait gagner du temps aux professionnels, d'autres services lui en font perdre : « *la gestion des dossiers médicaux informatisés, la gestion des parcours de soins, la recherche documentaire, la rédaction la documentation médicale, des courriers pour les confrères, des certificats médicaux ou encore la télétransmission des documents à l'assurance maladie sont autant de tâches inhérentes à la consultation médicale, que le médecin passe les yeux rivés à son écran. Tant et si bien que les praticiens passent en effet plus de temps à saisir des données (43 % de la journée) que face à leur patient (28 %)* »[999].

§2 La dématérialisation comme obstacle au respect des droits des patients

395. **Un point de vue mitigé**. Ces chiffres montrent que, même si certains services numériques en santé permettent indéniablement de garantir le respect des droits des patients et sont de véritables atouts, tant pour le patient que pour les professionnels et établissements de santé, ces services présentent des inconvénients, et mettent également en péril le respect des droits des patients. En effet, cela a été illustré précédemment ; l'utilisation des services numériques permettent aussi bien un gain qu'une perte de temps pour le professionnel.

Il en va de même pour l'accès au soin. Certes, le respect du droit d'accès et d'égal accès aux soins, est favorisé par l'utilisation des services numériques, mais ces mêmes services

[998] Isabelle POIROT-MAZERES, « Santé, Numérique et Droit-s », *Presses de l'Université Toulouse 1 Capitole,* coll. actes de colloques de l'IFR, 2018, pp. 23-57.
[999] Caducee, « Transformation numérique des soins de santé : un gain de temps pour les médecins ? », *caducee.net,* 2021.

entraînent, *a contrario,* un frein à l'accès aux soins (A). De plus, l'utilisation des technologies de l'information et de la communication facilite la transgression de ces droits qui n'est pourtant pas à craindre lors d'une prise en charge « traditionnelle », en l'absence de toute technologie (B).

A) Les nouvelles technologies comme frein à l'accès aux soins

396. **Le numérique et l'accès aux services publics**. La dématérialisation ne concerne pas que le monde de la santé, mais est présente dans notre quotidien, y compris dans nos rapports avec les procédures et les administrations publiques. Edouard Philippe a lancé le 13 octobre 2017 le programme « Action Publique 2022 », qui avait notamment pour objectif de dématérialiser l'ensemble des services publics entre 2017 et 2022. Or cette profonde transformation, devenue nécessaire avec l'évolution de notre société, le développement du numérique, de l'intelligence artificielle et des attentes de plus en plus fortes des usagers[1000], a également conduit à l'apparition d'inégalités face à l'accès aux services publics. Dans ses rapports « *dématérialisation et inégalités d'accès aux services publics* »[1001] de 2017 et « *dématérialisation des services publics : trois ans après où en est-on* ? »[1002] de 2022, le Défenseur des droits fait état des conséquences qu'entraînent les services publics 100% dématérialisés sur les publics les plus fragiles.

397. **Le numérique : une fin en soi**. *« Le numérique, à la base un moyen, est devenu une fin en soi. Il contribue à affaiblir et décentrer l'accessibilité des services publics, et ajoute une vulnérabilité technologique par-dessus la vulnérabilité territoriale. Il peut renforcer les discontinuités et les ruptures dans l'accès aux droits »*[1003]. En effet, un des objectifs principaux du programme « Action Publique 2022 » était de permettre d'accéder aux services publics plus facilement et de n'importe où, tant pour permettre aux citoyens de répondre à leurs obligations (réalisation de sa déclaration fiscale en ligne), mais également de faciliter leur accès à des services leur permettant de faire valoir leurs droits.

Bien qu'une partie de la population puisse voir des bénéfices à la dématérialisation complète des services publics, permettant pour la plupart, un meilleur accès à ces derniers, cela a

[1000] Gouvernement, « Action Publique 2022 : pour une transformation du service public », 2021. Disponible à l'adresse : https://www.gouvernement.fr/ (consulté le 29/07/2022).
[1001] Défenseur des droits, « *Dématérialisation et inégalités d'accès aux services publics »,* Rapport, 2019.
[1002] Défenseur des droits, « *Dématérialisation des services publics : trois ans après où en est-on ? »,* Rapport, 2022.
[1003] Laura FERNANDEZ RODRIGUEZ, « quels impacts de la dématérialisation sur les droits des usagers ? », *La Gazette des communes »,* 2021. Propos de David Charbonnel recueillis lors du colloque organisé par l'Université de Lorrains le 31 mai et 1 juin dans son intervention sur les impacts de la dématérialisation.

notamment conduit à « *l'émergence d'un nouveau public vulnérable : des usagers jusqu'ici en situation d'autonomie administrative et qui sont aujourd'hui fragilisés par le passage au numérique. […] En outre, la dématérialisation peut engendrer du non recours au droit, pour plusieurs raisons (par éloignement des services, manque de maîtrise du numérique, peur de la stigmatisation, non recours volontaire par choix idéologique envers les nouvelles technologies, etc.)* »[1004]. Le public le plus impacté par ces changements est sans nul doute les personnes âgées, les étrangers, ou encore les personnes faisant l'objet d'une mesure de protection, même si tout un chacun peut se retrouver démuni face à une procédure dite « intuitive » mais qui, dans les faits, présente des difficultés de compréhension et de complétion. Seul face à son ordinateur, tout citoyen peut baisser les bras.

398. **L'accès aux services publics VS l'accès aux soins**. Cette inégalité d'accès face aux services publics peut se transposer à l'accès aux soins. Précédemment, il a été évoqué que le numérique permettait aux patients d'avoir un meilleur accès aux soins. Or, un patient, à l'instar d'un formulaire administratif dématérialisé, peut se retrouver en difficulté lors d'une téléconsultation avec son médecin par exemple. Cette difficulté peut être engendrée par l'utilisation d'un service numérique demandant une aisance avec les outils technologiques. Cette malaisance ne concerne pas que le public le plus vulnérable physiquement et psychiquement, mais le public vulnérable technologiquement. Bon nombre de patients ne sont pas à l'aise avec la technologie, y compris la population la plus jeune qui peuvent être déconcertés de voir que leur accueil et leur admission au sein d'un établissement de santé, ne se réalise pas auprès d'une personne, mais d'une tablette. Même si le numérique permet d'accéder plus facilement aux soins, on se rend compte que le numérique en tant que tel peut en être le frein. Pour lutter contre cette fracture numérique dans le cadre de « Ma Santé 2022 » et plus particulièrement le déploiement de Mon espace santé, il a été décidé de « *développer un réseau massif d'ambassadeurs, des personnes qui seront sur le terrain pour aider les Français à utiliser Mon espace santé, à comprendre à quoi sert cet outil et quels sont les enjeux liés à l'accès à leurs données personnelles* »[1005]. Cette initiative, bien que louable, ne permet d'endiguer qu'une partie des failles puisque cet accompagnement ne concerne que Mon espace santé. Or, il ne s'agit que d'une goutte d'eau dans l'océan du numérique.

[1004] *Ibid.*

[1005] Laura LETOURNEAU, « Transformations numériques et entrepreneuriales – l'improbable transformation numérique de la santé », *op. cit.*, pp. 23-30.

Outre la difficulté d'accès au service due à leur utilisation, ces services peuvent également être inaccessibles au regard du manque d'équipement numérique d'un patient, entraînant une inégalité d'accès entre les patients. « *Le baromètre numérique Arcep/Credoc établissait qu'en 2017 19 % des Français n'avaient pas d'ordinateur à domicile, 27 % n'avaient pas de smartphone. Ce baromètre indique pour 2020 que 16 % des plus de 12 ans ne sont pas équipés en smartphone, mais avec de fortes variations : c'est le cas de 45 % des non diplômés, de 34 % des retraités, de 23 % des habitants des communes rurales, et de 41 % des plus de 70 ans. 3 % de la population utilise des cartes prépayées pour ses communications par téléphone mobile. Il indique par ailleurs que 22 % des personnes ne disposent à leur domicile ni d'un ordinateur, ni d'une tablette. Là encore, le taux d'équipement le plus faible se retrouve chez les non diplômés, les habitants des communes rurales, les retraités, les plus âgés. La part de personnes ne disposant à domicile d'aucun équipement permettant d'accéder à internet (ni ordinateur, ni tablette, ni smartphone) est de 9 %.* »[1006] De plus, encore une personne sur dix, n'a pas accès à internet. Ces chiffres montrent une grande disparité entre les citoyens français, ne leur permettant pas, entre autres choses, d'avoir un accès optimal aux soins.

B) Une transgression des droits facilitée

399. **Ce que la technologie permet mais que le Droit interdit**. Les nouvelles technologies ont permis beaucoup en santé, notamment la création des services numériques en santé ou encore la dématérialisation des données, des échanges et de la prise en charge du patient. Elles ont permis et permettent toujours de faire évoluer considérablement la santé au sens large, notamment par la création des services numériques. De nombreuses start-up ont vu le jour, dont certaines ont été créées avec l'aide de professionnels de santé, qui souhaitent, par le numérique, répondre à une de leur problématique, comme un dossier patient plus adapté et performant, spécifique à leur spécialité, ou encore un système de « chat » permettant aux professionnels d'une même équipe de soins de partager des informations concernant un même patient pris en charge. Mais cette multitude de possibilités que permet le numérique, engendre également certaines dérives, pouvant entraîner notamment une violation des droits du patient.

Prenons un exemple concret : lors d'une prise en charge à domicile, un ou plusieurs professionnels de santé sont sollicités par le patient. Mais que faire si, au cours de cette prise en charge, un de ces professionnels n'est pas disponible ? Une solution numérique a été

[1006] Défenseur des droits, « *Dématérialisation des services publics : trois ans après où en est-on ? », op. cit.*

trouvée pour répondre à ce besoin : un service numérique sollicitant, dans un rayon proche du domicile du patient, un professionnel pour suppléer celui absent. Comment cela fonctionne ? Les professionnels reçoivent une alerte par le biais d'une notification sur l'application, demandant s'ils peuvent prendre ou non, en charge le patient. Si le professionnel le peut, il accepte la prise en charge et intervient auprès du patient.

Dans le principe, cet outil permet une coordination et une prise en charge optimale pour le patient, mais quid de son droit à la liberté de choix de son praticien[1007] ? Certes le patient peut donner son consentement au préalable pour l'utilisation de ce service, mais il n'aura pas choisi le professionnel de santé. Il pourra certes, refuser l'acte de soin une fois le professionnel arrivé, mais cela engendrera une perte de temps et d'argent, pour le patient ainsi que pour le professionnel, ce qui peut entraîner des conséquences sur la santé du patient.

400. **D'une transgression volontaire des droits à une transgression involontaire**. Un des droits les plus impacté par le numérique et la dématérialisation des données est bien évidemment le droit au respect de la vie privée et au secret des informations concernant un patient[1008]. Les données de santé qui sont des données personnelles, sensibles mais également intimes, doivent rester maîtrisées par le patient et ne doivent être communiquées qu'aux professionnels de santé le prenant en charge. Ce secret permet « *à un individu de pouvoir maîtriser les informations sur sa vie »*[1009] et ainsi établir la relation de confiance permettant au patient de délier sa parole. Rappelons-le, « *il n'y a pas de médecine sans confiance, de confiance sans confidence, de confidence sans secret »*[1010]. Or l'arrivée du numérique en santé vient bouleverser cette relation dualiste qu'entretien un patient avec son médecin ou même la relation que le patient entretient avec son équipe de soins, notamment lorsque des outils numériques sont utilisés. Comme vu précédemment, l'utilisation du numérique n'est pas intuitif pour tout le monde, impliquant que certains patients demandent de l'aide à leur entourage pour se connecter à leur ENS, ou encore à la plateforme numérique utilisée par les laboratoires de biologie pour avoir leurs résultats. Or la personne « aidante » aura forcément accès aux données de santé de la personne en demande, impliquant la divulgation de certaines données de santé à une personne autre qu'un professionnel de santé. Pour autant, le patient qui ne souhaitait initialement pas que ses données personnelles soient divulguées, s'y trouve de

[1007] C. santé publ., art. L. 1110-8.
[1008] C. santé publ., art. L. 1110-4.
[1009] Bruno PY, *Le secret professionnel*, l'Harmattan, coll. « La justice au quotidien », 2005.
[1010] Portes L. « Du secret médical », Communication à l'Académie des Sciences Morales et Politiques, 5 juin 1950, publiée dans son ouvrage posthume : *À la recherche d'une éthique médicale,* Masson, 1964, p. 153.

fait contraint avec l'introduction du numérique en santé et la dématérialisation des données et l'obligent en quelque sorte à partager ses informations secrètes.

Le pendant de ce droit est le devoir de secret professionnel[1011] pour tous les professionnels de santé, qui oblige les établissements de santé à fournir à leurs collaborateurs, des outils garantissant le respect de ce devoir. L'outil de travail par excellence est le dossier patient informatisé, accessible par tous les collaborateurs. Mais comment garantir que seuls les professionnels autorisés et prenant en charge le patient, accèderont aux données, si tout le monde peut y avoir accès ? D'une part, grâce à une matrice d'habilitation[1012] qui permet de définir en fonction de chaque profession, quels accès il peut avoir et quelles données il peut visualiser ; d'autre part, par des contrôles aléatoires attestant qu'aucun dossier patient n'a été consulté en dehors d'une prise en charge. Pour autant, malgré ces précautions, il est tout à fait possible pour un professionnel de santé travaillant dans un établissement de santé, d'avoir accès aux informations concernant un patient. Même si cet accès peut, par la suite être sanctionné, le « mal » sera déjà fait à l'encontre du patient, puisque ses informations auront fuité, ce qui est plus difficile lorsque le dossier est papier. Le parallèle est également possible lors d'une cyberattaque engendrant un vol de dossiers : le patient verra ses informations communiquées à d'autres personnes que ses propres soignants.

[1011] C. pén., art. 226-13.
[1012] DMP, « Matrice d'habilitation », 2022. Disponible à l'adresse : https://www.dmp.fr/ (consulté le 21/07/2022).

Section 2 : Une adaptation des droits du patient rendue nécessaire

401. **La dématérialisation comme facilitateur et comme obstacle.** Il apparaît qu'en l'état actuel, le respect des droits du patient concernant sa prise en charge est à la fois facilité et entravé par l'utilisation des nouvelles technologies. Or on l'a vu, l'utilisation des outils et services numériques « *n'est que le signe avant-coureur d'une transformation profonde de la relation médicale et de la prise en charge des patients […], qui marque tant les pratiques professionnelles que la place du patient* »[1013]. Il serait inenvisageable de ne pas penser que les droits des patients eux-mêmes, institués depuis 2002 et n'ayant pas subi, pour la plupart, de gros changements, doivent être revus, pour s'adapter aux nouvelles pratiques engendrées par le numérique (§1). Parallèlement aux droits que détient le patient sur sa prise en charge, ce dernier bénéficie d'autres droits connexes tels que son droit d'accéder à son dossier médical[1014], son droit à la rectification ou à la portabilité de ses données[1015], ou encore son droit de s'opposer à l'hébergement de ses données par un tiers[1016]. Certains d'entre eux, ont notamment été créés, « *pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…)* »[1017] et ne sont pas spécifiques à la santé, comme le RGPD. Pour autant, ce dernier s'applique également au traitement des données de santé. Le développement des nouvelles technologies engendre inévitablement la création et la modification des droits du patient et du Droit en général (§2) pour faire face aux nouveaux enjeux du numérique.

§1 Une évolution des droits du patient nécessaire par les opportunités de la dématérialisation

402. **De nouvelles perspectives**. L'apparition des outils du numérique et la dématérialisation des données dans le domaine de la santé a permis de faire évoluer la manière dont est pris en charge le patient et a ouvert de nouvelles perspectives grâce aux possibilités qu'offrent ces derniers. Cependant, certaines de ces évolutions possibles grâce au numérique ne sont pas toujours compatibles avec les droits des patients, bien qu'elles servent leur intérêt. Afin de profiter au mieux des opportunités du numérique en santé, le Droit vient

[1013] Isabelle POIROT-MAZERES, « Santé, Numérique et Droit-s », *Presses de l'Université Toulouse 1 Capitole, op. cit.*
[1014] C. santé publ., art. L. 1111-7.
[1015] 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, JOUE, L 119, 04 mai 2016, art. 44 et s.
[1016] C. santé publ., art. L.1111-8.
[1017] Cnil, « RGPD de quoi parle-t-on ». Disponible à l'adresse : https://www.cnil.fr/ (consulté le 05/03/2022).

s'adapter dès lors qu'il s'agit de l'intérêt du patient (A). Pour autant, même si une adaptation des droits des patients est déjà en cours, certains restent encore (in)adaptés à l'ère du numérique (B).

A) Une adaptation des droits du patient en cours : le secret, l'échange et le partage d'informations

403. **Le droit du choix de son praticien ou le droit du choix de son praticien ET de son équipe**. Le lien qu'entretenait le patient avec son médecin a considérablement évolué aux cours des années : initialement, la relation patient-médecin était binaire, permettant la mise en place d'un cercle de confiance, propice aux confidences puisque le médecin était tenu au secret. *« Tout secret est, par nature, un obstacle à la libre circulation de l'information »*[1018], et comme ce dernier travaillait seul, l'information était bien gardée.

Pour autant, cette relation initialement binaire a subi une mutation progressive au fil des années, notamment au regard des progrès médicaux et des différentes découvertes en la matière obligeant le médecin à ne plus travailler seul. *« L'évolution des techniques médicales […] oblige les malades à faire de plus en plus confiance, non seulement à un médecin librement choisi par eux, mais aussi à l'équipe qui travaille avec lui* »[1019]. Il apparaît que le patient a le droit de choisir son praticien[1020], mais pour autant, il ne choisit pas l'ensemble des professionnels intervenant sur sa prise en charge puisqu'il est contraint d'accepter les personnes travaillant avec ce praticien. Finalement le patient ne choisit pas simplement un praticien, mais choisit un praticien et son équipe.

Une autre situation permet de montrer les limites du droit à la liberté de choix de son praticien ; le « nouveau » mode d'exercice en société des professionnels de santé. *« Lors d'une prise de rendez-vous auprès du secrétariat de la société, voire auprès d'un standard délocalisé, y a-t-il réellement libre choix ou y a-t-il une orientation imposée au regard des disponibilités de chacun, du nombre de malades constituant la « patientèle » de chaque professionnel, des accords concernant cette clientèle ou la répartition des nouveaux patients... ? Le rendez-vous peut être pris en fonction de l'emploi du temps de chaque praticien, afin d'optimiser les plannings et le fonctionnement du cabinet : l'organisation en commun prend alors le pas sur le libre choix. Le patient ne dispose plus que d'une faculté de*

[1018] Bruno PY, « réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *RDS*, 2013, hors-série n°50, p.161.
[1019] Jean SAVATIER, note sous Trib. Civ. de la Seine, 27 juin 1956, JCP 1956, 119624.
[1020] C. santé publ., art. L. 1110-8.

refus, souvent difficile à mettre en œuvre »[1021]. Aussi, on s'aperçoit que le droit de librement choisir son praticien n'est pas pleinement respecté, pour autant, cela présente certains avantages ; en cas d'absence de son médecin « préférentiel » (vacances, maladie etc.) ou d'indisponibilité (planning complet), un autre médecin du cabinet a la possibilité de prendre en charge le patient, évitant ainsi un long temps d'attente pour le patient.

404. **L'équipe**. L'élargissement du cercle de confiance incluant en son sein le patient, le praticien, mais également son équipe, n'est que la première étape de cet élargissement. En effet, la complexité de la médecine et la multiplicité des domaines de connaissances obligent les médecins à se spécialiser (pédiatrie, cardiologie médecine générale etc.) et à se surspécialiser (par l'ajout d'une compétence particulière à leur spécialité) transformant considérablement la prise en charge des patients. Un seul médecin, ne peut pas à lui seul prendre en charge le patient, il doit s'entourer de ses confrères spécialistes : « *spécialisés, nécessairement cantonnés dans leur champ d'intervention en raison de la complexité croissante des matières dans lesquelles ils interviennent, les praticiens isolés ne peuvent plus alors fournir à leur client une prestation d'ensemble […]. Le regroupement des praticiens s'impose* »[1022]. « *Le travail en équipe est donc aujourd'hui indispensable dans le monde médical et en ce sens le colloque singulier en est inévitablement altéré au profit d'un colloque pluriel »*[1023].

405. **L'évolution du champ du secret**. Ce travail d'équipe implique inévitablement une évolution du champ du secret ; pour permettre aux différents professionnels de travailler en équipe, tous doivent bénéficier des informations concernant un patient. Ce secret, initialement « *inhérent à la relation de soins qualifiée d'intimiste, binaire, singulière et ainsi propice à l'échange d'informations scellées sous le sceau du secret* »[1024] est devenu un secret davantage collectif. Aussi, l'information donnée par un patient à un médecin est désormais « *confiée à une équipe et non au seul professionnel qui reçoit la confidence* »[1025].

406. **De l'équipe médicale à l'équipe de soins**. Mais jusqu'où s'étend le périmètre des professionnels pouvant faire partie du cercle de confiance ? Au départ une relation binaire, puis transformée en relation patient/équipe purement médicale, cette équipe est,

[1021] Marion GIRER, « Droits des patients et exercice en société », *RDSS, op. cit.*
[1022] François VIALLA, L'introduction du fonds libéral en droit positif français, Litec, Coll. Bibliothèque de droit de l'entreprise, n°39, 1999, n°84, p. 24.
[1023] Morgan GRIT, *L'équipe de soins à l'épreuve de la mobilité des systèmes d'information,* Thèse dactylographiée, Montpellier, 2021, p-20.
[1024] Morgan GRIT, *L'équipe de soins à l'épreuve de la mobilité des systèmes d'information, op. cit.* p-53.
[1025] Céline BRETON-RAHALI, *Le secret professionnel et l'action médico-sociale*, Thèse dactylographiée, Nancy, 2014, p-104.

depuis 2016[1026], une équipe de soins. En effet, l'évolution de notre système de santé, la complexité des prises en charge du patient et l'évolution des pratiques professionnelles ont conduit le législateur à ouvrir le cercle de confiance aux professionnels du secteur social et médico-social, qui ont un rôle primordial dans le parcours de soins du patient. « *La pratique a confirmé la nécessité d'une dérogation au secret au bénéfice des professionnels* [du secteur médico-social]. *Cette dérogation a conduit à l'émergence du secret partagé qui s'applique quotidiennement dans la vie professionnelle des acteurs du secteur médico-social. La pratique du secret partagé est donc incontournable pour la qualité et la continuité de l'accompagnement de l'usager »*[1027]. A ce titre, les professionnels médicaux ne sont plus les seuls dépositaires de l'information de santé. Pour autant, les non-professionnels de santé n'ont pas tous le droit d'accéder aux données. L'article R. 1110-2 du Code de la santé publique prévoit une liste limitative des professionnels pouvant échanger et partager des informations concernant une personne prise en charge : les professionnels de santé et les non-professionnels de santé tels que les assistants de service social, les ostéopathes, les psychologues, ou encore les éducateurs et aides familiaux. Malgré cette ouverture aux non-professionnels de santé, des professionnels du droit estiment que l'ouverture est encore insuffisante, oubliant des personnes, acteurs de la prise en charge du patient, mais à qui les informations de santé ne peuvent être communiquées : à titre d'exemple les aidants[1028].

407. **Et après, jusqu'où va-t-on** ? L'élargissement progressif du cercle de confiance patient-médecin devenu patient-acteurs de santé et créant la notion d'équipe de soins[1029] a permis d'améliorer considérablement la prise en charge du patient grâce à la coordination des professionnels et au partage des informations du patient. Il a été pertinent d'ouvrir ce cercle de confiance au regard des possibilités technologiques qu'offrent le

[1026] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JORF n°0022, 27 janvier 2016, texte n°1.
[1027] Céline BRETON-RAHALI, *Le secret professionnel et l'action médico-sociale, op. cit.* p-231.
[1028] Elaine BUCKI, Guillem CASANOVAS, Stéphanie LANGARD, « Les règles d'échange et de partage d'informations : aux limites de la démarche empirique », *RDS*, 2017, n° 79, p. 658.
[1029] C. santé publ., art. L1110-12 : *« Pour l'application du présent titre, l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes, et qui :*
1° Soit exercent dans le même établissement de santé, au sein du service de santé des armées, dans le même établissement ou service social ou médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret ;
2° Soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge ;
3° Soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé ».

numérique et la dématérialisation des informations. Sans cela, une ouverture du cercle de confiance aurait-elle vu le jour, sachant qu'il aurait été très difficile de s'échanger et se partager les informations ? Toujours est-t-il que l'alliance entre l'équipe de soins d'aujourd'hui et les services numériques en santé permettent une prise en charge optimisée du patient, notamment grâce à une coordination favorisée et un réel parcours de soins pour le patient.

Or l'utilisation des services numériques en santé et donc de systèmes d'informations impliquent inévitablement le concours de professionnels n'entrant pas dans le champ des professionnels listés dans l'article R. 1110-2 du Code de la santé publique et pourtant, ces derniers vont pouvoir avoir accès aux données de santé d'une personne ; sont notamment concernés les informaticiens en charge de la maintenance de l'informatique, ou encore de l'hébergeur des données de santé. Ces derniers sont également soumis au secret professionnel puisque l'article L. 1110-4 du Code de la santé publique est rédigé de telle sorte que ces professionnels soient pris en compte : le secret « *s'impose à tous les professionnels intervenant dans le système de santé »*[1030]. Cette question avait déjà été soulevée ; la Cour de Cassation a rendu un arrêt en 2008, précisant que les informaticiens, même s'ils ne sont pas des professionnels de santé, sont soumis au secret professionnel.[1031] *« Force est de constater que toute personne œuvrant de près ou de loin dans le système de santé est soumise au respect du secret des informations concernant la personne* »[1032]. Le législateur est venu adapter les contours du secret, pour y inclure les professions inhérentes aux systèmes d'informations.

408. **Les frontières de plus en plus minces**. L'implication du numérique en santé implique que les frontières du secret sont de plus en plus minces, soit à cause même des accès qu'il offre, soit par obligation lors de la maintenance opérationnelle des services numériques utilisés, si bien que le secret bien gardé de la relation dualiste patient-médecin devient accessible pour bon nombre de personnes. Pour autant, toutes les personnes acteurs du système de santé pour la prise en charge du patient, du fait de leur profession et de leur fonction sont soumises au secret professionnel. Au regard de l'inclusion de certains professionnels dans le cercle de confiance du patient, du fait de leur fonction plutôt que de

[1030] C. santé publ., art. L. 1110-4 § 1 al. 2.
[1031] Cass. Crim. 3 juin 2008, n°08-80467. En dépit de cette constatation, la Cour rejette le pourvoi lui reprochant de ne pas avoir apporté « *de charges suffisantes contre quiconque d'avoir commis les délits reprochés, ni toute autre infraction* ».
[1032] Morgan GRIT, *L'équipe de soins à l'épreuve de la mobilité des systèmes d'information, op. cit.* p-77.

leur profession, le principe du secret professionnel « *pourra un jour conduire à préférer la notion de secret fonctionnel* »[1033].

B) Les droits du patient (in)adaptés à l'ère du numérique

409. **Une adaptation inadaptée**. La quantité de professionnels intervenant lors de la prise en charge d'un patient, que ce soit pour des questions médicales, informatiques ou administratives augmente de plus en plus obligeant le législateur à, comme on a pu le constater précédemment, adapter le Droit actuel pour prendre en compte ces mutations en cours.

Or, ces adaptations nécessaires, à l'ère du numérique, viennent au détriment d'un droit fondamental du patient, le droit au secret de ses informations. En effet, peut-on encore qualifier ces informations de secrètes alors même qu'une multitude de personnes peuvent y avoir accès, qui plus est, des personnes qui ne prennent pas le patient en charge ? Les bienfaits de la coordination, du parcours de soins et l'utilisation du numérique pour la prise en charge du patient sont-ils à ce point bénéfiques pour entraver ainsi un droit fondamental du patient ?

La réponse à la première question est mitigée. Il n'est plus possible d'envisager la notion de secret de la même manière qu'initialement, un secret entre deux personnes, c'est-à-dire quelque chose qui doit être tenu caché. Aujourd'hui, il faut entendre cette notion comme une « *discrétion,* [un] *silence qui entoure quelque chose »*[1034] et *« qui n'est connu que d'un nombre limité de personnes »*[1035] ne devant pas être divulgué à d'autres, permettant ainsi de partager l'information entre professionnels, mais dans un cercle plus ou moins restreint. La complexité est de fixer la limite de ce cercle afin de ne pas laisser la porte ouverte aux dérives. Cependant, même si le législateur a limitativement identifié les professionnels pouvant échanger et partager des informations de santé concernant une personne prise en charge, il n'en est rien des autres professionnels accédant à ces mêmes données par nécessité fonctionnelle. Une formulation générale permet « juste » de leur imposer le secret professionnel. Il est regrettable de ne pas avoir davantage de précisions.

La réponse à la seconde question est indéniablement oui, puisque le développement du numérique tend à s'accroitre de plus en plus permettant de nouvelles perspectives pour la prise en charge du patient, dans une optique simple : améliorer la prise en charge. Le

[1033] Bruno PY, Le secret professionnel, *op. cit.*
[1034] Larousse, *V° « secret »*, adj.
[1035] TLFi, *V° « secret »*, adj.

législateur doit ainsi jongler entre « *le nécessaire respect du secret professionnel et la transmission indispensable des informations aux différents acteurs de soins* »[1036] et plus généralement du système de santé, tout en respectant le droit au secret des informations du patient.

410. **La dévalorisation du secret professionnel ?** Finalement, l'élargissement du champ des personnes pouvant entrer dans le cercle de confiance, grâce, mais aussi à cause du numérique, implique que bon nombre de personnes vont pouvoir avoir accès aux données de santé du patient. Ces autorisations d'accès sont ni plus ni moins que des dérogations au principe du secret professionnel. *« Au premier regard,* [on pourrait] *penser qu'il s'est produit un renforcement de la protection des informations confidentielles : les catégories professionnelles soumises au secret se multiplient, les interprétations jurisprudentielles semblent protectrices. Mais une analyse plus globale conduit au contraire à observer qu'en systématisant les exceptions et dérogations, le secret professionnel est aujourd'hui considérablement dévalorisé ; un peu comme les assignats, présentés initialement comme une forme moderne de richesse, dont la trop large diffusion a progressivement détruit la valeur. Le secret autrefois fort, qualifié parfois même d'absolu, se fragilise au risque de disparaître »*[1037]. L'inclusion du numérique en santé et la volonté toujours plus grande d'impliquer le maximum de professionnels dans la prise en charge du patient vient certes, améliorer sa prise en charge, mais au détriment du droit au secret de ses informations, dévalorisant la portée autrefois si emblématique du secret professionnel. Pourtant, il ne faut pas oublier que même si par principe, davantage de personnes peuvent techniquement accéder aux données, ces dernières n'y accèdent pas toutes ; pour y accéder, les professionnels doivent avoir un motif légitime, tel que la prise en charge du patient. Ainsi, le secret professionnel perd de sa valeur par rapport à autrefois en ce sens que le secret n'est plus seulement connu d'un patient et de son médecin, mais d'un patient et de l'équipe entourant le médecin (voire les médecins), équipe qui n'est plus seulement médicale. Les risques de divulgation, même accidentels, sont dès lors davantage présents.

De plus, les cas de dérogations du secret professionnel ne cessent de se multiplier[1038] : l'obligation de signalement de certaines maladies, la levée du secret au nom de la sécurité

[1036] Caroline ZORN-MACREZ, *Données de santé et secret partagé : pour un droit de la personne à la protection de ses données de santé partagées*, *op. cit.*
[1037] Bruno PY, « Cent ans de secret professionnel », *RDS*, 2021, n°100, pp. 230-250.
[1038] *Ibid.*

sanitaire, ou encore la divulgation en cas de péril imminent. Autant de dérogations fragilisant le principe même du secret professionnel.

411. **Un consentement toujours libre et éclairé ?** Le recueil du consentement du patient par voie dématérialisée est un enjeu de taille aujourd'hui et tend à se développer et se généraliser. Comme cela a pu être démontré, il permet de tracer l'identité du patient et recueillir son accord par l'apposition d'une signature électronique ; la date et l'heure du consentement sont clairement établies, il est possible d'y insérer des éléments d'informations afin de pouvoir prouver que le consentement est bien éclairé puisqu'une information a été fournie. En soi, le droit au consentement n'a pas subi de changement depuis l'implémentation du numérique, ce dernier vient justement garantir le respect des critères libres et éclairés du consentement. En revanche, ce consentement dématérialisé ne présente-t-il pas certains risques ? En effet, *« les innombrables formulaires relatifs aux cookies nous poussent à banaliser nos choix numériques. On clique par habitude, par lassitude, pour gagner du temps, sans réfléchir. Si nous faisons de même pour une intervention qui engage notre pronostic vital, le consentement sera vidé de son sens* »[1039] bien qu'en apparence, le consentement recueilli de manière dématérialisée réponde aux deux critères. Ne faudrait-il pas en ajouter un autre pour garantir le consentement du patient afin de prendre en compte l'utilisation du numérique ? Si oui, quel critère ajouter ? Un consentement libre, éclairé et réfléchi ? Il serait très difficile d'évaluer la qualité de la réflexion d'une personne et ce serait une démarche très hasardeuse. N'est-il pas mieux de privilégier l'effort sur l'ergonomie et les fonctionnalités de l'outil utilisé pour garantir un recueil du consentement non automatisé ? Cela passerait notamment par des actions du patient sur le service de recueil du consentement, comme remplir un questionnaire s'assurant que l'information a bien été comprise, ou encore recueillir la signature du patient par voie électronique. Ces éléments permettent de montrer que le patient n'a pas été passif et n'a pas simplement coché une case pour valider son consentement à l'instar des cookies. En l'espèce, le patient serait véritablement actif.

412. **Le consentement, le non-consentement ou le refus d'utiliser la dématérialisation**. L'autre problématique du consentement dématérialisé est le suivant : si le consentement dématérialisé est généralisé, est-ce que l'absence de consentement du patient signifie qu'il refuse la prise en charge ? En effet, le service de recueil de consentement permet, comme son nom l'indique, de recueillir le consentement. Mais si un patient n'a pas

[1039] Charles-Clémens RULING, « santé : un consentement numérique peut-il être « libre et éclairé » ? », *Grenoble école de management*, 2022.

rempli son formulaire de consentement, est-ce qu'il refuse la prise en charge ou refuse-t-il simplement le recueil du consentement par voie dématérialisée ? Rappelons-le, bon nombre de personnes n'ont pas internet, ne bénéficient pas d'accès à des outils tels qu'un ordinateur ou un smartphone, ou bien ne les maîtrisent pas. Pour toutes ces personnes, le recueil du consentement par voie dématérialisée semble compromis. Or ce n'est pas parce qu'elles ne peuvent, ou ne veulent pas donner leur consentement par voie dématérialisée, qu'elles refusent la prise en charge en tant que telle.

Il est donc impératif de mettre en place dans ces services de recueil du consentement, la possibilité pour le patient de refuser la prise en charge, transformant le formulaire de consentement, en formulaire de non-consentement. Cela permettrait d'une part, de s'assurer que le patient refuse bien la prise en charge et non l'utilisation du numérique, d'autre part, de prouver que le patient a refusé la prise en charge et, pour finir, d'établir que l'absence de retour de ce formulaire signé signifie que le patient n'a pas eu accès à ce formulaire ou qu'il refuse sa dématérialisation. Dans ce dernier cas, une procédure dégradée doit pouvoir être mise en place afin de recueillir le consentement du patient afin de ne pas entraver l'accès et l'égal accès à ses soins.

Doit-on ajouter au sein du Code de la santé publique que le recueil du consentement par voie dématérialisée doit permettre également de signifier son refus, ou en tous cas, que le professionnel de santé doit impérativement s'assurer que le patient a bien eu la possibilité de consentir ? Cela reviendrait à complexifier une procédure qui se veut être simplificatrice, d'autant que cela relève du bon sens. Pour autant, même si le Droit ne le dit pas clairement, il serait pertinent que l'usage en fasse une règle d'or afin que le patient ne soit pas lésé dans sa prise en charge.

§2 La création de nouveaux droits/Droits inhérents aux nouvelles technologies

413. **Une mutation du Droit en perspective ?** Le numérique et la santé font partie intégrante de notre système de santé actuel impliquant la mise en place de garde-fous juridiques pour encadrer ces « nouvelles » pratiques. Concernant le droit des patients, on se rend compte que l'implication du numérique n'a pas engendré beaucoup de modifications, sauf concernant le secret des informations concernant un patient pris en charge et les conditions d'échange et de partage d'informations, même si quelques précisions ou ajouts pourraient être souhaitables. Qu'en est-il du Droit en général ? Les dispositions sont-elles suffisantes ou faut-il créer un Droit spécifique au numérique (A) ? En l'état actuel des choses,

même si le Droit au numérique n'est pas imminent, une mutualisation du Droit pourrait déjà être un premier pas (B).

A) Un droit relatif au numérique, un Droit à part entière

414. **Un Droit du numérique**. Existe-t-il aujourd'hui un droit du numérique ? Le droit du numérique n'est pas un droit en tant que tel à l'instar du droit civil, du droit pénal ou du droit de la santé, mais est le rassemblement de plusieurs de ces droits. Le droit du numérique rassemble le droit des données, le droit du commerce électronique, le droit des contrats, l'open data, la propriété intellectuelle, ou encore le droit de la cybersécurité, si bien que des masters complets sont destinés à former les juristes de demain sur ce droit à part entière[1040].

La difficulté de ce droit est qu'il est très disparate, dans le sens où un seul code ne rassemble pas tous les principes généraux, mais qu'il puise sa source dans tous les textes juridiques, toutes les jurisprudences touchant de près ou de loin au numérique. Il est la partie du droit qui régit les nouvelles technologies, y compris lorsque celui-ci est associé à un autre droit, à l'instar du droit de la santé lorsqu'un service numérique entre en jeu.

Serait-il envisageable et souhaitable d'avoir un code du numérique ? Souhaitable, oui, pour simplifier son application ; envisageable, à court terme, non. En effet, le droit du numérique est en plein essor et en constante mutation, il permet en l'espèce, d'inclure toutes les nouvelles dispositions applicables aux nouvelles technologies. C'est ainsi qu'est applicable la Loi informatique et liberté[1041], la Loi pour la confiance dans l'économie numérique[1042], ou encore la Loi pour une République numérique[1043]. Toutes ces Lois viennent régir un domaine particulier sur lequel le numérique a un impact. Comment envisager qu'un seul code puisse être applicable à toutes les disciplines sachant que le numérique n'est à la base qu'un outil, un moyen de parvenir à ses fins. On voit pour autant que cela n'est plus tout à fait vrai, par exemple avec le développement de l'Intelligence Artificielle, qui est une discipline purement numérique.

[1040] On peut citer en exemple le master mention droit du numérique parcours-types droit numérique, IA de l'Université Toulouse 1, le master droit du numérique de l'Université de Lille ou encore le master 2 droit du numérique de L'université de Rennes 1.

[1041] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[1042] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1), JORF n°0143, 22 juin 2004, texte n°2.

[1043] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235, 8 octobre 2016, texte n°1.

En tout état de cause, le droit du numérique tend à se développer de plus en plus avec la parution systématique de nouvelles dispositions entrant dans le champ du numérique, dont les dernières en date sont la Loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public[1044], ou encore la Loi visant à renforcer la régulation environnementale du numérique par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse[1045].

415. **La création de nouveaux droits.** Outre la création quasi-constante de nouvelles dispositions sur le droit du numérique, les droits des personnes de manière générale sont impactés puisque son utilisation implique de « *dégager de nouveaux droits (par exemple, l'accès aux données, leur durée de conservation, l'accessibilité des personnes handicapées, etc.)* »[1046]. Prenons l'exemple du droit à l'accessibilité numérique : l'article 47 de la Loi pour l'égalité des droits et des chances[1047] ainsi que son décret d'application[1048] prévoient que tous les services publics numériques ainsi que certains services privés numériques doivent être accessibles de manière équivalente à tout citoyen, impliquant qu'ils doivent également être accessibles aux personnes en situation de handicap (visuel, moteur, auditif etc.). Ce droit à l'accessibilité des services numériques est un nouveau droit créé, au regard de l'utilisation du numérique.

Ainsi, le Droit et notamment les droits des personnes évoluent, se créent en fonction des besoins, et des développements du numérique, y compris pour répondre à des problématiques qui ne se posaient pas à l'ère du non-numérique.

416. **Vers un Droit à l'Internet**. Même si le droit du numérique est encore en construction, il apparaît que de nombreuses dispositions permettent de l'encadrer. En revanche, pour qu'un pays comme la France puisse prétendre à un Etat 100% dématérialisé ou encore, à plus petite échelle, à un service public ou encore à un établissement de santé 100% dématérialisé, encore faut-il que chaque citoyen puisse avoir accès à Internet. Or aujourd'hui en France, le droit à l'Internet n'existe pas réellement.

[1044] Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public**,** JORF n°0053, 4 mars 2022, texte n°1.
[1045] Loi n° 2021-1755 du 23 décembre 2021 visant à renforcer la régulation environnementale du numérique par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (1), JORF n°0299, 24 décembre 2021, texte n°2.
[1046] Yannick GIRAULT, « La dématérialisation au service de la performance de l'administration », *Gestion & Finances Publiques*, 2017, n°6, pp. 81-83.
[1047] Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées (1), JORF n°36, 12 février 2005, texte n°1.
[1048] Décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne, JORF n°0171, 25 juillet 2019, texte n°38.

En effet, pour pouvoir utiliser des services numériques quels qu'ils soient, un accès à Internet est essentiel surtout lorsque qu'il est imposé d'utiliser ces services pour s'acquitter de ses devoirs, comme la déclaration d'impôts. Aujourd'hui, l'accès à Internet devient aussi vital que l'accès à l'eau ou à l'électricité. « *La loi pour une République numérique reconnaissait déjà, théoriquement, un droit au maintien de la connexion Internet, pour qu'un client dans l'incapacité de payer puisse bénéficier d'un maintien de sa connexion Internet, sur le modèle des fournitures en eau, électricité et téléphone, les expérimentations des départements restaient timides sur le sujet, avec en pionniers les départements de Haute-Saône, Marne et Seine-Saint-Denis en 2017* »[1049]. Ce droit à l'Internet n'est aujourd'hui pas suffisamment adapté pour maintenir la connexion Internet de la population.

A l'occasion du 117ème congrès des notaires sur le thème « le numérique, l'Homme et le droit »[1050], des propositions ont été soumises afin *« d'accompagner et sécuriser la révolution digitale »*[1051] en cours. Parmi ces propositions figurent[1052] :

i. Faire de l'accès à internet un droit fondamental.

ii. Qualifier d'indispensables et rendre insaisissables les outils permettant de se connecter à internet : « *Le numérique est omniprésent dans tous les aspects de nos vies : l'accès à la santé se fait via des applications, la consultation et la gestion des opérations bancaires en ligne se généralise, l'immatriculation des véhicules est totalement dématérialisée, l'accès à la culture pour les jeunes majeurs se fait pas un « Pass Culture » accessible via une application dédiée... Les outils numériques et en particulier la tablette, l'ordinateur ou le téléphone permettent de se connecter à internet pour effectuer toutes ces démarches et favorisent une insertion minimale de l'individu dans une société ultra connectée. Les créanciers d'un débiteur peuvent toutefois recouvrer leur créance sur ces outils indispensables à l'existence dématérialisée de l'individu car ils ne figurent pas dans la liste des biens déclarés insaisissables fixée par le Code de procédure civile d'exécution. Puisque les outils permettant de se connecter à internet sont désormais indispensables à l'existence de l'individu et à son*

[1049] Laura FERNANDEZ RODRIGUEZ, « quels impacts de la dématérialisation sur les droits des usagers ? », *op. cit.*
[1050] Anne BERDAH, Olivier BOUDEVILLE, Manuella BOURASSIN, Pascale BURGAUD, Elisabeth DUPART-LAMBLIN, Stéphanie GAILLARD-SEROUGNE, Olivier HERRNBERGER, Lionel MONJEAUD, « *Le numérique, l'Homme et le droit – accompagner et sécuriser la révolution digitale* », Rapport du 117ème congrès des notaires de France, 2021.
[1051] Rédaction LEXTENSO, « « Le numérique, l'Homme et le droit » : les propositions du 117e congrès sont présentées ! », *Defrénois*, coll. la revue du notariat, 2021, n°DEF203C4, p.5.
[1052] *Ibid.*

action dans la vie sociale, il convient de les rendre insaisissables au même titre que les biens nécessaires à la vie et au travail du débiteur saisi et de sa famille »[1053].

Une proposition de Loi constitutionnelle pour une nouvelle démocratie citoyenne et participative[1054] enregistrée à la Présidence de l'Assemblée nationale le 10 novembre 2021 propose « *d'inscrire le droit d'accès à Internet dans la Constitution »*[1055] française, à l'instar d'autres pays de l'Union Européenne comme l'Estonie.

D'autres idées peuvent-être envisagées ; ne pourrait-on pas s'inspirer de ce qui a déjà été fait dans d'autres domaines ? En effet, en l'absence d'une ligne téléphonique, il est tout de même possible d'appeler les numéros d'urgence. Il pourrait être envisageable de transposer ce principe en fournissant un accès à certains sites alors même que la personne ne bénéficie pas de connexion internet, tels que les sites gouvernementaux, nécessaires à la réalisation d'actes administratifs obligatoires, à l'instar de la déclaration d'impôt. Cette solution permet certes de pallier l'absence de connexion internet, mais pas l'absence d'outil informatique.

Nous pouvons le constater, le Droit à l'Internet pour toute personne est le premier pas indispensable vers le tout numérique.

B) Une mutualisation du Droit souhaité ?

417. **La problématique actuelle**. Le Docteur en droit Bénédicte Bévière-Boyer a exposé plusieurs problèmes juridiques sur le développement du numérique en santé, notamment la multiplicité des règles de droit, d'autant plus que tous les domaines du droit sont impactés par le numérique. « *Toute la question est de savoir si le droit, tel qu'il existe aujourd'hui, est suffisant ou s'il convient de l'adapter, de le transformer, de le compléter. Le premier réflexe de nombre de juristes est de considérer que le droit actuel est suffisant. Pourtant, peu à peu se développe le droit du numérique en santé, notamment les règles portant sur la protection des données (RGPD), le système national des données de santé (SNDS), le Health Data Hub, la télémédecine ou encore l'article 11 du projet de loi de bioéthique portant sur le principe de garantie humaine* »[1056.] Comme on a pu le voir, il apparaît que le droit actuel n'est pas à lui seul suffisant puisque bon nombre de dispositions

[1053] *Ibid.*
[1054] Proposition de Loi Constitutionnelle pour une nouvelle démocratie citoyenne et participative, enregistré à la Présidence de l'Assemble nationale le 10 novembre 2021 (n°4661).
[1055] *Ibid.*
[1056] Aurélie PASQUELIN, « Droit et éthique du numérique en santé : « une exigence absolue, la protection de l'humain » », *Hospitalia,* 2021.

voient le jour dans tous les domaines, y compris dans celui de la santé, rendant très difficile l'application du droit au regard de sa quantité et donc de sa complexité d'application.

« Paradoxalement, dans le même temps, un lobbying important milite en la nécessité de privilégier le droit souple. Les professionnels et les entreprises de la santé doivent donc à la fois prendre en considération un code de la santé publique de plus en plus imposant, et répondre aux régulations du droit souple qui deviennent tentaculaires. Au final, cette situation pénalise les entreprises et les professionnels, mais aussi les patients qui se trouvent au cœur du dispositif de santé. Le millefeuille des régulations devient un réel fardeau »[1057].

418. **Nemo censetur ignorer lege**. Qui ne connaît pas le célèbre adage « nemo censetur ignorare lege », « nul n'est censé ignorer la Loi », pourtant, il est bien impossible de connaître l'intégralité des textes de loi, y compris pour les juristes les plus érudits, « *avec, au 25 janvier 2019, environ 318 000 articles législatifs et réglementaires en vigueur en France* »[1058], sans compter les principes jurisprudentiels. Pour autant, un citoyen ne peut se défendre en prétextant la méconnaissance de la Loi et cela, pour garantir le bon fonctionnement de l'ordre juridique.

A travers les développements de ce travail de recherche, a été mis en avant le droit applicable pour garantir la valeur probante d'un document, dont les règles juridiques tirent leur fondement : du code civil, du code de la santé publique et plus particulièrement des référentiels sécurité et interopérabilité établis par l'ANS, mais également du code pénal, de la Loi informatique et liberté et des recommandations de la Cnil ainsi que du code du patrimoine. Et cela ne concerne que la partie garantissant la valeur probante même d'un seul document dématérialisé. Comment s'y retrouver alors que les sources juridiques sont aussi disparates.

Un code rassemblant l'intégralité de ces règles n'est pas envisageable puisque des dispositions très spécifiques au domaine de la santé doivent être respectées. Mais quelle solution fournir sachant que certains de ces textes sont davantage techniques que juridiques[1059] ? A l'heure actuelle, une des pistes à envisager est, pour le domaine de la santé, de créer un document permettant d'indiquer aux professionnels de manière générale, les textes applicables pour un domaine donné, par exemple, un corpus documentaire permettant d'établir des liens vers les dispositions juridiques applicables pour la mise en place d'un

[1057] *Ibid.*
[1058] Vie publique, « Que signifie « nul n'est censé ignorer la loi » ? », *Fiche thématique*, 2021.
[1059] Par exemple les référentiels sécurité et interopérabilité de l'ANS.

service numérique en santé. Or cette solution n'est pas optimale, car suppose une mise à jour régulière pour que ce corpus ne soit jamais obsolète et surtout, ne puisse pas concerner le numérique en santé de manière générale ; une solution est d'utiliser le numérique pour automatiser la modification du corpus documentaire selon les évolutions juridiques.

Pour l'heure, la mutualisation des efforts et le travail d'équipe est la clé pour la transformation d'un établissement en 100% numérique. La mutualisation : pourquoi repartir de zéro sur un projet de dématérialisation alors qu'un autre établissement de santé a déjà mis quelque chose de similaire en place ? Et pourquoi ne pas mutualiser les efforts ; les établissements pourraient s'allier dans le but de dématérialiser. Cela permettrait un gain de temps, financier et permettrait une homogénéisation entre les différents établissements. Travail d'équipe : le numérique en santé n'est pas qu'une question de droit, c'est un enjeu social mais également technique y compris dans l'application des règles de droit. Un juriste seul ne peut pas mettre en place une dématérialisation, même partielle d'un établissement, c'est un travail d'équipe !

Conclusion du chapitre. Les droits des patients sur leur prise en charge, n'ont pas subi de grandes transformations depuis 2002, si bien que la garantie de leur respect face au développement du numérique en santé permet, soit de le favoriser, soit au contraire de l'entraver. Pour autant, on constate petit à petit que le Droit est en mutation, y compris concernant les droits du patient, pour venir les adapter face aux nouveaux enjeux du numérique, à l'instar du droit au respect du secret des informations concernant un patient. Mais en soi, les droits du patient n'ont pas besoin de subir un toilettage complet. Quelques adaptations ou encore des recommandations d'application suffisent à répondre aux nouvelles problématiques engendrées par le numérique.

En revanche, le numérique en santé et la dématérialisation des données entraînent la création de nouveaux droits pour les patients lors de leur prise en charge médicale, à l'instar du droit de portabilité[1060] ou encore le droit à l'accessibilité des services numériques aux personnes en situation de handicap[1061]. Finalement, c'est le Droit en général qui est en constante évolution pour faire face aux nouvelles questions de Droit qu'engendre le numérique, tant dans le domaine de la santé, que dans tous les domaines concernés.

Qu'en est-il des règles concernant la déontologie médicale face au numérique ? *« Il en ressort, après examen de chaque article au prisme du numérique, que le code n'exige pas de réforme approfondie. Il est adapté au développement du numérique en santé, sous réserve d'en faire une lecture souple, une interprétation ouverte. Il est clair que le numérique bouge les lignes, mais ce sont surtout l'organisation des soins et les pratiques professionnelles qui sont bousculées »*[1062]. Il a été envisagé de créer un code de e-déontologie pour l'usage des nouvelles technologies mais *« il est apparu plus opportun et suffisant de s'appuyer sur le cadre déontologique existant »*[1063]. La plupart des articles du code de déontologie n'ont pas vocation à être modifiés, cependant des clarifications seront apportées en commentaire, notamment pour aider à leur application. En revanche, un nouvel article 13-1 sera créé au sein du code de déontologie médicale afin de le dédier à la e-santé. « *Même si le numérique ne pose pas des questions déontologiques inédites,* [le Cnom a pensé] *utile d'introduire un*

[1060] 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, JOUE, L 119, 04 mai 2016, art. 20.
[1061] Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées (1), JORF n°36, 12 février 2005, texte n°1, art. 47.
[1062] Lina WILLIATTE, « Santé : la révolution numérique – Le droit dit et l'éthique invite au questionnement », *Médecins – le bulletin de l'ordre national des médecins,* 2022 (numéro spécial), p.14.
[1063] Anne-Marie TRARIEUX (Dr), « Santé : la révolution numérique – Donner un cadre déontologique à l a e-santé », *Médecins – le bulletin de l'ordre national des médecins,* 2022 (numéro spécial), p.18.

article spécifique pour [s']*assurer que le virage majeur que constitue le numérique sera suffisamment pris en compte et encadré* »[1064].

Conclusion du titre. En l'état actuel des choses, même si le numérique et la dématérialisation vont parfois entraver les droits des patients, de manière générale ils permettent davantage de favoriser leur application et leur respect. Ainsi, les patients voient leurs droits sur leur prise en charge garantis. La dématérialisation des droits des patients est également avantageuse pour les professionnels et les établissements de santé, puisque d'une part, cela permet de mieux prendre en charge la personne et d'autre part, de pouvoir fournir des preuves en cas de contentieux. C'est du gagnant-gagnant, sous réserve d'utiliser le numérique et de dématérialiser conformément au Droit et aux règles de l'art. Or, cela ne dépend pas que des professionnels et des établissements de santé, mais aussi des industriels.

En effet, ce sont les industriels qui sont en première ligne ; pour qu'un patient, un professionnel de santé ou un établissement de santé utilise un service numérique, il faut que ces services existent. Les industriels sont donc les premiers concernés par la législation applicable ; ils doivent fournir des services conformes au Droit et notamment aux droits des patients, mais également des services bénéfiques et efficaces pour les professionnels, les établissements de santé et surtout, pour les patients. En revanche, même si le devoir des industriels est de fournir des services numériques conformes au Droit, il est également de la responsabilité des professionnels et des établissements de santé de s'assurer qu'ils sont réellement conformes. Pour autant, s'agissant des services à usage exclusif des usagers, il est difficile de leur imposer la même rigueur de contrôle, au regard de la complexité du Droit en la matière. Aussi, les industriels doivent, tant au regard de leur éthique que de leurs obligations professionnelles, garantir des services numériques fiables et conformes au Droit.

Les industriels ont aujourd'hui un rôle important à jouer et leur implication va conduire à créer de nouveaux droits pour le patient usager : *« 20 ans après la loi Kouchner, l'éthique du numérique pourrait créer de nouveaux droits pour les usagers de la santé, garantissant le « bien agir » des industriels et start-ups du numérique en santé vis à vis des citoyens, comme la loi Kouchner a garanti en 2002 le « bien agir » des médecins et de l'ensemble des professions de la santé envers les patients »*[1065]. En effet, il est impératif d'imposer un contrôle strict des services numériques en santé avant leur mise sur le marché, au regard des

[1064] *Ibid.*

[1065] Pierre SIMON (Dr), « Comment 20 ans après la loi Kouchner, l'éthique du numérique rejoint l'éthique médicale ? Le Docteur Pierre SIMON nous explique », *ManagerSante*, 2022, n°53.

données sensibles qui y seront traitées et des conséquences préjudiciables pour le patient en cas de fuite ou perte de données. Ce contrôle *a priori* est le gage d'une fiabilité en amont de tout traitement de données.

Conclusion de la partie. La dématérialisation et l'utilisation des services numériques en santé au sein d'un établissement de santé permettent incontestablement une meilleure prise en charge des patients et un meilleur respect de leurs droits grâce aux opportunités rendues possibles par les nouvelles technologies.

Pourquoi une meilleure prise en charge ? La dématérialisation des données permet l'émergence de services numériques qui ont pour objet :

i. De faciliter la prise en charge des patients, grâce aux outils de télémédecine ;

ii. De faciliter la coordination des professionnels de santé afin de prendre en charge le patient de manière collégiale, favorisant son parcours de soins. Les services permettant cela sont multiples : le DPI, interne aux établissements de santé ; les outils de parcours de soins, à l'instar de Parceo, un service de e-Parcours[1066] ; la messagerie sécurisée de santé.

iii. De créer de nouveaux services nécessaires à la prise en charge du patient tels que le ROR[1067] ; des services de visioconférence sécurisés permettant la réalisation de réunions à distance entre professionnels afin qu'ils puissent échanger des informations médicales en toute sécurité ; des services de partage d'imagerie (à l'instar de Krypton, le service du GRADeS ESEA de Nouvelle-Aquitaine).

Pourquoi un meilleur respect des droits du patient ? Car la dématérialisation des données permet de répondre aux enjeux liés à ses droits :

i. Ses droits à l'accès et notamment l'égal accès aux soins facilité par la télémédecine. Les patients isolés au sein d'un désert médical peuvent aujourd'hui avoir accès à un médecin, y compris à des spécialistes ;

ii. Ses droits à l'information et au consentement, d'autant plus respectés lorsqu'un service de recueil du consentement dématérialisé est utilisé.

[1066] Pulsy, « Parcours », disponible à l'adresse : https://www.pulsy.fr/ (consulté le 23/08/2022). Parceo, proposé par le GRADeS Pulsy est « *le service régional e-Parcours du Grand Est. Il offre aux acteurs de santé un bouquet de services numériques de coordination, facilitant la prise en charge du patient et de l'usager dans son parcours de soins* ».

[1067] Ministère de la santé et de la prévention, « Le répertoire national de l'offre de santé et d'accompagnement médicosocial – ROR – un socle d'informations utiles sur l'offre de santé », 2022. Disponible à l'adresse : https://solidarites-sante.gouv.fr/ (consulté le 26/07/2022). Pour rappel, le ROR est un répertoire opérationnel des ressources qui est « *un référentiel recensant l'ensemble de l'offre sanitaire et médico-social, et comprenant un volet sur la disponibilité des lits en établissement de santé* ».

De manière générale, la dématérialisation permet au patient de mieux gérer sa santé, notamment grâce aux outils lui permettant d'avoir accès directement à ses résultats de biologie, ou ceux lui permettant de trouver un professionnel de santé, de voir ses disponibilités et pouvoir prendre rendez-vous directement en ligne, sans passer par le secrétariat ou encore les services lui rappelant qu'il est nécessaire qu'il aille consulter tel ou tel spécialiste.

Pour autant, il faut tout de même garder à l'esprit les risques potentiels du numérique en santé, notamment un risque éthique, la déshumanisation de la santé : *« au-delà du « patient numérique » saura-t-on encore reconnaître les singularités et les vulnérabilités humaines, les incertitudes et les discriminations qui menacent notamment lorsque l'appariement de fichiers produit des données préjudiciables au respect de la sphère privée et plus encore aux droits fondamentaux. […] Agnès Buzyn invoque à juste titre à « un humanisme dans le numérique, un numérique incarné par des humains ». ».*[1068] Ne perdons pas de vue que même si numérique et dématérialisation permettent une meilleure prise en charge du patient et un meilleur respect de ses droits, il ne faut pas oublier que le patient est humain, et qu'il ne faut pas le traiter comme une machine, réduit à être un simple numéro.

[1068] Emmanuel HIRSCH, « Espace numérique en santé : qu'en sera-t-il du patient numérique ? », *Espace éthique – Ile-de-France,* 2009.

CONCLUSION GENERALE

419. La dématérialisation au sein des établissements de santé présente de nombreux avantages tant pour l'établissement, pour les professionnels de santé que pour les patients. Son avantage le plus évident et le plus pertinent est évidemment une meilleure prise en charge du patient, en son sens général.

Pour autant, même si sa pertinence n'est en aucun cas remise en cause, sa mise en place au sein des établissements de santé peut présenter des controverses ; comment garantir que la dématérialisation des données de santé n'est pas préjudiciable malgré les bénéfices évidents ? En d'autres termes, les bénéfices dépassent-ils les risques ? Tout au long des développements, il a été établi que la dématérialisation présente un réel potentiel pour le système de santé en général, à condition de respecter le Droit applicable en la matière, afin de garantir d'une part, la valeur et la force probante des données dématérialisées, et d'autre part la prise en charge optimisée du patient. Mais la complexité du Droit en la matière ainsi que son application présentent de réelles difficultés pour les établissements de santé et sont un défi de taille à relever ; la dématérialisation des données de santé[1069] est *« un véritable casse-tête pour les établissements et les professionnels. Ceux qui s'y confrontent trouvent un cadre juridique compliqué et instable que nous sommes tentés de qualifier de réglementation surréaliste »*[1070].

Pour aboutir à la dématérialisation totale d'un établissement de santé, il est impératif de travailler en équipe au sein d'un même établissement (informaticiens, professionnels de santé, direction, ressources humaines, juristes), et de mutualiser les efforts entre les différents établissements de santé. Il serait notamment souhaitable de pouvoir s'appuyer sur des institutions nationales pour aider à la mise en place d'un processus de dématérialisation

[1069] La dématérialisation des données de santé présente un enjeu majeur pour le système de santé, mais les textes juridiques encadrant cette pratique sont nombreux et très difficiles à concilier et à accorder. Comme l'a très justement évoqué Claire DEBOST (Claire DEBOST, « La donnée de santé à l'ère du numérique », RDS, 2016, hors-série 50e numéro, pp. 94-107), *« nous assistons depuis quelques années, en droit de la santé, à l'émergence d'un corpus normatif dédié à la dématérialisation des données de santé. Pour autant, l'articulation de différentes normes, à savoir la loi Informatique et Libertés, la loi relative aux droits des patients et ses nombreux décrets d'application, n'est pas sans poser de difficultés. Cette réglementation éparse manque de cohérence et nuit à sa juste application par les acteurs du sec. […] Il est vrai que l'appréhension par le droit de faits techniques nouveaux incite à des évolutions législatives incontournables, mais on ne peut que déplorer leur méthode d'élaboration au coup par coup conduisant à multiplier les antinomies textuelles ».*

[1070] Caroline ZORN-MACREZ, « « CHRONIQUE MARTIENNE », DES DONNEES DE SANTE NUMERISEES. Brèves observations sur une réglementation surréaliste », *RDS*, 2010, n°36, p. 331.

comme l'ANS ou encore l'ANSSI afin de garantir que la dématérialisation mise en place au sein d'un établissement, est conforme aux exigences actuelles.

La dématérialisation et les services numériques sont l'avenir de notre système de santé, et il est impératif d'accompagner les établissements de santé en ce sens d'autant plus que le développement constant du numérique en santé et des technologies en général vont conduire à de nouvelles pratiques. Un accompagnement national est dès lors fortement souhaité pour faire face aux nouveaux enjeux liés à la dématérialisation et au numérique. « *On assiste d'ores et déjà à une mutation sous-jacente des métiers de la santé qui joue tout à la fois sur le contenu même des missions ou leurs outils, comme sur les modes de collaboration. La place du médecin en particulier est désormais clairement interrogée, que certains prédisent leur fin ou d'autres annoncent un changement profond dans leur rôle auprès des patients. Cette place du médecin est appelée à évoluer à trois niveaux : dans son rapport à la technologie qu'il sera appelé à utiliser de plus en plus, dans sa relation aux autres intervenants autour du patient, dans sa relation au patient. […] Les métiers eux-mêmes sont appelés à se diversifier, en un double mouvement : d'une part par les montées en compétences des professions paramédicales, portées par la télémédecine, la « pratique avancée » et le recours à des techniques facilitant certains actes autrefois fortement spécialisés et complexes (75% des pratiques médicales d'aujourd'hui pourraient être transférées en 2050 à des professions de santé non médicaux) ; et d'autre part, en raison de l'intégration nécessaire dans les processus de soins de plus en plus d'ingénieurs et techniciens de la santé, des bio informaticiens aux datascientit. […] Il faut également imaginer que bien des métiers de la santé sont en train d'émerger en lien notamment avec la télémédecine ou les plateformes à haut débit, dont nous n'anticipons qu'une partie. Pierre Simon*[1071] *cite ainsi comme exemples dans le champ de la santé, le coordonnateur de télémédecine, le chirurgien superviseur de robot en télé-chirurgie ou l'ingénieur qualité en e-santé et dans celui des sciences sociales et humaines, le métier de psychotechnicien(ne) en télémédecine et d'éthicien(ne) des algorithmes et des robots »*[1072]. Ces évolutions à venir, liées à la dématérialisation auront de nombreux impacts sur la prise en charge du patient et sur le Droit applicable en la matière, y compris sur les droits des patients.

[1071] Ancien président de la Société française de télémédecine, Paris.
[1072] Isabelle POIROT-MAZERES, « Santé, Numérique et Droit-s », *Presses de l'Université Toulouse 1 Capitole, op. cit.*

BIBLIOGRAPHIE

1. Ouvrages généraux et spéciaux

BABINET Olivier, **ISNARD BAGNIS** Corinne, *La e-santé en question(s)*, Hygée éditions, 2020.

BERTIER-LESTRADE (de) Bérénice, *Les affres de la qualification juridique – La frontière entre l'acte juridique et le fait juridique*, Presses de l'Université Toulouse 1 Capitole, mars 2018.

DE FONTETTE François, *Vocabulaire juridique*, Que sais-je coll., Presses Universitaires de France, 1994.

LABBEE Xavier, *Introduction générale au droit – pour une approche éthique*, Presses Universitaires du Septentrion, 2010.

MARTIN Dominique et **TABUTEAU** Didier, « 18. Les droits des personnes malades », François Bourdillon éd., *Traité de santé publique*, Lavoisier, 2016.

MISTRETTA Patrick, *Le droit pénal médical*, LGDJ, 2013.

MOUGENOT Dominique, *Droit des obligations – La preuve*, Larcier, 2002.

MOULIN Thierry et **SIMON** Pierre, *Télémédecine et télésoin – inclus 100 cas d'usage pour une mise en œuvre réussie*, Elsevier Masson, 2021.

NETTER Emmanuel, *Numérique et grandes notions du droit privé – la personne, la propriété le contrat.*, Ceprisca, coll. Essais, 2019.

PASCON Jean-Louis, **MORAND-KHALIFA** Nathalie et **RIETSCH** Jean-Marc, *Mise en œuvre de la dématérialisation – De l'étude préalable à la certification du système*, Dunod, 2010.

POIROT-MAZERES Isabelle, « Santé, Numérique et Droit-s », *Presses de l'Université Toulouse 1 Capitole*, coll. actes de colloques de l'IFR, 2018.

PORTES L., « Du secret médical », Communication à l'Académie des Sciences Morales et Politiques, 5 juin 1950, publiée dans son ouvrage posthume : *À la recherche d'une éthique médicale*, Masson, 1964.

PY Bruno, *Le secret professionnel*, L'Harmattan, coll. « La justice au quotidien », 2005.

RENARD Isabelle et **RIETSCH** Jean-Marc, *Aide-mémoire de droit à l'usage des responsables informatique*, Dunod, 2012.

SABOURIN Jean-Luc, « L'établissement, la transmission et la conservation des informations juridiques », *UNJF*.

SCHWAB Klaus, *La quatrième révolution industrielle*, Dunod, 2017.

VIALLA François, *L'introduction du fonds libéral en droit positif français*, Litec, Coll. Bibliothèque de droit de l'entreprise, n°39, 1999, n°84.

2. Thèses et monographies

BRASSELET Renato, *La circulation de la donnée à caractère personnel relative à la santé, - disponibilité de l'information et protection des droits de la personne,* Thèse dactylographiée, Nancy, 2018.

BRETON-RAHALI Céline, *Le secret professionnel et l'action médico-sociale*, Thèse dactylographiée, Nancy, 2014.

CASSAR Bertrand, *La transformation numérique du monde du droit,* Thèse dactylographiée, Strasbourg, 2020.

CIPERE Sébastien, *Un système de médiation distribué pour l'e-santé et l'épidémiologie*, Thèse dactylographiée, Clermont-Ferrand, 2016.

DEBOST Claire, *Les technologies de l'information et de la communication et la relation de soins : invariances et inconstances*, Thèse dactylographiée, Montpelier, 2014.

DIONE Albert Ndiack, *Les aspects juridiques de la dématérialisation des documents du commerce maritime*, Thèse dactylographiée, Paris, 2018

GRIT Morgan, *L'équipe de soins à l'épreuve de la mobilité des systèmes d'information,* Thèse dactylographiée, Montpellier, 2021.

LANGARD Stéphanie, *Approche juridique de la télémédecine – entre Droit commun et règles spécifiques*, Thèse dactylographiée, Nancy, 2012.

LARSEN Raphaël, *Traçabilité et intégrité de l'information au sein de systèmes critiques : analyse et proposition de méthodes statistiques,* Thèse dactylographiée, Nantes, 2022.

LE GOUES Morgan, *Le consentement du patient en droit de la santé,* Thèse dactylographiée, Avignon, 2015.

OLECH Valérie, *Le secret médical et les technologies de l'information et de la communication,* Thèse dactylographiée, Nancy, 2019.

VOILLEMET Agathe, *L'usage de la donnée médicale – Contribution à l'étude du droit des données,* Thèse dactylographiée, Lille, 2022.

ZORN-MACREZ Caroline, *Données de santé et secret partagé - Pour un droit de la personne à la protection de ses données de santé partagées*, Thèse dactylographiée, Nancy, 2009.

3. Articles, notes, observations et commentaires de jurisprudence

ABALLEA Thierry, « La signature électronique en France, état des lieux et perspectives », *Dalloz,* 2001, n°35.

ABDESSELAM Stéphanie, **GAILLARD** Laetitia, **KADAR** Daniel, « Données de santé : un vecteur d'innovation sous trop haute surveillance ? », *RJSP*, juin 2021, n°21.

AGOSTI Paul et **CAPRIOLI** Éric, « Principales évolutions du régime de la signature, du cachet et de la copie numérique », *AJC,* octobre 2016.

ALBERT Eric et **HAVRYLCHYK** Olena, « L'argent liquide disparaîtra un jour, mais pas tout de suite », *Le monde,* 2022.

ANCEL Pascal et **FIEVEE** Alexandre, « Contrat et immatériel – Rapport Luxembourgeois », *Travaux de l'Association Henri CAPITANT Bruylant,* 2014, tome LXIV.

ARFI-ELKAIM Dahlia, « e-mails, SMS, captures d'écran des réseaux sociaux : quelle valeur probante ? », *JDB Avocats*, 2018.

BALIMA Serge Théophile, « Une ou des « sociétés de l'informatique » ? », *Hermès, La Revue,* 2004/3, n°40.

BALIQUE Hubert, **GENTILE** Gaëtan, **GENTILE** Stéphanie, **GIUSIANO** Bernard, **JEGO** Maeva, **SAMBUC** Roland, « Prise en charge des personnes sans chez-soi : intérêt du dossier médical partagé ? », *Santé Publique,* 2018/2, vol. 30.

BANAT-BERGER François, « De l'écrit à internet : comment archive-t-on l'immatériel ? », *Pouvoirs*, 2015/2, n°153.

BANAT-BERGER Françoise, **CANTEAUT** Anne, « Intégrité, signature et processus d'archivage », *INRIA*, 2013.

BANAT-BERGER Françoise et **MEISONNIER** Antoine, « La gestion des archives dans le secteur médical à l'ère numérique », *Médecine & Droit*, 2015, vol. 2015, Issue 131,

BASTIAN Marie, « e-Santé : où est le droit ? », *SIH Solutions*, 2019.

BAUJARD Corinne et **BEN HAMOUDA** Iman, « La gestion du projet à l'Hôpital : dossier patient informatisé et qualité de soins », *Recherches en Sciences de Gestion*, 2015/4, n°109.

BEJEAN Mathias, **KLETZ** Frédéric et **MOISDON** Jean-Claude, « Création de valeur organisationnelle et technologies de l'information à l'hôpital : le cas du dossier patient informatisé », *Gestion et Management Public*, 2018/2, vol. 6/n°4.

BERG-MOUSSA Alexandra et **RAZAVI** Mahasti, « Publication de l'ordonnance portant réforme du droit des contrats », *AD article*, 2016.

BERGOIGNAN-ESPER Claude, « Le consentement médical en droit français », *Laennec*, 2011/4, tome 59.

BERNELIN Margo, « Le référentiel d'identification électronique en santé approuvé », *Editions Législatives*, 2022.

BIGLE Polyanna,

- « Archivage électronique : le Luxembourg précurseur », *Lexing*, 2015.
- « Quand la numérisation de document intègre le droit français », *Lexing*, 2017.

BIGOT Rodolphe, « Le secret médical à l'épreuve du numérique », *BJDA*, 2021, n°75.

BLANCHARD Manon, « Données de santé : une définition, trois critères », *Desmarais avocats*, 2018.

BLERY Corinne, « Communication par voie électronique », *Dalloz action Droit et pratiques de la procédure civile »*, 2021-2022.

BONDU Nicolas et **SOLER** Marc (Dr.), « Chronique Estonienne chapitre II », *Innovation e-santé*, 2018.

BONNIOL Vincent, **GANNE** Madeline, « Protéger le secret du dossier médical hospitalier :

une utopie ? », *RDS*, 2016, n°71.

BOUGHRIET Nora, SAISON-DEMARS Jeanne, « Les notes personnelles des médecins : un point d'incertitude dans la détermination du contenu transmissible du dossier », *RGDM*, 2014, n°53.

BOUTEILLE Magali, « La preuve de l'information », *RDS*, 2007, n°19.

BRETHES Jean-Paul, « La télécopie : 150 ans d'histoire (1843-1993) », *Réseaux, communication – technologie - société*, volume 11, n°59, 1993. Droit et communication.

BRIENT Isabelle, « Dossier médical perdu ou incomplet : renversement de la charge de la preuve », *village-justice*, 2018.

BUCKI Elaine, **CASANOVAS** Guillem, **LANGARD** Stéphanie, « Les règles d'échange et de partage d'informations : aux limites de la démarche empirique », *RDS*, 2017, n° 79.

CABUT Sandrine, et **SANTI** Pascale, « Droit des malades : les vingt ans d'une révolution inachevée », *Le Monde*, 2022.

CALVET Florence, **DEMONCHAUX** Jean-Paul, **LAMAND** Régis et BORNERT Gilles, « La brève histoire de la colombophilie », *Revue historique des armées*, 2007.

CAPRIOLI Éric**,**

- « Cadre juridique de l'archivage et régime juridique des tiers archiveurs », *Caprioli Associés*, 2013.
- « L'archivage des documents électroniques », *Caprioli Associés*, 2013.
- « Le juge et la preuve électronique. Réflexions sur le projet de Loi portant adaptation du droit de la preuve aux technologies de l'informations et relatif à la signature électronique », *Caprioli Associés*, 2014.

CAPRIOLI Éric et **CANTERO** Isabelle, « Traitement et hébergement de données de santé : entre protection et risques », *Revue pratique de la prospective et de l'innovation,* 2021, n°2.

CASSAR Bertrand, « Données – Gouvernance des données », *Répertoire IP/IT et Communication*, 2022.

CASSUTO Thomas, « Signature électronique des décisions juridictionnelles rendues en matière civile : nouvel arrêté », *Dalloz actualité*, 2020.

CAUVIN Emmanuel, « Loi du 13 mars 2000 sur la preuve électronique : le grand bug (législatif) de l'an 2000 », *village justice*, 2010.

CAZEIN Françoise, **CHE** Didier, **DUBOIS** D., **DURAND** Julien, **LOT** F., **LUCAS** E., « e-DO : retour sur le déploiement en ligne pour l'affection par le VIH et le sida », *Revue d'Epidémiologie et de Santé Publique,* 2018.

CHARBONNEAU Cyrille et **PANSIER** Frédéric-Jérôme, « La dématérialisation des données médicales et les enjeux de leur hébergement », *La gazette du Palais,* 2002, n°351.

CHERIF Anaïs et **MANIERE** Pierre, « L'Estonie, royaume du tout numérique », *La Tribune,* 2018.

CHOCQUE Jean-Claude, « Impacts et enjeux de l'informatisation dans le système de santé », *Gazette du Palais*, 2000, n°293.

CHOMIAC DE SAS Pierre-Xavier, « La signature scannée et sa valeur juridique », *PCS Avocat*, 2018.

CORTHESY Bastien « Le nombre de Mails envoyés par jour en 2021 », *Le monde du mail,* 2021.

COURY Annelore, **PON** Dominique, « Accélérer le virage numérique – rapport final », *Stratégie de transformation du système de santé,* 2018.

DEBOST Claire,

- « La donnée de santé à l'ère du numérique », RDS, 2016, hors-série 50^{e} numéro.
- « Les établissements de santé dans le viseur du ministère pour imposer la MSSanté », *RDS,* 2015, n°64.

DEBOST Claire, **BOURRET** Rodolphe, **MARTINEZ** Éric et **VILLA** François, « La télémédecine, lecture contingente d'un cadre juridique invariant », *RDS,* 2014, n°58.

DECHAMPS Thomas et **SADUTTO** Maurizio, « Les applications e-santé sont-elles fiables ? », *RTBF,* 2022.

DE LA MARDIERE Christophe, « Dématérialisation de la preuve : la facture électronique », *Gestion & Finances Publiques*, 2017/6, n°6.

DE LAMBERTRIE Isabelle, « Qu'est-ce qu'une donnée de santé ? », *RGDM, num. spé. « Le droit des données de santé »,* LEH, 2004.

DUBOURG Christian,

- « Copie fidèle + copie durable = copie fiable », *spark archives,* 2017.

- « La norme NF Z42-026 pour détruire le document papier original numérisé fait-elle loi ? », *spark archives,* 2017.
- « Introduction à la force probante des documents de santé », *spark archives,* 2020.

DUCHENE Céline, « Question du secret partagé », *Encyclopédie des collectivités locales,* 2020.

DUGUE-CHAUVIN Emmanuelle, « Droit du travail : une signature scannée apposée sur une contrainte a-t-elle une valeur juridique ? », *emo avocats,* 30 juin 2020.

DUPONT Marc, « Dossier médical – Dossier en établissement de santé. Dossier dématérialisé », *Droit médical et hospitalier,* Litec, fasc. 10-20, 2022.

DUPUY Olivier,

- « La signature électronique et la communication des données de santé informatisées », *RDS,* 2006, n°9.
- « La réforme des règles de durée de conservation des dossiers médiaux gérés par les établissements de santé », *RDS,* 2006, n°11.

DUROX Solenne, « L'Estonie concilie e-santé et sécurité », *La Gazette des communes,* 2018.

EL AIBA Sami et **MAILLET** Perrine, « Le droit de la santé à l'heure des nouvelles technologies », *Affiches parisiennes,* 2022.

EON Florence, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS,* 2019, hors-série.

FERNANDEZ RODRIGUEZ Laura, « quels impacts de la dématérialisation sur les droits des usagers ? », *La Gazette des communes »,* 2021.

FERRAND Frédérique, « Preuve », *Répertoire de procédure civile – Dalloz,* 2013 (actualisation 2022).

GARAUD Eric, « Quelle valeur accorder à la copie fidèle et durable… d'un écrit imparfait ? », *Dalloz,* 2013, n°15.

GAVANON Isabelle, « Blockchain, PI et mode : enjeux de la blockchain au regard des règles relatives à la preuve électronique », *Dalloz,* 2019.

GENTILHOMME Rémy, « Dématérialisation, oui, mais…», *Defrénois,* 2012, n°19.

GIRAULT Yannick, « La dématérialisation au service de la performance de l'administration », *Gestion & Finances Publiques,* 2017, n°6.

GIRER Marion,

- « Droits des patients et exercice en société », *RDSS,* 2014.
- « A la recherche du juste consentement en matière de soins », *Les cahiers de la justice,* 2021/4, n°4.
- « La loi n°2002-303 du 4 mars 2002 et les droits individuels des patients, vingt ans après », 2022, n°107.

GRIT Morgan, « La naissance de deux actes de télémédecine en EHPAD », *RDS,* 2017, n°78.

GRUSON David, « Saurez-vous décrypter les enjeux santé de demain ? », *MSN Connect,* 2022.

GRYNBAUM Luc, « Preuve », *Répertoire de droit commercial »,* 2010 (actualisation en octobre 2020).

GUIGUE Marion, PONSEILLE Anne, « Condamnation de l'obstétricien pour altération d'un document concernant un délit pour faire obstacle à la vérité », *RDS,* 2012, n°49.

HAAS Gérard et **SOUYRIS** Jean-Philippe, « Qu'est-ce qu'une copie numérique fiable ? », *HAAS avocats,* 2017.

HIRSCH Emmanuel, « Espace numérique en santé : qu'en sera-t-il du patient numérique ? », *Espace éthique – Ile-de-France,* 9mais 2009.

HUET Jérôme, « Efficacité d'une signature scannée », *RDC,* 2021/1, n°117m1.

INCONNU Amandine, « Quel est le rôle de la secrétaire médicale au sein d'un cabinet médical ? », *Le blog du Centre Européen de Formation,* mai 2018.

JAUNAIT Alexandre « Comment peut-on être paternaliste ? Confiance et consentement dans la relation médecin-patient », *Raisons politiques,* 2003/3, n°11.

JEROME Benjamin, « L'Estonie, paradis du tout-numérique », *Le Parisien Week-end,* 2018.

JOBIN Pierre-Gabriel, « L'influence de la doctrine française sur le droit civil québécois : Le rapprochement et l'éloignement de deux continents », *Revue internationale de droit comparé,* 1992.

JONQUET Olivier, « Les GHT : de quoi s'agit-il ? Le point de vue d'un médecin et universitaire », 2019, n°92.

KORSIA-MEFFRE Stéphane, « HTA : une célèbre application mobile pour iPhone mésestime les chiffres tensionnels », *VIDAL,* 2016.

LABBÉE Xavier, « L'hologramme, la téléprésence et l'être immatériel », *LPA* 20 sept. 2012, n° 264.

LANCRY Pierre-Jean, « Le médicament - Médicament et régulation en France », *Revue Française des Affaires Sociales,* 2007/3-4.

LARDEUX Gwendoline, « Preuve : modes de preuves », *Répertoire de droit civil,* 2019.

LE DEUFF Olivier, « Contrôle des métadonnées et contrôle de soi », *Etudes de communication,* 2011/1, n°36.

LE QUELLENEC Eric, « Généralisation de l'e-prescription avec l'ordonnance du 18 novembre 2020 », *Lexing*, 2019.

LEROY Aurélie, **RIOU**, Christine et **SCHOENZETTER-LAUTE** Julie, « Procédure d'élimination des dossiers médicaux », Journal de Gestion et d'Economie Médicales, 2017/1 (Vol.35).

LETOURNEAU Laura, « Transformations numériques et entrepreneuriales – l'improbable transformation numérique de la santé *», Le journal de l'école de Paris du management,* 2022, n°155.

LORIEAU Sophie, « Consentement écrit du patient égaré tout n'est pas perdu ! », *MACSF,* 2020.

LUCAS (Dr) Jacques, « Le partage des données personnelles de santé dans les usages du numérique en santé à l'épreuve du consentement exprès de la personne », *Ethics, Medicine and Public Health,* 2017, vol 1.

MACRON Alain, « Loi de modernisation de notre système de santé et partage d'informations de données de santé : consécration du secret partagé tous azimuts », *RDS,* 2016, n°74.

MADAY Charlotte, « Autorisation d'élimination d'archives et vérification d'archives et vérification du représentant du contrôle scientifique et technique », *spark archives.*

MAILLE Pablo, « En France, l'administration sert l'Etat, en Estonie elle sert le citoyen », *Usbek & Rica »,* 2018.

MALONE Antoine, « Innovations en santé publique, des données personnelles aux données massives (Big Data) », *Ethique biomédicale et normes juridiques*, Dalloz 2018.

MARTIN Laure, « e-consentement : pour une meilleure information du patient », *Mind Health,* 2021.

MEISSONNIER Antoine et **ROQUES** Rémy, « L'archiviste, les normes et le droit », *Gazette des archives,* 2015, n°240.

MIGNOT Marc, « Commentaire article par article de l'ordonnance du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations (XIII) », *actu-juridique,* mai 2016.

MISTRETTA Patrick, « La loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. Réflexions critiques sur un droit en pleine mutation », *JCPG,* 2002, doctr. 141.

MORALY Jessica, et **TORELLI,** Marie « Référentiel sur l'identification électronique : ce qui change pour la e-santé », *HAAS Avocats,* 2021.

MORLET-HAIDARA Lydia, « L'espace numérique de santé : une création de la loi relative à l'organisation et à la transformation du système de santé », *Journal du Droit de la Santé et de l'Assurance-Maladie,* 2019/3, n°24.

NICOD Marc, *Les affres de la qualification juridique,* Presses de l'Université Toulouse 1 Capitole, 2018.

NYS Jean-François, « La télémédecine, simple évolution ou véritable révolution des usages dans le système de santé français ? », *Marché et organisations,* 2020/2, n°38.

OLECH Valérie, **PY** Bruno, « La loi 24 juillet 2019 et le virage numérique, le DMP de troisième génération et l'espace numérique », *RDS*, 2019, n°92.

PAPIN Etienne, « De la disparition de la signature et des mutations de la preuve écrite », *village justice,* 2021.

PARROT Jean, « Le dossier pharmaceutique ou la réussite d'un projet mené par une profession », *Les tribunes de la santé,* 2011/3, n°32.

PASQUELIN Aurélie, « Droit et éthique du numérique en santé : « une exigence absolue, la protection de l'humain » », *Hospitalia,* 2021.

PETRA, « La prescription « dématérialisée » : un droit et non une obligation pour le citoyen », *recip-e,* 2021.

PIERRAT Emmanuel, « La validité juridique des copies numériques », *lagbd,* 2017.

PY Bruno,

- « Réquisitoire contre l'expression de secret médical : plaidoyer pour l'expression de secret professionnel », *RDS*, 2013, hors-série n°50.
- « Cent ans de secret professionnel », *RDS*, 2021, n°100.
- « Le secret professionnel est-il un droit du patient ? », *RDSS*, 2022, n°02.

RAYMOND Gérard, « Le patient acteur de sa santé », *Bull. Acad. Méd ?*, 2013, n°8.

Rédaction LEXTENSO, « « Le numérique, l'Homme et le droit » : les propositions du 117e congrès sont présentées ! », *Defrénois*, coll. la revue du notariat, 2021, n°DEF203C4.

RENARD Isabelle,

- « Valeur juridique d'une copie numérisée ? Peut-on ou non détruire l'original papier ? », *LegalTech*, 2016.
- « Droit de la preuve », *LegalTech*, 2016.

ROCHFELD Judith, « Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique », *RTD civ.*, 2000.

ROSSIGNOL Guy, « Soigner au-delà des frontières. La télématique au service de la santé mondiale », *ADSP* déc. 1998, n° 25.

RULING Charles-Clémens, « santé : un consentement numérique peut-il être « libre et éclairé » ? », *Grenoble école de management*, 2022.

SAVATIER Jean, note sous Trib. Civ. de la Seine, 27 juin 1956, JCP 1956, 119624.

SEBAI Jihane, « La e-santé et le patient 2.0 : la colonisation démocratique ! », *Marché et organisations*, 2020/2, n° 38.

SIMON Pierre (Dr),

- « Ne confondons pas les services de l'e-santé avec les pratiques professionnelles de télésanté », *telemedaction*, 2019.
- « Comment 20 ans après la loi Kouchner, l'éthique du numérique rejoint l'éthique médicale ? Le Docteur Pierre SIMON nous explique », *ManagerSante*, 2022, n°53.

TABUTEAU Didier, « e-santé et nouvelles technologies », *Les tribunes de la santé*, 2010, n°29.

TRARIEUX Anne-Marie (Dr), « Santé : la révolution numérique – Donner un cadre déontologique à l a e-santé », *Médecins – le bulletin de l'ordre national des médecins,* 2022 (numéro spécial).

VALLUET Nicolas, « Présentation générale des nouvelles technologies de communication et d'information », *LPA* 06 nov. 1996, n° 134.

VIALLA François,

- « Existe-t-il des notes personnelles ? Points de vue divergents », *RDS*, 2005, n°2.
- « Brèves remarques sur la *nouvelle* charte de la personne hospitalisée », *RDS*, 2006, n°12.
- « Explication de texte : qu'est-ce que le consentement éclairé ? – CA Toulouse, 25 octobre 2010, n°508, 10/01705 », *RDS*, 2011, n°39.
- « Bref retour sur le consentement éclairé », *Recueil Dalloz*, 2011.
- « La défaillance dans l'information : une faute d'humanisme », *RJOI*, n°16, 2013.

VIBOUD Olivier, « e-administration », *Dictionnaire d'administration publique,* 2014.

VIDAL Pierre-Laurent,

- « Le patient : unique bénéficiaire du secret médical », *RDS*, 2012, n°46.
- « La signature d'un consentement éclairé n'est ni nécessaire ni suffisant pour apporter la preuve du respect de l'obligation d'information du patient », *RDS*, 2014, n°60.

WILLIATTE Lina, « Santé : la révolution numérique – Le droit dit et l'éthique invite au questionnement », *Médecins – le bulletin de l'ordre national des médecins,* 2022 (numéro spécial).

ZORN-MACREZ Caroline,

- « CHRONIQUE MARTIENNE », DES DONNEES DE SANTE NUMERISEES. Brèves observations sur une réglementation surréaliste », *RDS*, 2010, n°36.
- « Les « notes personnelles » du médecin ? : les conséquences d'un décret d'arrière-garde », *RDS*, 2012, n° 49.

4. Colloques, conférences, communications, études, contributions à des ouvrages collectifs et rapports

Afnor, *Prestations de numérisation fidèle de documents sur support papier,* 2021, disponible à : http://cdn.afnor.org/download/reglements/FR/REGNF544.pdf

ANAES, *Dossier du patient : réglementation et recommandations,* 2003, disponible à : http://www.has-sante.fr/.

ANAP,

- *Zéro papier pour soigner : pourquoi ? Comment ?,* 2017, disponible à : https://ressources.anap.fr/
- *Comprendre les problématiques d'un projet de Dossier Patient Informatisé et Interopérable*, 2015, disponible à : https://ressources.anap.fr/

ANNSI,

- *Une année 2021 marquée par la professionnalisation des acteurs malveillants,* 2021, disponible à : https://www.ssi.gouv.fr/
- *Rapport sur l'état de la menace cyber sur les établissements de santé,* 2021, disponible à : https://www.ssi.gouv.fr/
- *Règlement EIDAS – champ d'application et destinataires,* disponible à : https://www.ssi.gouv.fr/
- *Référentiel Général de Sécurité,* disponible à : https://www.ssi.gouv.fr/

ANS,

- *Qu'est-ce que le corpus documentaire de la PGSSI-S ?,* 2021, disponible à : http://esante.gouv.fr/
- *Ce que la e-santé fait pour vous,* disponible à : http://esante.gouv.fr/
- *La petite histoire de la e-santé,* 2021, disponible à : http://esante.gouv.fr/
- *Cartes de Professionnels de Santé,* disponible à : http://esante.gouv.fr/
- *e-CPS,* disponible à *:* http://esante.gouv.fr/
- *Référentiel force probante des documents de santé – Document introductif*, PGSSI-S, 2021.
- *Référentiel force probante des documents de santé – Annexe 1 – Socle commun de principes techniques et organisationnels*, PGSSI-S, 2021.
- *Référentiel force probante des documents de santé – Annexe 2 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation,* PGSSI-S, 2021.
- *Référentiel force probante des documents de santé – Annexe 3 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques*, PGSSI-S, 2021.

- *Référentiel force probante des documents de santé – Annexe 4 – Mécanismes de sécurité à mettre en œuvre dans le cadre de la matérialisation des documents de santé numériques,* PGSSI-S, 2021.
- *Référentiel force probante des documents de santé – Annexe 6 – Classification des documents de santé,* PGSSI-S, 2021.
- *HDS – certification Hébergeur de Données de Santé,* disponible à : http://esante.gouv.fr/
- *Feuille de route « accélérer le virage numérique en santé,* 2020, disponible à : http://esante.gouv.fr/
- *e-prescription,* Doctrine technique du numérique en santé soumise à concertation, version novembre 2020, disponible à : http://esante.gouv.fr/
- *PGSSI-S,* disponible à : http://esante.gouv.fr/
- *Référentiel d'identification électronique – usagers »,* PGSSI-S, 2022.
- *Référentiel d'identification électronique – acteurs des secteurs sanitaire, médico-social et social [personnes physiques],* PGSSI-S, 2022.

Archives de France, « *autoriser la destruction de documents sur support papier après leur numérisation – quels critères de décision ? »,* Vade-mecum du Service interministériel des Archives de France, 2014.

Assurance Maladie,

- « *Améliorer la qualité du système de santé et maîtriser les dépenses »,* Rapport au ministère chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et des produits de l'Assurance Maladie au titre de 2020 (loi du 13 août 2004), 2019.
- *Le Dossier Médical Partagé (DMP) en pratique,* 2022, disponible à https://www.ameli.fr/

BAGARRY Delphine, « *Maillage territorial et accès aux soins »,* Compte-rendu de la concertation du 20 juin 2020, 2020.

Banque Centrale Européenne, *« Study on the payment attitudes of consumers in the euro area (SPACE)* », Etude, 2020.

BEORCHIA Sylvain, « e-Médecine, e-santé et informatique – entre espoirs technologiques et désillusion humaniste », *Hegel,* 2017, n°4.

BERDAH Anne, **BOUDEVILLE** Olivier, **BOURASSIN** Manuella, **BURGAUD** Pascale, **DUPART-LAMBLIN** Elisabeth, **GAILLARD-SEROUGNE** Stéphanie, **HERRNBERGER**

Olivier, **MONJEAUD** Lionel, « *Le numérique, l'Homme et le droit – accompagner et sécuriser la révolution digitale »,* Rapport du 117ème congrès des notaires de France, 2021.

BOYER Louis (Pr), *Démographie médicale radiologique en France*, JFR de printemps – Nimes, 2019.

BUZYN Agnès, « *Discours »,* Inauguration de la Paris Healthcare Week, 2018.

BUZYN Agnès, **LETOURNEAU** Laura, **PON** Dominique, « *Feuille de route « accélérer le virage numérique » »,* Dossier d'infirmation – conférence ministre, 2019.

CNOM,

- « *Dématérialisation des documents médicaux »,* Rapport, 2010.
- « Santé connectée – De la e-santé à la santé connectée », *Livre Blanc du Conseil national de l'Ordre des médecins,* 2015.
- *Recueillir le consentement de mon patient,* 2019, disponible à : https://www.conseil-national.medecin.fr/
- *Le dossier du patient,* Information, 2022, disponible à : https://www.conseil-national.medecin.fr/

Conseil supérieur du notariat, « Les notaires avancent avec vous », *Rapport annuel,* 2015.

Cour des comptes, « *La dématérialisation des prescriptions médicales : un facteur d'efficience du système de santé, des chantiers ambitieux à faire aboutir* », Rapport, 2021.

Défenseur des droits,

- « *Dématérialisation et inégalités d'accès aux services publics »,* Rapport, 2019.
- « *Dématérialisation des services publics : trois ans après où en est-on ? »,* Rapport, 2022.

FALQUE-PIERROTIN Isabelle, « Forum des droits sur l'internet : rapport d'activité – année 2005 », *Forum des Droits sur l'Internet,* décembre 2005.

GOUJON Yaël et **TOURNIER** Jérôme, « Nous les européens. Le coronavirus #etaprès ? Serons-nous tous fichés », *Reportage France 3,* 2020.

Harris interactive, « *Baromètre : les français et la téléconsultation – vague 2 »,* Enquête Harris Interactive pour Livi, 2020.

HAS,

- *Les conditions de mise en œuvre de la télémédecine en unité de dialyse médicalisée*, Recommandations en santé publique - Synthèse et recommandations, 2010.
- *Délivrance de l'information à la personne sur son état de santé*, Recommandation de bonne pratique, 2012.
- *Prise en charge médicamenteuse,* 2013, disponible à : https://www.has-sante.fr/
- *E-santé,* 2016, disponible à : https://www.has-sante.fr/
- *Droits des usagers : Information et orientation,* 2020, disponible à : https://www.has-sante.fr/

Institut Montaigne, « *e-santé : augmentons la dose ! »,* Rapport juin 2020, 2020.

JARDRY Jean-Pierre (Dr), *« Renforcer le lien ville hôpital »*, Rapport de la FEMAS, 2018.

KASPERSKY, *« Telehealth take-up : the risks and opportunities »,* Healthcare report 2021, 2021.

KERKOUR, Tom « Les cyberattaques contre les établissements d santé ont doublé en 2021 », *Le Figaro,* 2022.

Leem, « Santé 2030 : quels défis pour la santé de demain ? », *Analyse prospective de l'innovation en santé,* 2019.

LE VAN KY Etienne, « Protection des données : comment l'Estonie est devenue la référence de la cybersécurité », *Nice Matin,* 2021.

LOCARCHIVES, « Numérisation fidèle & destruction des originaux », *livre blanc,* 2017.

MSSanté,

- *Comprendre MSSanté, 2021,* disponible à : https://mssante.fr/
- *Industriels, 2021*, disponible à : https://mssante.fr/

ROJOUAN Bruno, « *Rapport d'information fait au nom de la commission de l'aménagement du territoire et du développement durable (1) par la mission d'information sur les perspectives de la politique d'aménagement du territoire et de cohésion territoriale (2), sur le volet « renforcer l'accès territorial aux soins »,* Rapport d'information n°589, 2022.

THERY Gérard, « les autoroutes de l'information : rapport au premier Ministre », *Collection des rapports officiels*, 1994.

VIE PUBLIQUE,

- *Qu'est-ce que le taylorisme ?, 2019,* disponible à : https://www.vie-publique.fr/

- *La télémédecine, une pratique en voie de généralisation*, 2020, disponible à : https://www.vie-publique.fr/
- *Ordonnance du 18 novembre 2020 portant mise en œuvre de la prescription électronique*, 2020, disponible à : https://www.vie-publique.fr/
- *Les déserts médicaux : définition et mesures des pouvoirs publics*, 2021, disponible à : https://www.vie-publique.fr/
- *Que signifie « nul n'est censé ignorer la loi » ?*, Fiche thématique, 2021, disponible à : https://www.vie-publique.fr/
- *Loi Kouchner sur les droits des malades : 20 ans après la loi, quel bilan ?*, Eclairage, 2022, disponible à : https://www.vie-publique.fr/

5. Jurisprudence

a. Cour de cassation

i. Chambres civiles

Cass. civ. 1ère, 29 mai 1951.

Cass. civ. 1ère, 30 avril 1970, 68-13.534, Publié au bulletin.

Cass. civ 1ère, 12 juillet 1972, 71-12.249, Publié au Bulletin.

Cass. civ. 1ère, 25 juin 1996, 94-11.745, Publié au bulletin.

Cass. civ. 1ère, 25 fév. 1997, 94-19.685, Publié au bulletin.

Cass. civ. 1re, 30 mai 2000, n° 98-16519.

Cass. civ. 1ère, 18 mai 2005, 04-13.745, Publié au bulletin.

Cass. civ. 1ère, 10 avril 2013, 11-19.530, Publié au bulletin.

Cass. civ., 1ère, 26 septembre 2018, 17-20.143, Publié au bulletin.

Cass. civ., 1ère, 05 mars 2015, 14-12.292.

Cass. civ. 1ère, 23 sept. 2020, n° 19-11.441, Publié au bulletin.

Cass. civ. 1ère, 7 octobre 2020 n°19-18.135, Publié au bulletin.

Cass. civ. 2ème, 4 décembre 2008, 07-17.622, Publié au bulletin.

Cass. civ. 2ème, 28 mai 2020, 19-11.744, Publié au bulletin.

Cass. civ., 2ème, 12 mai 2021, 20-10.584 20-10.826, Inédit.

ii. Chambre criminelle

Cass. crim. 3 juin 2008, n°08-80467, Publié au bulletin.

Cass. crim., 25 octobre 2011, n°10-87.179.

Cass. crim., 16 mai 2012, n°11-83.834, Publié au bulletin.

Cass. crim., 1 avril 2020, n°19.80.375.

iii. Chambre commerciale

Cass, com, 2 décembre 1997, 95-14.251, Publié au bulletin.

Cass. com., 23 mai 2007, 06-43.209, Publié au bulletin.

iv. Chambre sociale

Cass. soc., 17 mai 2016, 04-46.706, Inédit.

b. Conseil d'Etat

CE, 10/ 7 SSR, 27 avril 1994, 147203 148545, publié au recueil Lebon.

c. Cour d'appel

CA Besançon, ch. soc., 20 oct. 2000, D. 2001, IR p. 432, CA Rouen, ch. Soc., 20.09.2017, n°16/05131.

CA Toulouse, 1ère ch. sect., 25 octobre 2010, 10/01705.

CA Toulouse, 25 octobre 2010, n°508, 10/01705.

CA, Fort de France, 14 décembre 2012, n°12/00311.

CA, Lyon, 6e ch., 3 septembre 2015 – n° 13/09407.

CA, Aix-en-Provence, 8e chbre b, 27 avril 2017, n° 15/06339.

CA, Douai, 2e ch. 2e sect., 19 décembre 2019, n°18/06253.

CA, Nancy 2e ch. civ., 10 mars 2022, n°21/0101223.

d. Cour administrative d'appel

CAA Bordeaux, 22 mai 2007, n°04BX01203.

CAA Marseille, 2ème, 13 février 2014, n°11MA02696, Inédit au recueil Lebon.

e. Tribunal judiciaire

TJ Paris, 6 nov. 2020, n°20/54799.

f. Juridictions extranationales

i. Cour de justice des communautés européennes

CJCE, 6 nov. 2003, aff. C*101/01, procédure pénale contre *Bodil Lindqist*.

6. Principaux textes

a. Règlement

Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, JOUE, 28 août 2014.

Règlement grand-ducal du 25 juillet 2015 relatif à la dématérialisation et à la conservation de documents, mémorial A n°150/2015.

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, JOUE, L 119, 04 mai 2016.

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 90/385/CEE et 93/42/CEE du Conseil, JOUE, L 117, 5 mai 2017.

b. Loi

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

Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JORF n°62, 14 mars 2000, texte n°1.

Loi concernant le cadre juridique des technologies de l'information entrée en vigueur le 1er novembre 2001 (Québec).

Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (1), JORF, 5 mars 2002, texte n°1.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1), JORF n°0143, 22 juin 2004, texte n°2.

Loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées (1), JORF n°36, 12 février 2005, texte n°1.

Loi n° 2005-370 du 22 avril 2005 relative aux droits des malades et à la fin de vie (1), JORF n°95, 23 avril 2005, texte n°1.

Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires (1), JORF n°0167, 22 juillet 2009, texte n°1.

Loi du 25 juillet 2015 relative à l'archivage électronique et portant modification : 1. De l'article 1334 du Code civil ; 2. De l'article 16 du Code de commerce ; 3. De la loi modifiée du 5 avril 1993 relative au secteur financier (Luxembourg).

Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, JORF n°0022, 27 janvier 2016, texte n°1.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235, 8 octobre 2016, texte n°1.

Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé (1), JORF n°0172, 26 juillet 2019, texte n°3.

Loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020 (1), JORF n°0302, 29 décembre 2019, texte n°1.

Loi n° 2021-1755 du 23 décembre 2021 visant à renforcer la régulation environnementale du numérique par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (1), JORF n°0299, 24 décembre 2021, texte n°2.

Loi n°2021-1017 du 2 août 2021 relative à la bioéthique (1), JORF n°0178, 3 août 2021, texte n°1.

Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, JORF n°0053, 4 mars 2022, texte n°1.

c. Projet et Proposition de Loi

Projet de loi ratifiant les ordonnances n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel et n° 2017-29 du 12 janvier 2017 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique (AFSZ1703539L).

Projet de Loi relatif à l'archivage électronique et modifiant la loi modifiée du 6 avril 1993 relative au secteur financier. (Luxembourg)

Proposition de Loi Constitutionnelle pour une nouvelle démocratie citoyenne et participative, enregistré à la Présidence de l'Assemble nationale le 10 novembre 2021 (n°4661).

d. Décret

Décret n°71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JORF, 3 décembre 1971.

Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, JORF n°0077, 31 mars 2001, texte n°19.

Décret n° 2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice, JORF n°186, 11 août 2005, texte n°33.

Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, JORF n°186, 11 août 2005, texte n°34.

Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine, JORF n°0245, 21 octobre 2010, texte n°13.

Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, JORF n°0283, 6 décembre 2016, texte n°61.

Décret n° 2017-770 du 4 mai 2017, portant obligation pour les notaires d'effectuer par voie électronique leurs dépôts de documents auprès des services chargés de la publicité foncière, JORF n°0107, 6 mai 2017, texte n°23.

Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique, JORF n°0229, 30 septembre 2017, texte n°8.

Décret n° 2018-788 du 13 septembre 2018 relatif aux modalités de mise en œuvre des activités de télémédecine, JORF n°0212, 14 septembre 2018, texte n°11.

Décret n° 2019-528 du 27 mai 2019 relatif à l'expérimentation d'une « e-carte d'assurance maladie », JORF n°0124, 29 mai 2019, texte n°7.

Décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne, JORF n°0171, 25 juillet 2019, texte n°38.

Décret n° 2020-395 du 3 avril 2020 autorisant l'acte notarié à distance pendant la période d'urgence sanitaire, JORF n°0082, 4 avril 2020, texte n°1.

Décret n°2020-446 du 18 avril 2020 relatif à l'établissement du certificat de décès, JORF n°0096, 19 avril 2020, texte n°2.

Décret n° 2021-573 du 10 mai 2021 complétant la liste des maladies faisant l'objet d'une transmission obligatoire de données individuelles à l'autorité sanitaire, JORF n°0110, 12 mai 2021, texte n°22.

Décret n° 2021-707 du 3 juin 2021 relatif à la télésanté, JORF n°0128, 4 juin 2021, texte n°15.

e. Ordonnance

Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°0035, 11 février 2016, texte n°26.

Ordonnance n° 2020-1408 du 18 novembre 2020 portant mise en œuvre de la prescription électronique, JORF n°0280, 19 novembre 2020, texte n°46.

Ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie, JORF n°0111, 13 mai 2021, texte n°38.

a. Arrêté

Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques de l'ANAES (HAS aujourd'hui) relatives à l'accès aux informations concernant la santé d'une personne, JORF n°65, 17 mars 2004, texte n°16.

Arrêté du 20 octobre 2016 portant approbation de la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016, JORF n°0248, 23 octobre 2016, texte n°10.

Arrêté du 1er août 2018 portant approbation de l'avenant n°6 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016, JORF n°0183, 10 août 2018, texte n°16.

Arrêté du 2 juin 2017 définissant le champ d'application de l'obligation faite aux notaires d'effectuer par voie électronique leurs dépôts de documents auprès des services chargés de la publicité foncière, JORF n°0137, 13 juin 2017, texte n°14.

Arrêté du 22 mars 2017 fixant les modalités de numérisation des factures papier en application de l'article L. 102 B du livre des procédures fiscales, JORF n°0076, 30 mars 2017, texte n°14.

Arrêté du 21 août 2019 portant approbation de l'accord conventionnel interprofessionnel en faveur du développement de l'exercice coordonné et du déploiement des communautés professionnelles territoriales de santé signé le 20 juin 2019, JORF n°0196, 24 août 2019, texte n°5.

Arrêté du 20 novembre 2020 relatif à la signature électronique des décisions juridictionnelles rendues en matière civile, JORF n°0283, 22 novembre 2020, texte n°13.

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.

Arrêté du 4 avril 2022 relatif à des moyens d'identification électronique immatériels mis à disposition des professionnels, personnes physiques des secteurs sanitaire, social et médico-social pour l'utilisation des services numériques en santé, JORF n°0087, 13 avril 2022, texte n°18.

b. Circulaire

Circulaire DHOS/E1/DGS/SD1B/SD1C/SD4A/2006/90 du 2 mars 2006 relative aux droits des personnes hospitalisées et comportant une charte de la personne hospitalisée.

c. Instruction

Instruction N°DGS/SP2/DGOS/PF5/2016/112 du 4 juillet 2016 relative au déploiement de l'application e-DO pour la télé-déclaration de l'infection par le VIH/Sida.

Instruction n°SG/DSSIS/2017/8 du 10 janvier 2017 relative à l'organisation à déployer pour la mise en œuvre de la stratégie d'e-santé en région.

Instruction n°DGOS/PF5/2019/32 du 12 février 2019 relative au lancement opérationnel du programme HOP'EN.

INDEX ALPHANBETIQUE

Les numéros renvoient aux numéros des paragraphes

TABLE DES MATIERES

Auteur : Elaine BUCKI

Sujet : La dématérialisation en établissement de santé – analyses juridiques

Matière : Droit privé – Sciences criminelles

Résumé : Depuis de nombreuses années, la dématérialisation des données fait partie de notre vie personnelle et professionnelle, y compris dans les domaines traitant de données sensibles, à l'instar du domaine bancaire ou plus récemment, de celui de la santé.

Posons-nous deux questions : qui, aujourd'hui, n'a jamais vu ses données de santé se dématérialiser pour intégrer un dossier patient informatisé ou pour être transmises par internet ? Ou encore, qui n'a jamais été pris en charge par un médecin *via* la téléconsultation ? A priori, personne.

Pour autant, même si la dématérialisation et l'utilisation du numérique en santé se généralisent et deviennent une pratique courante, de nombreuses problématiques juridiques restent en suspens : la valeur probante des documents contenant des données de santé, ou encore la garantie que la dématérialisation, lors de la prise en charge du patient, ne présente pas de risques pour lui, ses données ou ses droits.

En effet, l'utilisation du numérique en santé présente des avantages qui ne sont plus à démontrer, mais fait naître de nouveaux risques qui n'existaient pas lors d'une prise en charge dite « traditionnelle ». Il est donc essentiel d'étudier les risques encourus par cette dématérialisation afin de déterminer des mécanismes juridiques permettant la dématérialisation des données de santé « dans les règles de l'art » et conforme à une bonne, voire une meilleure prise en charge du patient.

Mots clés : dématérialisation – données de santé - valeur probante – copie numérique – document natif numérique – signature électronique – archivage électronique – intégrité – traçabilité – hébergement des données de santé – dossier patient informatisé – e-santé – télémédecine – prise en charge médicale – droits des patients – consentement – secret professionnel.

Abstract : Since many years, data dematerialization has become part of both our personal and professional life, including in areas dealing with sensitive data, such as the banking sector and more recently, the health sector.

Two questions thus arise: have you ever seen your health data dematerialized integrate a computerized patient file or via the Internet? Have you ever been taken care of by a doctor via teleconsultation? Your answer may only be yes.

However, even if dematerialization and the use of digital health are becoming widespread and common practice, many legal issues remain unsolved: the probative value of documents containing health data, or the guarantee that dematerialization, when caring for the patient, does not present any risk to them, their data or their rights.

Indeed, the use of digital health has advantages that no longer need to be demonstrated, but new risks which did not exist during so-called "traditional" care now occur.

Therefore, it is essential to study the risks incurred by this dematerialization in order to determine the judicial mechanisms enabling the dematerialization of health data in the best way possible and in accordance with good or even better patient care.

Key-words : dematerialization – health data – probative value – digital copy – digital native document – electronic signature – data storage – integrity – traceability – health data hosting – computerized patient file – e-health – telemedecine – medical care – patient rights – consent – professional secret.