ComUE Lille Nord de France

Thèse délivrée par

L'Université de Lille, Droit et Santé

N° attribué par la bibliothèque

__|__|__|__|__|__|__|__|__|__|

THÈSE

Pour obtenir le grade de Docteur en Droit public

Présentée et soutenue publiquement par

Laora TILMAN

Le 28 septembre 2017 à 14h30.

L'utilisation des technologies de l'information et de la communication à l'hôpital face au droit

JURY

Directeur de thèse : **Madame Johanne SAISON-DEMARS,** Professeur des universités, Université Lille 2, Droit et Santé.

Membres du jury: **Madame Cécile MANAOUIL,** Professeur des universités, Université de Picardie Jules Verne, Rapporteur.
Monsieur Marcel MORITZ, Maître de conférences des universités, Université Lille 2, Droit et Santé, Suffragant.
Monsieur François VIALLA, Professeur des universités, Université Montpellier 1, Rapporteur.
Madame Caroline ZORN, Docteur en droit privé, Suffragante.

L'Université de Lille 2 n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse. Elles doivent être considérées comme propres à leur auteur.

Remerciements

J'adresse d'abord mes remerciements à Madame Johanne Saison- Demars, qui m'a accordé sa confiance et a accepté de diriger mes travaux de recherche. Son soutien, sa disponibilité et ses conseils m'ont permis d'arriver au terme de cette thèse.

Je remercie les membres du jury qui m'ont accordé le privilège de leur présence : Madame le Professeur Cécile Manaouil, Monsieur Marcel Moritz, Monsieur le Professeur François Vialla et Madame Caroline Zorn.

Je tiens à remercier l'Association Nationale de la Recherche et de la Technologie (ANRT) pour le soutien financier qu'elle m'a accordé. Je remercie également le CHRU de Lille pour son accompagnement.

J'exprime ma profonde gratitude à Monsieur Paul Barincou, ancien Directeur des Affaires Juridiques du CHRU de Lille, qui m'a permis de préparer cette thèse dans le cadre d'une CIFRE. Ces travaux n'auraient pas vu le jour sans l'opportunité qu'il m'a accordée. Je remercie également Madame Marie-Charlotte Dalle, Directrice des Affaires Juridiques du CHRU de Lille, pour son soutien et sa bienveillance au quotidien.

Je tiens à exprimer ma reconnaissance à l'égard de mes proches : mes parents, qui m'ont soutenue au long de mes études de droit et ma sœur, pour son écoute sans faille. Je remercie sincèrement mon conjoint pour sa présence, sa patience, ses encouragements.

La thèse est un travail long et prenant. Dans ce contexte, l'appui et le soutien de mes amis a été une aide précieuse. Je leur en suis extrêmement reconnaissante.

Je tiens enfin à remercier mes relecteurs : Alice, dont les bons mots ont égayé mes corrections ; Elise, qui m'a accompagnée tout au long de ma thèse ; Emmanuelle, François et Marie qui ont pris le temps de m'épauler et de s'intéresser à mes travaux ; Heidi, pour sa rigueur et ses conseils avisés ; Rodolphe, qui a pris le temps de ponctuer sa relecture de remarques précieuses.

Sommaire

PREMIERE PARTIE. Le cadre juridique de l'utilisation des TIC à l'hôpital, un cadre incomplet.

Titre 1.TIC et informatisation des données de sante : un cadre parfois inadapté.

Chapitre 1. Le traitement informatisé des données du patient

Chapitre 2. Les modalités de conservation et de communication des informations relatives aux patients.

Titre 2. TIC et prise en charge médicale : un cadre en évolution.

Chapitre 1. La dématérialisation des dossiers médicaux : l'exemple du DMP.

Chapitre 2. L'utilisation des TIC dans la prise en charge du patient.

SECONDE PARTIE. Les voies de sécurisation de l'utilisation des TIC à l'hôpital.

Titre 1. L'impulsion de la sécurisation au niveau national.

Chapitre 1. Une gouvernance forte des systèmes d'information en santé, une priorité

Chapitre 2. La refonte du cadre juridique, un effort nécessaire.

Titre 2. Les établissements de santé, acteurs clés de la sécurisation de l'utilisation des TIC à l'hôpital.

Chapitre 1. Les établissements de santé, au cœur de la sécurisation de leurs pratiques.

Chapitre 2. Un exemple de sécurisation réussie : le CHRU de Lille.

Principales abréviations

AJDA	Actualité Juridique, Droit Administratif
AN	Assemblée nationale
Ass. Plén.	Assemblée plénière
Bull. crim.	Bulletin des arrêts de la Cour de cassation : chambre criminelle
C.A.A.	Cour administrative d'appel
C.C.	Conseil constitutionnel
C.E.	Conseil d'Etat
Cass. civ.	Cour de cassation, chambre civile
Cass. crim.	Cour de cassation, chambre criminelle
Cass. soc.	Cour de cassation, chambre sociale
Chron.	Chronique
CHU	Centre hospitalier universitaire
CJUE	Cour de justice de l'Union européenne
Comm.	Commentaires
Concl.	Conclusions
CPOM	Contrats pluriannuels d'objectifs et de moyens
D.	Recueil Dalloz
DDS	Droit, déontologie et soin
DGOS	Direction générale de l'offre de soins
DMP	Dossier médical partagé
éd.	Edition
Fasc.	Fascicule
Gaz. Pal.	Gazette du palais
GHT	Groupement hospitalier de territoire
Ibid.	Même ouvrage, à la même page
Id.	Même ouvrage
In	Dans
INS	Identifiant national de santé
Infra	Ci-dessous
JCP	Jurisclasseur périodique (La semaine juridique)

JORF	Journal officiel de la République française
L.G.D.J	Librairie Générale de Droit et de Jurisprudence
LPA	Les petites affiches
n°	Numéro
NIR	Numéro d'inscription au répertoire
Obs.	Observations
Op. cit.	Opere citato (dans l'ouvrage précité)
PUF	Presses universitaires de France
PUN	Presses universitaires de Nancy
RDP	Revue de droit public
RDC	Revue de droit des contrats
RDS	Revue Droit et santé
RDSS	Revue de droit sanitaire et social
Rec.	Recueil Lebon
RF adm. publ.	Revue française d'administration publique.
RFDC	Revue française de droit constitutionnel
RGDM	Revue générale de droit médical
RTD civ.	Revue trimestrielle de droit civil
s.	Suivant
S.	Recueil Sirey
Supra	Ci-dessus
TA.	Tribunal administratif
TC.	Tribunal des conflits
TGI	Tribunal de grande instance
TIC	Technologies de l'information et de la communication
V.	Voir
vol.	Volume

Introduction Générale

« *Dans le domaine de la santé, le XIXème siècle avait connu la "révolution pasteurienne", le XXème celle entraînée par la découverte de la pénicilline, il est probable que le XXIème en connaîtra deux : la génétique et l'intégration à la médecine des nouvelles technologies de l'information qui vont bouleverser en profondeur l'organisation et la conception que nous nous faisons de la médecine.* »[1]

1. L'introduction réussie des Technologies de l'Information et de la Communication (TIC) dans la pratique médicale représente un enjeu important dans la rénovation du système de santé français. Les TIC apparaissent en effet comme l'outil idéal, permettant de répondre aux défis majeurs que rencontre notre système de santé aujourd'hui. D'abord, elles participent à une meilleure coordination des soins, en améliorant le recueil des informations relatives aux patients et la communication de celles-ci entre les professionnels de santé. Elles permettent également d'assurer un accès aux soins à certains patients situés dans certaines zones du territoire mal dotées en termes d'offre de soins. Il s'agit, en effet, d'outils capables de « *répondre aux situations d'isolement et d'éloignement géographique, dues à la raréfaction des médecins généralistes et spécialistes dans certaines régions* » mais permettant également d'atténuer « *les effets du cloisonnement et de la complexité de l'organisation des soins et des aides sociales, notamment à la sortie de l'hôpital lorsque l'état du patient nécessite une télésurveillance médicale à domicile et des aides non médicales* »[2]. Ensuite, leur utilisation est source d'économies non négligeables en matière de dépenses de santé. Enfin, les TIC en santé garantissent un accès élargi à l'ensemble du territoire aux expertises médicales de pointe.

2. Le dictionnaire Larousse définit les Technologies de l'Information et de la Communication comme l'« *ensemble des techniques et des équipements informatiques permettant de communiquer à distance par voie électronique.* ». Les TIC peuvent également

---

[1] DIONIS du SEJOUR, Jean. ETIENNE, Jean-Claude. « Les télécommunications à haut débit au service du système de santé », rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques, 2004, p. 8.

[2] LABORDES, Pierre. « La télésanté : un nouvel atout au service de notre bien-être », *La Documentation française*, p. 39.

être définies comme les technologies qui « *englobent toutes les technologies numériques facilitant la saisie, le traitement, le stockage et l'échange électroniques d'informations* »[3]. Dans le domaine plus spécifique de la santé, l'utilisation des TIC est multiple. Ces outils sont utilisés dans de nombreuses situations assez diverses et derrière l'expression de "TIC en santé", nous retrouvons de nombreuses pratiques telle que la e-santé, les activités de télémédecine (ou parfois appelées plus largement télésanté), l'informatisation des données de santé par le biais de la création de dossier médicaux informatisés, mais également le dispositif SESAM-Vitale (dans le cadre de la mise en place de la télétransmission des feuilles de soins), le développement des cartes puce (carte Vitale, carte CPS), les sites d'information en santé sur Internet ou encore, plus récemment, le développement des objets connectés en santé.

3. Face à la multiplicité et à la complexité du sujet, nous avons fait le choix de concentrer notre recherche plus spécifiquement sur l'utilisation des TIC dans la pratique médicale, c'est-à-dire l'utilisation des TIC comme outils intervenant directement dans la prise en charge médicale d'un patient par les professionnels de santé, et plus particulièrement dans le cadre d'actes de soins, de diagnostic ou de prévention.

4. L'hôpital[4], de par ses missions[5] et son organisation, apparait alors comme étant le terrain idéal de notre étude. Le système de santé français se caractérise par la coexistence de plusieurs types d'établissements de santé : les établissements publics de santé d'une part, et les établissements privés d'autre part. Parmi ces derniers, nous retrouvons les établissements de santé d'intérêt collectif (ESPIC) et les établissements poursuivant un but lucratif. Les

---

[3] GAGNON, Marie-Pierre. BRETON, Erik. « L'influence des technologies de l'information et des communications sur le maintien en poste des infirmières », *Santé Publique*, 2013/3 (Vol. 25), p. 126.

[4] Le dictionnaire Larousse définit l'hôpital comme étant un « *établissement public ou établissement privé ayant passé certaines conventions avec l'État et où peuvent être admis tous les malades pour y être traités* ».

[5] L'article L. 6111-1 du Code de la santé publique prévoit que « *les établissements de santé publics, privés d'intérêt collectif et privés assurent, dans les conditions prévues au présent code, en tenant compte de la singularité et des aspects psychologiques des personnes, le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes et mènent des actions de prévention et d'éducation à la santé. Ils délivrent les soins, le cas échéant palliatifs, avec ou sans hébergement, sous forme ambulatoire ou à domicile, le domicile pouvant s'entendre du lieu de résidence ou d'un établissement avec hébergement relevant du code de l'action sociale et des familles. Ils participent à la coordination des soins en relation avec les membres des professions de santé exerçant en pratique de ville et les établissements et services médico-sociaux, dans le cadre défini par l'agence régionale de santé en concertation avec les conseils départementaux pour les compétences qui les concernent. Ils participent à la mise en œuvre de la politique de santé et des dispositifs de vigilance destinés à garantir la sécurité sanitaire. Ils mènent, en leur sein, une réflexion sur l'éthique liée à l'accueil et la prise en charge médicale. Ils peuvent participer à la formation, à l'enseignement universitaire et post-universitaire, à la recherche et à l'innovation en santé. Ils peuvent également participer au développement professionnel continu des professionnels de santé et du personnel paramédical*. »

établissements publics de santé, quant à eux, sont des personnes morales de droit public, dotées d'une autonomie administrative et financière[6]. Le secteur public se caractérise par une règlementation abondante et diversifiée portant sur l'organisation des établissements, leur fonctionnement ou encore la gestion de leur personnel. C'est notamment pour cette spécificité que nous avons fait le choix de concentrer nos recherches sur les établissements publics de santé.

5. Dans ce contexte, l'introduction des TIC a ouvert de nombreuses possibilités de prises en charge innovantes (Paragraphe I), en permettant, notamment, le déploiement, de la télémédecine. Néanmoins, l'utilisation de ces nouveaux outils peut également être source de dérives et de nombreuses questions se posent quant à l'encadrement de leur mise en place (Paragraphe II). Le droit apparait alors comme un outil incontournable pour accompagner l'expansion de l'utilisation des TIC en santé. Cependant, il va également se révéler être, dans certaines situations, un frein au développement pérenne des TIC dans la pratique médicale, soit par ses lacunes, soit par son excès de rigueur et, généralement, par son caractère inadapté. Notre étude va ainsi s'attacher à présenter le caractère lacunaire du cadre juridique de l'utilisation des TIC en santé, avant de réfléchir aux pistes de sécurisation possibles (Paragraphe III).

§1. Les multiples possibilités offertes par l'introduction des TIC dans la pratique médicale

« *L'essentiel c'est d'abord cette conviction que nous partageons tous que la télésanté n'est pas un sujet comme un autre mais le système qui, dans les années à venir, va transformer les pratiques médicales, voire la manière même dont nous concevons la* santé »[7].

6. Qualifiée de « *nouvelle révolution médicale* »[8], l'introduction des TIC dans la pratique médicale représente le renouveau de l'activité médicale et le développement croissant de leur utilisation ouvre de nouvelles possibilités dans la prise en charge et le suivi à distance des

[6] Article L. 6141-1 du Code de la santé publique.
[7] Déclaration de Mme Roselyne Bachelot, Ministre de la santé, de la jeunesse, des sports et de la vie associative, sur l'utilisation des technologies de l'information et de la communication au service de la santé, Paris le 4 novembre 2008. Disponible sur [http://discours.vie-publique.fr]
[8] LABORDES, Pierre. « La télésanté : un nouvel atout au service de notre bien-être », *op. cit.*, p. 39.

patients. Celles-ci sont nombreuses, et certaines d'entre elles ont retenues plus particulièrement notre attention. Véritable espoir pour les zones géographiques mal desservies, mais également pour les populations isolées, les TIC permettent l'accès à des expertises de pointe (A). Par ailleurs, l'utilisation des TIC présente également un intérêt dans la mise en œuvre de politiques de prévention, au travers du développement des objets connectés (B). Deux possibilités qui méritent que nous nous y attardions.

A. Les TIC, nouvel espoir pour les prises en charges difficiles

7. La répartition de l'offre de santé sur le territoire français est inégale. A titre d'exemple, en 2015, alors que la région Ile-de-France comptait plus de 3000 cabinets médicaux, la Picardie n'en comptait qu'entre 500 et 1000 et la Corse moins de 500.[9] Bien que les effectifs de médecin aient augmenté jusqu'en 2008, l'abaissement du numerus clausus dans les années 90 a pour conséquence, depuis 2009, une baisse du nombre de médecins, qui devrait continuer jusqu'en 2019, et qui sera accompagné, à compter de 2025, d'un départ massif à la retraite de médecins, provoquant ainsi une baisse de 10% de leur nombre[10.] Ces départs risquent de fragiliser grandement certains territoires, déjà mal desservis. Dans ce contexte difficile, la télémédecine, qui s'est développée grâce à l'introduction des TIC dans la pratique médicale, apparait comme un des outils à privilégier afin de maintenir un égal accès aux soins sur le territoire. D'ailleurs, le Ministère de la santé, lors du lancement du pacte santé territoire[11] n°2 en 2015, a prévu, au titre de ses dix nouvelles actions, un investissement de plus de 40 millions d'euros pour développer la télémédecine en ville, en particulier pour les patients chroniques et les soins urgents.

8. La télémédecine présente des avantages multiples : elle facilite l'accès à des soins de qualité pour des personnes situées dans des zones isolées, et contribue au maintien de l'offre de soins de proximité tout en apportant une expertise de pointe, accessible via les TIC. Elle permet également le suivi à distance des populations fragiles ou chroniques, limitant ainsi

[9] DGOS. « Les chiffres clés de l'offre de soin », édition 2015, p. 4. Disponible sur [http://www.fnehad.fr], consulté le 2 mai 2017.
[10] LABORDES, Pierre. « La télésanté, un atout au service de notre bien-être », *op. cit.*, p. 46.
[11] Lancé en 2012 et complété en 2015, le Pacte Santé Territoire a pour objectifs de lutter contre la désertification médicale et d'assurer une meilleure répartition des médecins sur le territoire.

leurs déplacements et améliorant leur qualité de vie. L'introduction de la télémédecine dans la pratique des professionnels de santé va également rendre le temps médical plus efficient[12]. Enfin, la prise en charge de certaines urgences vitales va être améliorée, la télémédecine permettant aux services d'urgence de recueillir plus facilement et plus rapidement des avis spécialisés nécessaires. C'est le cas par exemple de l'accident vasculaire cérébral ischémique (AVC), pour lequel l'avis d'un neuroradiologue est nécessaire. Le recours à la téléexpertise, dans ce cas, permet alors d'établir rapidement un diagnostic et d'envisager la suite de la prise en charge du patient, en limitant ainsi toutes pertes de chance.

9. C'est pourquoi, dès 2011, la Direction Générale de l'Offre de Soins (DGOS), en charge du pilotage de la stratégie nationale de déploiement de la télémédecine sur le territoire, avait identifié cinq thématiques considérées comme prioritaires. Il s'agissait de la permanence des soins en imagerie médicale, de la prise en charge des accidents vasculaires cérébraux (AVC), de la santé des personnes détenues, de la prise en charge d'une maladie chronique (et notamment l'insuffisance rénale chronique, l'insuffisance cardiaque, diabète, ...) et des soins en structure médico-sociale ou en hospitalisation à domicile (HAD).
Ainsi, plusieurs projets de télémédecine ont été développés en France autour de ces problématiques. L'ANAP, dans un guide publié en mai 2012, avait d'ailleurs dressé un premier bilan de 25 projets s'inscrivant dans les cinq thématiques prioritaires et identifiés comme suffisamment matures pour servir d'exemple aux acteurs souhaitant développer un projet de télémédecine.

10. Dans ce contexte, les établissements publics de santé apparaissent être les acteurs centraux de la majorité des projets de télémédecine actuellement recensés[13]. De nombreux exemples pourraient être cités[14], nous faisons le choix de nous attarder sur deux projets spécifiques qui démontrent bien, à notre sens, les enjeux de la télémédecine.

---

[12] SIMON, Pierre. « Comment développer la télémédecine ? Où ? », disponible sur |http://esante.gouv.fr/actus/telemedecine]. Consulté le 15 mai 2017.
[13] « Le recensement des activités de télémédecine », rapport de la DGOS, décembre 2012.
[14] *V.* notamment en ce sens : HERVIEU-BEGUE, Marie. GIROUD, Maurice. BEJOT, Yannick. «Un réseau de télémédecine pour AVC », *Soins Aides-Soignantes*, Volume 14, 2017, p. 13-14 ; Le BŒUF, Dominique. « La télémédecine en France, du concept à la pratique », *Soins*, Volume 61, 2016, pp. 28-30 ; PERRIER-BONNET, Sabine. « Une consultation de télémédecine dans le cadre d'un réseau plaies et cicatrisation », *La Revue de l'Infirmière*, Volume 65, 2016, pp. 35-37.

11. Le premier est un projet de télépsychiatrie, développé par le centre hospitalier de Rouvray dès 2007[15]. Cet établissement psychiatrique dispose d'un service de psychogériatrie, comprenant notamment une équipe mobile intervenant au sein de différents EHPAD. Un projet de télépsychiatrie pour les sujets âgés s'est développé, initialement sur cinq sites (le CHR de Rouvray, 3 CMP, un EHPAD et une unité d'accueil familial thérapeutique). Les premiers retours de cette expérimentation étant positifs, l'activité de télépsychiatrie a été maintenue et s'est accentuée. Ainsi, le nombre des téléconsultations assurées par les cinq psychiatres dédiés à l'activité ont augmenté, passant de près de 100 téléconsultations en 2012 à 462 en 2014. Pour les équipes mobiles, cet outil a permis d'étendre leur couverture territoriale et d'améliorer leur réactivité, diminuant ainsi le recours aux services d'urgences. Cette expérience, qui s'inscrit dans le contexte particulier de la baisse de l'offre de soins psychiatriques dans certaines zones rurales, et de la prise en charge de populations fragiles à mobilité réduite (les personnes âgées) démontre l'intérêt et la plus-value de la télémédecine dans ce type de prise en charge.

12. Le second est un projet de téléexpertise pour les urgences neurochirurgicales développé par le CHRU de Lille : le réseau TELURGE. Ce dispositif est un pionnier en la matière puisque le réseau, composé de 22 centres hospitaliers, a été créé en 1996. Le principe consiste en l'obtention à distance, pour les services d'urgences des différents centres hospitaliers, de l'avis d'un neurochirurgien du CHRU de Lille ou, depuis 2012, du Centre hospitalier de Valenciennes. Le neurochirurgien, sur la base d'un dossier médical et d'examen d'imagerie transmis à distance, va formuler un avis, véritable aide à la décision diagnostique et thérapeutique pour l'équipe prenant en charge le patient. Ce dispositif permet donc à vingt et un centres hospitaliers de bénéficier d'une expertise de pointe, et d'assurer ainsi une prise en charge optimale pour leurs patients, arrivant parfois dans des situations critiques telles que les hémorragies cérébrales ou les traumatismes crâniens. Par ailleurs, cette expertise permet d'éviter au patient un transfert inutile et de limiter toute perte de chance.

13. Ces deux exemples,[16] permettent, à notre sens, de démontrer que l'introduction des TIC dans la pratique médicale, au travers de la télémédecine, améliore de manière

---

[15] DESBORDES, Marie. « La télémédecine en psychiatrie du sujet âgé : enjeux et perspectives La télémédecine en psychiatrie du sujet âgé : enjeux et perspectives », *NPG Neurologie - Psychiatrie - Gériatrie*, Volume 15, 2015, pp. 270-273.

[16] Définition de la HAS. Disponible sur [http://www.has-sante.fr], consulté le 15 mai 2017.

considérable l'offre de soin existante. Elle permet de résoudre certaines difficultés rencontrées dans un contexte de diminution de l'offre de santé en zone rurale, et de vieillissement de la population, mais également de faire bénéficier aux patients des meilleurs soins et des expertises les plus pointues et ce, sans avoir à les déplacer inutilement. La télémédecine permet ainsi de gommer certaines inégalités dans l'accès aux soins et, à ce titre, permet d'assurer le droit à la protection de la santé, tel que prévu par l'alinéa 11 du préambule de la Constitution de 1946.

B. Les TIC, outil majeur dans la mise en place d'actions de prévention en santé.

14. Inscrite parmi les missions des établissements publics de santé[17], la prévention en santé représente un enjeu essentiel des politiques de santé en France. Or, comme le soulignait l'avis du conseil économique, social et environnemental, la politique sanitaire actuelle est encore trop centrée sur le curatif[18]. Selon la Haute Autorité de Santé (HAS), la prévention consiste à « *éviter l'apparition, le développement ou l'aggravation de maladies ou d'incapacités; sont classiquement distinguées la prévention primaire qui agit en amont de la maladie (ex : vaccination et action sur les facteurs de risque), la prévention secondaire qui agit à un stade précoce de son évolution (dépistages), et la prévention tertiaire qui agit sur les complications et les risques de récidive* »[19].

15. Les actions de prévention, pour être efficaces, nécessitent une adhésion, voire, comme le soulignait le conseil, une appropriation de celles-ci par les patients, en tant qu'acteur de leur santé. L'utilisation des TIC au sein de projets de prévention en santé, et plus particulièrement des objets connectés en santé, devient alors un moyen efficace pour diffuser des politiques de prévention en obtenant l'adhésion des usagers. Ces objets connectés sont des objets mobiles et communicants qui permettent, par le biais d'une connexion Internet, « *d'identifier, capter et*

---

[17] L'article L. 6111-1 dispose que « *les établissements de santé publics, privés d'intérêt collectif et privés assurent, dans les conditions prévues au présent code, en tenant compte de la singularité et des aspects psychologiques des personnes, le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes et mènent des actions de prévention et d'éducation à la santé [...]* ».

[18] GROS Jeannette, « Santé et nouvelles technologies de l'information », *JORF*, avis et rapports du Conseil économique et social, 2002, p. 4.

[19] Définition de la HAS, disponible sur [https://www.has-sante.fr], consulté le 25 mai 2017.

transmettre des informations, provoquer une interaction avec l'environnement et alimenter une application présente sur une interface (par exemple, un smartphone)»[20]

16. En la matière, les assureurs et les mutuelles font figure de pionniers. A titre d'exemple, en 2013 la société AXA en partenariat avec la société WITHINGS, proposait d'offrir aux 1000 premiers souscripteurs d'une nouvelle complémentaire santé un objet connecté permettant de tracer l'activité physique, mais également le rythme cardiaque et la qualité de sommeil de son porteur. L'assureur complétait également son offre en proposant un chèque « médecine douce » d'une valeur de 50 euros pour les clients réalisant plus de 7000 pas par jour. Selon Dimitri CARBONNELLE[21], « *[les objets connectés] sont une formidable opportunité pour les assureurs car cela leur permet de vendre de nouveaux services* ».

17. Les établissements de santé commencent également à développer des actions de prévention en santé, par le biais de l'utilisation d'objets connectés en santé. Ainsi, un Professeur des Universités, Praticien Hospitalier (PU-PH) du CHRU de Lille a développé, avec l'appui du Ministère de la santé, le projet intitulé « 10 000 pas, le défi pour la vie ». Il s'agit d'un programme de prévention de l'activité physique, piloté par le Professeur Philippe AMOUYEL, et ayant pour but de lutter contre la sédentarité, afin de prévenir le développement de maladies telles que le diabète, les cancers, ou encore les maladies cardiovasculaires. Ainsi, afin d'augmenter leur nombre de pas quotidiens, un kit, composé d'un podomètre et d'une application smartphone, a été distribué à certains agents du CHRU de Lille, volontaires pour s'inscrire dans la démarche. Le podomètre enregistre de manière quotidienne les performances de son porteur, et celui-ci peut, grâce à l'application smartphone reliée et spécialement conçue pour ce programme, se fixer des objectifs, suivre son évolution et lancer des défis aux autres participants du programme. Des conseils diététiques sont également dispensés de manière régulière. Ce programme, d'abord diffusé au niveau régional, a pour but d'être étendu ensuite au niveau national.

---

[20] CAMBON, Linda. « Objets connectés, mobiles, communicants en prévention : dépasser l'outil, penser l'intervention… », *Santé Publique*, vol. 28, n°. 1, 2016, pp. 5-6.
[21] CARBONELLE, Dimitri. « Les objets connectés transforment le secteur de l'assurance », *Le monde économie*, 15 juin 2015.

18. Les TIC en santé ont donc un rôle important à jouer dans la prévention en santé. La santé mobile (ou m-Health), qui repose sur des dispositifs mobiles, se développe en effet de manière considérable[22]. Le législateur s'est même récemment attaché à définir certaines notions qui entourent la santé mobile. Ainsi, la notion "d'automesure connectée" est-elle apparue au sein d'un avis de la commission d'enrichissement de la langue française, publié au Journal Officiel du 4 mars 2017[23]. Celle-ci est définie comme une « *pratique consistant, pour une personne, à mesurer elle-même à l'aide d'objets connectés des variables physiologiques la concernant, relatives notamment à sa nutrition, à ses activités physiques ou à son sommeil* ».

Les TIC en santé, et notamment les objets connectés, vont donc être amenés à jouer un rôle majeur dans la prévention en santé,

§2. Les TIC, des outils sources de risques éthiques et juridiques majeurs

19. Bien que l'utilisation accrue des TIC dans la pratique médicale présente de nombreux intérêts indéniables, elle s'accompagne également de risques. Leur développement doit se faire dans le strict respect des règles juridiques et déontologiques qui s'appliquent à l'exercice de la médecine. Or, ces nouvelles pratiques vont s'accompagner de l'apparition de nouveaux risques, qui vont peser aussi bien sur les patients, et plus particulièrement sur leurs données de santé (A) que sur la pratique médicale d'une manière générale (B).

A. Les risques pesant sur la vie privée du patient

20. L'utilisation des TIC dans la pratique médicale va modifier les modalités de prise en charge des patients. Néanmoins, la distance et la dématérialisation des échanges, fondements même de ces nouvelles pratiques médicales, ne doivent pas aller à l'encontre des droits fondamentaux des patients.

---

[22] DESMARAIS, Pierre. « Santé mobile - Quel régime pour la m-Health ? », *Communication Commerce électronique* n° 3, Mars 2013, étude 5.

[23] Avis de la commission d'enrichissement de la langue française, vocabulaire de la santé, *JORF* n°0054 du 4 mars 2017, texte n° 92.

21. La loi du 4 mars 2002[24], dite loi "Kouchner", a consacré des droits individuels aux patients tels que le droit au respect de la dignité, le respect de la vie privée et du secret des informations, le droit à la sécurité des soins, le droit à l'information, le respect du consentement ou le droit d'obtenir communication de son dossier médical. Ces droits sont aujourd'hui bien ancrés dans les pratiques courantes et ne doivent pas être négligés au profit du développement des TIC dans la prise en charge médicale. Or, comme le souligne Merav GRIGUER, *« si le secteur de la santé vit actuellement sa "transformation digitale", les utilisateurs manifestent encore un certain scepticisme. Parmi leurs principales préoccupations figurent le respect du secret médical, la protection de leurs données personnelles et de leur vie privée, la sécurisation des données, la transparence et le contrôle de l'utilisation de leurs données.* »[25].

22. L'utilisation des TIC en santé conduit de fait à un accroissement considérable du nombre de données personnelles dématérialisées. Ces données sont ensuite partagées entre professionnels, par le biais des TIC et ce, plus facilement et surtout, plus rapidement qu'auparavant. Cependant, le secret professionnel et la protection des données personnelles du patient, essentiels au maintien de la relation de confiance entre un professionnel de santé et son patient, ne doivent pas être négligés au profit d'une technique certes efficace, mais néanmoins risquée. En effet, si la « *multiplication exponentielle » des données de santé peut offrir de réelles opportunités, elle représente aussi certains risques pour le respect de la vie privée et la confidentialité de ces données* »[26]. Leur protection est donc essentielle afin de préserver le respect de la vie privée du patient et assurer le maintien du secret professionnel. Mais au-delà de la crainte d'une mauvaise protection des données, subsiste la crainte d'un mésusage des données collectées. Les TIC apparaissent ici comme un danger pour le respect de la finalité de ces données, pouvant mener à une utilisation à mauvais escient, voir, pire, une marchandisation de celles-ci. Il apparait alors évident que l'ensemble des utilisations qui pourraient aller à l'encontre de l'intérêt du patient doivent alors être interdites[27]. Toutefois, ces interdictions doivent être mises en perspective avec l'intérêt que présentent certaines

[24] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* du 5 mars 2002, p. 4118.
[25] GRIGUER, Merav. « Quel cadre légal pour l'e-santé ? », *Cahiers de droit de l'entreprise*, n° 5, 2016, prat. 25.
[26] VAYR, Jonathan. « Les données de santé, un enjeu pour le futur », *LPA*, septembre 2016, n° 185-186, p. 4.
[27] *Ibidem.*

données. Finalement, toute la difficulté repose dans les finalités pour lesquelles ces données dématérialisées vont être utilisées.

B. Les risques « d'ubérisation » de la médecine : la nouvelle crainte

L'introduction des TIC en santé a été immédiatement accompagnée de multiples craintes de la part des professionnels de santé, et plus spécifiquement de la communauté médicale.

23. Le Conseil National de l'Ordre des Médecins (CNOM) s'attache ainsi, depuis plusieurs années, à suivre de près l'évolution des TIC dans la pratique médicale, n'hésitant pas à réaliser de nombreuses études et rapports sur le sujet. Considérant que « *par son rôle de fédérateur des médecins, de toutes disciplines et de tous secteurs, réunis autour des mêmes principes déontologiques, [il] a la responsabilité de s'engager dans les projets de système d'information de santé au nom de l'avenir scientifique, mais dans le respect absolu des libertés individuelles* »[28] mais également que « *le respect absolu de la vie privée et des libertés individuelles est un impératif premier dans l'examen du développement utile des moyens informatiques* »[29], l'ordre accompagne les évolutions techniques qui viennent bouleverser l'exercice médical.

24. L'introduction des TIC dans la relation de soin a d'abord fait naitre, chez les médecins, la crainte d'une déshumanisation de l'acte médical. Les TIC apparaissaient aux yeux des médecins comme une barrière entre leurs patients et eux, créant de la distance et pouvant, ainsi, détériorer le colloque singulier nécessaire à la prise en charge du patient.
Mais, au-delà de ce risque, lié au changement des pratiques professionnelles, la communauté médicale, au travers du CNOM a récemment exprimé une crainte quant à « *l'ubérisation de la santé* », constatant « *un risque de dérive vers du commerce électronique non régulé qui*

[28] « L'informatisation de la santé », Livre blanc du CNOM, 2008, p. 1.
[29] « Télématique de santé », CNOM, 2006. Disponible sur [https://www.conseil-national.medecin.fr], p. 1, consulté le 15 mai 2017.

réduirait la pratique médicale à une simple prestation électronique moyennant rétribution, via des plateformes du secteur marchand »[30].

25. La notion d' "ubérisation" est très récente et ne possède pas de réelle définition. Elle peut être vue comme « une stratégie de contournement des règles, par l'utilisation optimale des Technologies de l'Information et de la Communication, et ce afin de fournir un accès facilité, plus rapide et en principe moins coûteux à un service »[31]. Dans le domaine de la santé, l'"ubérisation" se révèle par l'apparition, au sein de l'offre numérique, de services médicaux, qui s'affranchissent du cadre légal actuellement en place (notamment en ce qui concerne la télémédecine). Parmi ces offres dires "ubérisées", nous trouvons principalement des offres de téléconseil et de téléconsultation. A titre d'exemple, l'assureur AXA propose, dans le cadre de ses contrats d'assurance santé complémentaire, un service de téléconsultation, disponible 7 j/7 et 24h/24, permettant au patient de pallier l'indisponibilité (avérée ou supposée) de son médecin traitant. Ces offres, souvent à la limite de la légalité, viennent concurrencer l'offre existante. Par ailleurs, ces offres contreviennent totalement à certains principes déontologiques fondamentaux qui s'imposent aux médecins et notamment l'interdiction de pratiquer la médecine comme un commerce[32].

26. A ce sujet, le CNOM s'inquiète d'une tendance à l'augmentation des *« offres en ligne qui correspondent à du commerce électronique non régulé et qui tendent à réduire la pratique médicale à une simple prestation électronique moyennant rétribution, via des plateformes du secteur marchand* »[33].En effet, certaines offres dites de téléconseils tendent à se développer. Cette activité *« consiste à mettre en relation des internautes qui se connectent à un site avec un médecin qui leur fournit secondairement, à l'occasion d'un entretien téléphonique, "des informations personnalisées"*»[34]. Or, le téléconseil ne fait pas partie des cinq actes de télémédecine aujourd'hui reconnus et encadrés par le décret d'octobre 2010[35]. Se pose alors la question du cadre juridique, déontologique mais également éthique, dans lequel cette

[30] CNOM. « Télémédecine et autres prestations médicales électroniques », rapport de mission adopté lors de la session du Conseil national de l'Ordre des médecins de février 2016, p. 2.
[31] LEQUILLERIER, Clémentine. « "L'ubérisation" de la santé », *Dalloz IP/IT*, 2017, p. 155.
[32] Article R. 4127-19 du Code de la santé publique.
[33] CNOM. « Télémédecine et autres prestations médicales électroniques », *op. cit.*, p. 4
[34] Disponible sur [https://www.conseil-national.medecin.fr/article/teleconseil-personnalise-1155]. Consulté le 15 mai 2017.
[35]Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine, *JORF* n°0245 du 21 octobre 2010, texte n° 13.

prestation pourrait s'inscrire. Pour le CNOM, le téléconseil reste, quoi qu'il en soit, soumise aux dispositions du Code de déontologie médicale, en tant que prestation médicale. Il considère cependant que « l'offre marchande repose, pour une large part, sur la confusion qu'il est possible d'entretenir, auprès du grand public, entre la télémédecine – notamment la téléconsultation –, désormais définie par la loi, et des activités qui s'en réclament mais qui, il faut le souligner clairement, n'entrent pas dans le champ des nouveaux textes réglementaires »[36].

27. Face à ce phénomène, le CNOM tente d'interpeller les pouvoirs publics, se demandant, à juste titre, si l'Etat pouvait « *continuer de produire des textes réglementaires normatifs appliqués à l'exercice de la médecine utilisant des moyens numériques, et laisser prospérer des offres numériques non régulées sur le marché de la e-santé ?* ». En effet, l'ordre demande, depuis plusieurs années maintenant, à ce que ce secteur soit régulé afin d'éviter toutes dérives commerciales. Le CNOM souhaite que « le flou juridique soit levé. Il considère que l'exercice du téléconseil devrait donner lieu à une réglementation sanitaire spécifique et à des obligations contraignantes, assurant la sécurité des informations données à l'internaute, la protection des données personnelles de santé et leur caractère non marchandisable ».[37]

Nous pouvons alors observer les premières limites du cadre juridique des TIC en santé, la « *réglementation trop stricte de cette pratique [ayant] nui à son développement et [ayant] précisément favorisé l'émergence d'offres "ubérisées"*»[38].

28. Enfin, le développement de cette offre "ubérisée", en plus d'accentuer les risques déjà existants pour la protection des données du patient (les prestataires s'affranchissant des contraintes mises en place dans le cadre de la télémédecine), aura tendance à créer une offre de santé à deux vitesses, renforçant les inégalités existantes déjà en la matière. Or, utilisées à bon escient, les TIC peuvent, au contraire, réduire ces inégalités.

---

[36] « Déontologie médicale sur le web », *Le Livre blanc du Conseil national de l'Ordre des médecins*, décembre 2011, p. 29.
[37] *Idem*, p. 30.
[38] LEQUILLERIER, Clémentine. « L'"ubérisation" de la santé », *op. cit.*

§3. Problématique de la thèse

29. Notre problématique est partie d'un constat : celui des difficultés, pour les TIC en santé, de se développer de manière pérenne. A titre d'exemple, alors que « *malgré les ambitions et les incitations, la généralisation de la télémédecine progresse lentement* »[39], le Dossier Médical Partagé (DMP), projet phare des pouvoirs publics, institué par la loi n°2004-810 du 13 août 2004[40], peine à se défaire de son étiquette d'Arlésienne.

30. Se pose alors la question de savoir quels peuvent être les freins à ce développement. Au-delà des aspects purement économiques de certains projets (les TIC coûtent chers) et des difficultés à obtenir l'adhésion des acteurs face à des changements de pratiques, parfois très ancrées, de nombreuses difficultés juridiques jalonnent la voie du développement des TIC dans la prise en charge médicale. En effet, quand on en vient à réfléchir aux aspects juridiques liés à la mise en place des TIC dans la pratique médicale, nous ne pouvons que constater, très rapidement, que le droit occupe une place importante. De nombreuses questions vont se poser. Celles-ci ont trait à la pratique elle-même, qui, sous sa nouvelle forme dématérialisée, va poser des difficultés en termes de responsabilités mais également de droit des patients. Mais les questions concernent également l'encadrement de la mise en œuvre de ces pratiques : quel cadre applique-t-on à l'utilisation de ces nouveaux outils ? Comment sécurise-on et encadre-t-on ces pratiques ? D'ailleurs, doit-on les encadrer ? Enfin, l'introduction des TIC dans la pratique médicale a des impacts juridiques. C'est notamment le cas de l'informatisation massive des données de santé, conséquence directe de l'utilisation des TIC, et dont la gestion juridique sera nécessaire mais complexe.

31. Finalement, le Droit se dresse parfois devant ces nouvelles pratiques comme un obstacle. Les initiatives innovantes peuvent se trouver alors freinées par ce Droit, complexe, rigide, et parfois inadapté. Pourtant, celui-ci est loin d'être insurmontable. Des solutions peuvent être apportées afin de faire du Droit, non plus le frein mais bien l'accompagnateur, si ce n'est même le moteur du développement de l'utilisation des TIC dans la pratique médicale.

---

[39] VIOUJAS, Vincent. « La télémédecine : entre expérimentations réussies et généralisation au ralenti », *RDSS*, 2015, p. 681.
[40] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, *JORF* n°0190 du 17 août 2004, p. 14598.

32. Avec ces travaux, nous tenterons d'établir que, si le cadre juridique actuel n'est pas propice au développement serein et pérenne de l'utilisation des TIC dans la pratique médicale, des solutions existent afin de permettre aux établissements de santé de sécuriser leurs pratiques. Ainsi, dans un premier temps, nous étudierons de manière critique le cadre juridique qui s'applique aujourd'hui à l'utilisation des TIC dans la pratique médicale (Première partie), avant d'envisager les différentes pistes de sécurisation de ces pratiques, permettant d'assurer leur développement dans un contexte propice (Seconde partie).

PREMIERE PARTIE

LE CADRE JURIDIQUE DE L'UTILISATION DES TIC A L'HÔPITAL, UN CADRE INCOMPLET

« *[La] technique ne doit pas progresser plus vite que son contrôle* »[41].

33. En posant ce principe de base, simple et logique, le député M. Jean FOYER mettait en exergue ce qui est un des plus grands problèmes liés à l'utilisation des technologies d'information et de communication dans la pratique médicale. En effet, aujourd'hui, alors que la technique se développe régulièrement et que les sociétés proposent des solutions toujours plus innovantes, le législateur se montre, quant à lui, peu réactif et tarde à donner aux Technologies de l'Information et de la Communication le cadre règlementaire nécessaire à leur bon développement. Car il est certain que l'informatisation croissante de la pratique médicale ne peut être que bénéfique pour la prise en charge du patient, et les avancées en la matière offrent de nouvelles possibilités chaque jour. A titre d'exemple, désormais les radiographies sont plus souvent numérisées et conservées sur des logiciels spécialisés. De même, les hôpitaux investissent désormais dans des logiciels de gestion informatisée des dossiers médicaux, et la prescription informatisée se développe de plus en plus, les Agences Régionales de Santé (ARS) incitant à leur utilisation par le biais des contrats de bon usage notamment[42].

34. Toutefois, force est de constater que le législateur n'a pas su accompagner en temps et en heure ce développement fulgurant. Alors que la France se posait comme l'un des précurseurs en la matière en adoptant, en 1978, une législation encadrant le traitement des données à caractère personnel, elle a ensuite perdu sa longueur d'avance, tardant à transposer la directive européenne de 1995[43], et proposant ensuite des cadres incomplets, difficiles à respecter voire même pour certains, totalement inapplicables.

35. A l'heure actuelle, l'encadrement législatif et règlementaire propre à l'utilisation des TIC dans la pratique médicale présente un visage flou et complexe. En ce qui concerne la

---

[41] FOYER, Jean. « Rapport au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur : le projet de loi (n° 2516) relatif à l'informatique et aux libertés, la proposition de loi (n° 1004) de Pierre-Bernard Cousté tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens , la proposition de loi (n° 3092) de François Villa et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique », *Assemblée Nationale*, t.1, n° 3125, Paris, 1977, p. 13.

[42] Décret n° 2015-355 du 27 mars 2015 relatif au contrat de bon usage des médicaments et des produits et prestations mentionné à l'article L. 162-22-7 du code de la sécurité sociale, *JORF* du 29 mars 2015, p. 5763.

[43] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JO* n° L 281 du 23 novembre 1995, p. 31.

gestion globale et l'utilisation des données du patient, le cadre de leur traitement informatique peut paraitre trop général et par conséquent inadapté (titre premier, chapitre premier), tandis que les règles relatives à leur hébergement et leur communication peuvent sembler illisibles et parfois insuffisantes (titre premier, chapitre second). L'utilisation des TIC dans le cadre de la prise en charge des patients ne bénéficie pas non plus d'un encadrement adéquat : d'une part le développement de la dématérialisation des dossiers médicaux montre les limites des règles en place (titre second, chapitre premier), d'autre part, la réalisation d'actes de soins, via les TIC souffre d'un cadre incomplet, quand il n'est pas inexistant (titre second, chapitre second).

TITRE 1

TIC ET INFORMATISATION DES DONNEES DE SANTE : UN CADRE PARFOIS INADAPTE

36. Les données relatives au patient, qu'il s'agisse des données strictement administratives telles que leur nom, leur adresse ou encore leur numéro de sécurité sociale, ou des données médicales les concernant, sont fondamentalement nécessaires à la bonne prise en charge de celui-ci. Elles doivent donc être recueillies, ordonnées et conservées. Ces données sont un bien précieux pour les professionnels de santé à de nombreux égards. Elles leur permettent d'apporter aux patients les meilleurs soins possibles, sécuriser leur diagnostic et assurer la bonne coordination des soins. Les données constituent également une source de matière première pour les recherches médicales.

37. Aujourd'hui, l'introduction des TIC dans la pratique médicale va avoir pour conséquence une informatisation massive de ces données, qui vont être dématérialisées, enregistrées, stockées et partagées par le biais de systèmes informatiques. Cette informatisation de données particulièrement sensibles, doit être accompagnée d'un cadre juridique adéquat, afin d'assurer aux patients une protection efficace de leur vie privée.

38. Notre réflexion va nous amener à nous pencher, dans un premier temps, sur l'encadrement juridique du traitement informatisé des données, cadre de droit commun, parfois inadapté aux TIC en santé (chapitre 1). Puis, dans un second temps, nous nous pencherons sur les modalités actuellement en place en matière de conservation et de communication des informations du patient (chapitre 2).

Chapitre 1

Le traitement informatisé des données du patient

39. Le traitement systématique des données relatives au patient n'est pas nouveau. Les toutes premières traces de dossier médical datent du IXème siècle. RHAZES, médecin arabe, avait l'habitude de conserver les cas qu'il estimait intéressants dans un registre intitulé « observation de l'hôpital ». L'ensemble a ensuite été publié dans l'ouvrage « *continens* ». La notion de dossier médical pour chaque patient n'apparaît qu'à la fin du XVIIIème siècle mais son contenu reste succinct. Ce n'est qu'au XIXème siècle que le dossier médical en tant que tel apparaît : il contient alors les données médicales ainsi que les données administratives du patient. Les médecins de ville vont, eux aussi, formaliser petit à petit des fiches d'information relatives à leurs patients. Aujourd'hui, la tenue d'un dossier médical est, pour les établissements de santé, une obligation règlementaire, codifiée à l'article R. 1112-2 du Code de la santé publique.[44] Un dossier médical doit être constitué pour chaque patient, contenant *a minima* certaines informations obligatoires (et notamment les motifs de l'hospitalisation, les conclusions de l'évaluation clinique initiale, les résultats des différentes examens et analyses, le dossier de soins infirmiers). Ce dossier médical doit d'ailleurs être conservé pour une durée de 20 ans après le dernier passage du patient à l'hôpital.

40. Depuis plusieurs années, l'introduction puis le développement massif des TIC à l'hôpital a transformé le traditionnel dossier papier en dossier informatisé. Parfois craint, souvent appréhendé, ce passage au "tout informatique" ne crée pas forcément de risques nouveaux. Toutefois, une attention particulière doit être portée aux traitements des données du patient. Pour cela, leur protection est un préalable nécessaire (section I). Celle-ci est assurée par un corpus de textes épars dont l'efficacité peut se révéler relative. De même, leur partage est soumis au respect de certaines conditions, qui vont être différentes selon le but recherché par leur utilisation (section II).

[44] L'article R. 1112-2 du Code de la santé publique prévoit qu'« *un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé* ».

Section 1. La protection des données du patient

41. En matière de protection des données du patient, il faut se référer à la législation de droit commun qui existe en la matière, à savoir la loi Informatique et Libertés. En effet, les principes généraux édictés par cette loi trouveront à s'appliquer en matière de données de santé (paragraphe I), même si celle-ci est complétée par quelques dispositions particulières aux données de santé. Toutefois, cet état des lieux pointe les lacunes des protections mises en place (paragraphe II).

§1. La législation de droit commun à disposition du droit de la santé

42. La loi n° 78-16 du 6 janvier 1978 dite « loi Informatique et Libertés »[45] a été l'une des premières lois protégeant les données à caractère personnel en encadrant leur traitement en Europe. Cette loi, réformée en 2004[46], affiche une volonté d'apporter une protection forte (A). En ce qui concerne les données de santé, cette protection est toutefois complétée par des dispositions spécifiques à ces données (B)

A. La loi Informatique et Libertés, pilier de l'encadrement

43. La France est une pionnière en matière d'encadrement des traitements de données à caractère personnel (1) et la loi Informatique et Libertés marque la volonté du législateur d'instaurer une protection forte (2).

1) La France parmi les précurseurs

44. Au cours des années 1970, l'utilisation de l'informatique se développe, notamment dans les administrations publiques. Toutefois, l'opinion publique craint une augmentation des

[45] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* du 7 janvier 1978, p. 227.
[46] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* du 7 août 2004, p. 14063.

atteintes aux libertés publiques ainsi qu'une violation de la sphère privée. Cette crainte est particulièrement bien exprimée dans l'article de Philippe BOUCHER, intitulé « SAFARI ou la chasse aux français »[47]. Celui-ci expose au grand jour un projet, dénommé Système automatisé pour les fichiers administratifs et le répertoire des individus (SAFARI), « *qui devait permettre, à partir du répertoire national d'identification des personnes physiques, de faciliter les intercommunications entre les fichiers qui auraient recours au numéro national d'identité, soit comme base de classement, soit comme élément de référence* »[48]. Or, comme le révélait l'article de Pierre BOUCHER, et contrairement aux recommandations émises par le Conseil d'Etat, le Premier Ministre de l'époque, Pierre MESSMER, avait écarté tout projet de débat public sur les projets d'informatisation du gouvernement. L'opinion publique, vivement émue, amena le Premier Ministre à constituer une commission, présidée par le vice-président du Conseil d'Etat, Bernard CHENOT, et chargée de proposer des mesures permettant de garantir que le développement de l'informatique dans les secteurs public, semi-public et privé se réalise dans le respect de la vie privée, des libertés individuelles et des libertés publiques. Le rapport[49] de cette commission, rédigé par Bernard TRICOT et le Professeur Pierre CATALA, fut remis le 27 juin 1975. C'est sur la base de ce rapport que le projet de loi relatif à l'informatique et aux libertés fut rédigé.

45. Pour autant, la France, bien qu'en avance sur de nombreux pays, n'était pas le premier à légiférer sur le sujet. En effet, avant cela, l'Allemagne avait adopté une loi relative au traitement automatisé des informations nominatives en octobre 1970. Elle fut rapidement suivie par la Suède qui adopta une loi sur le même sujet en 1973. Hors Europe, les Etats-Unis adoptèrent, quant à eux, un Privacy Act en 1974, dont l'application est toutefois limitée aux fichiers détenus par les administrations fédérales.

46. En France, plusieurs propositions de loi relatives au sujet vont être déposées successivement auprès de l'Assemblée Nationale : la première émanant de Pierre-Bernard

---

[47] BOUCHER., Pierre. « SAFARI ou la chasse aux français », *Le Monde*, 21 mars 1974.

[48] FOYER, Jean. « Rapport au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur : le projet de loi (n° 2516) relatif à l'informatique et aux libertés, la proposition de loi (n° 1004) de Pierre-Bernard Cousté tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens , la proposition de loi (n° 3092) de François Villa et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique », *op. cit.*

[49] CATALA, Pierre. TRICOT, Bernard. « Rapport de la commission Informatique et Libertés », *La Documentation française*, Paris, 1975.

COUSTE et tendant à créer une commission de contrôle des moyens informatiques afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens et une autre émanant de François VILLA et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique. De même, un projet de loi relatif à l'Informatique et aux Libertés va également être présenté. Ces trois textes feront l'objet d'un rapport commun de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République[50].

47. La loi relative à l'informatique, aux fichiers et aux libertés va être adoptée le 6 janvier 1978. Elle comporte alors des dispositions organiques (création de la commission nationale de l'informatique et des libertés – CNIL) ainsi que des dispositions matérielles[51]. Très symbolique, l'article premier de la loi dispose : « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés publiques ou individuelles* ».

48. Au niveau international, une crainte du développement de législations trop protectrices est alors apparue. Ainsi, l'Organisation de Coopération et de Développement Economique (OCDE), le 23 septembre 1980, arrêta des lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel, dénuées de force obligatoire, mais ayant pour ambition d'éviter que la protection des données personnelles n'entrave la libre circulation de l'information ainsi que le développement des relations économiques et sociales des pays membres. Le Conseil de l'Europe adopta quant à lui la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel**,** dite « convention 108 », signée le 28 janvier 1981 et ayant pour but de concilier la protection de la vie privée avec la libre circulation de l'information entre les peuples[52].

---

[50] FOYER, Jean. « Rapport au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur : le projet de loi (n° 2516) relatif à l'informatique et aux libertés, la proposition de loi (n° 1004) de Pierre-Bernard COUSTE tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens , la proposition de loi (n° 3092) de François Villa et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique », *op. cit.*

[51] *V. Infra*. n° 52 et s.

[52] Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, disponible sur [http://www.coe.int/fr/], consulté le 15 mai 2017.

49. En 1995, afin de réduire les divergences qui peuvent exister entre les législations des différents Etats, l'Union Européenne adopta la directive 95/46/CE relative à la protection des données personnelles et à la libre circulation de ces données[53]. L'ambition de cette directive était de prendre en compte trois évolutions majeures en matière d'informatisation des données, à savoir la marchandisation des données, l'internationalisation des flux et le phénomène de traçabilité.[54] Les Etats membres avaient alors jusqu'au 25 octobre 1998, date d'entrée en vigueur de la directive, pour la transposer.

50. Toutefois, en France, la procédure va s'avérer très longue. Le 12 septembre 1997, le Premier Ministre de l'époque confie à Guy BRAIBANT un travail préparatoire à l'élaboration d'un avant-projet de loi en vue de la transposition de la directive de 1995. Le 3 mars 1998, Guy BRAIBANT remet son rapport[55] dans lequel il expose notamment les enjeux de la transposition mais formule également plusieurs propositions afin de maintenir un haut niveau de protection des libertés. Puis, entre le 5 octobre et le 5 décembre 1999, une consultation publique est lancée sur le futur projet de loi intitulé « société de l'information ». Le projet de loi relatif à la protection des données à caractère personnel est présenté à l'occasion d'un conseil des ministres, le 18 juillet 2001. Toutefois, suite aux différents examens, la loi n'entrera en vigueur que le 7 août 2004, et la France sera parmi l'un des derniers pays à transposer la directive. Ainsi, la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel remanie profondément la loi du 6 janvier 1978. De façon très symbolique, l'article premier de la loi a été conservé.

51. A l'heure actuelle, la protection des données personnelles reste un sujet très important en France et en Europe. La CNIL a, depuis plusieurs années, fait connaître sa volonté de renforcer ce principe de protection des données personnelles, en préconisant notamment une constitutionnalisation du principe. Au niveau européen, une révision du cadre existant a par ailleurs été initiée en 2012 avec une proposition de règlement européen réformant le cadre de

---

[53] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *JOUE* n° L 281 du 23 novembre 1995, p. 31.

[54] DESGENS-PASANAU, Guillaume. « La protection des données à caractère personnel », *Lexis-Nexis*, 2ème édition, Paris, 2016, p. 5.

[55] BRAIBANT, Guy. « Données personnelles et sociétés de l'information. Rapport au premier ministre », *La Documentation française*, 1998.

la protection des données à caractère personnel[56], adoptée le 25 janvier 2012 par la Commission Européenne. Afin d'instaurer une politique plus générale et cohérente en matière de protection des données à caractère personnel, le législateur européen a fait le choix d'utiliser le règlement comme instrument juridique. En effet, l'article 288 du traité sur le fonctionnement de l'Union Européenne prévoyant l'applicabilité directe des règlements, l'utilisation de cet outil permet d'éviter les transpositions limitées et surtout très longues comme ce fut le cas avec la directive de 1995. Les débats ont tout de même duré quatre ans, puisque ce n'est qu'en avril 2016 que ce texte a été définitivement adopté[57].

Nous ne nous attarderons pas ici sur les apports particuliers de cette proposition de règlement en matière de protection des données à caractère personnel, ces éléments étant abordés tout au long de ces travaux. Il est simplement nécessaire à ce stade de constater la volonté au niveau européen d'instaurer un cadre unifié et solide et ce dans un but double : protéger les données à caractère personnel et favoriser l'utilisation des Technologies de l'Information et de la Communication.

2) Une protection forte

52. La loi Informatique et Libertés avait pour ambition d'apporter un cadre très protecteur au traitement des données à caractère personnel. Les modifications subies par la loi initiale, suite à la transposition de la directive européenne 95/46/CE du 24 octobre 1995 vont également en ce sens. Avec la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le législateur montre une réelle volonté d'instaurer une protection forte vis-à-vis de ce type de données. Pour ce faire, il est prévu à la fois une protection *a priori* et une protection *a posteriori*.

---

[56] Proposition de règlement du parlement européen et du conseil 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, n°2012/0011, 25 janvier 2012.

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

53. La protection *a priori* relève à la fois de l'encadrement mis en place par les textes, mais également des formalités à accomplir préalablement à tout traitement de données à caractère personnel. Certaines conditions de licéité des traitements sont posées dès les premiers articles de la loi. Ainsi, l'article 6 dispose que : « *les données sont collectées de manière loyale et licite […] pour des finalités déterminés, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités […] elles sont adéquates, pertinentes et non excessives […] elles sont exactes, complètes et, si nécessaire, mises à jour,[…] elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ».

54. Nous pouvons constater que l'accent est mis ici sur le respect du principe de proportionnalité. Ce principe, bien qu'il ne figure pas dans la Constitution, est régulièrement invoqué par le Conseil constitutionnel dans ses décisions. Les données collectées doivent avant tout répondre à une finalité bien précise et ne pas être disproportionnées par rapport au but recherché. Le principe de proportionnalité apparaît également au travers de l'obligation de conserver ces données pour une durée limitée et adaptée aux besoins du traitement. Les données ne peuvent être conservées que pour une durée strictement définie. La législation consacre ici le principe de "droit à l'oubli"[58]. Ce principe de proportionnalité permet d'assurer un certain équilibre entre droits des personnes concernées par les données traitées et intérêts du responsable du traitement.

55. La seconde exigence préalable à tout traitement est posée à l'article 7 de la loi Informatique et Libertés : « *un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée* ». Cette exigence permet de s'assurer d'une part que les personnes concernées par les données sont au courant de l'utilisation qui va en être faite et d'autre part qu'ils en sont d'accord. Toutefois, il est utile de préciser que ce même article, qui prévoit l'obligation de consentement, introduit immédiatement une liste d'exceptions. Ainsi, le consentement de la personne concernée par les données traitées ne sera pas nécessaire si le traitement satisfait à l'une des conditions suivantes : « *le respect d'une obligation légale incombant au responsable du traitement, la sauvegarde de la vie de la personne concernée,*

[58] DESGENS-PASANAU, Guillaume. « La protection des données à caractère personnel », *op. cit.*, p. 41.

l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement, l'exécution soit d'un contrat auquel la personne concernée est partie soit de mesures contractuelles prises à la demande de celle-ci, la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire sous réserve de ne pas méconnaitre l'intérêt ou les droits et libertés fondamentaux de la personne concernée. ». En outre, le responsable du traitement devra le déclarer auprès de la CNIL. Différentes formes de déclarations existent et celle qui devra s'appliquer dépendra de la finalité poursuivie par le traitement et non pas de l'application utilisée pour mettre en œuvre le traitement. Ces différents régimes sont traités au sein du chapitre IV de la loi Informatique et Libertés, intitulé « Formalités préalables à la mise en œuvre des traitements ». Le régime de droit commun est celui de la déclaration normale, décrite à l'article 23 de la loi Informatique et Libertés et applicable à tous les traitements qui ne relèveraient pas d'une procédure spécifique. Il s'agit en réalité d'un engagement de la part du responsable du traitement, qui certifie que son traitement est conforme aux exigences de la CNIL.

56. Afin de gérer au mieux les différentes déclarations, mais également de faciliter les traitements de données dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée et aux libertés, il est également prévu que la CNIL puisse établir des normes afin de simplifier les obligations de déclaration. A titre d'exemple, la norme simplifiée n° 50 relatif à la gestion des cabinets médicaux et paramédicaux[59] permet aux professionnels de santé libéraux de déposer une simple déclaration de conformité à cette norme afin d'être en règle avec la législation. Cette norme s'applique à la gestion courante des cabinets médicaux, qu'il s'agisse des dossiers médicaux, de la télétransmission des feuilles de soins ou encore de la comptabilité. La CNIL peut également, en vertu des dispositions prévues à l'article 24 de la loi Informatique et Libertés, décider que certaines catégories courantes de traitements, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés compte tenu de leur finalité, de leur destinataire, des données à caractère personnel traitées, de leur durée de conservation et des catégories de personnes concernées, peuvent être dispensées de déclaration. La liste de ces traitements est publiée au Journal Officiel. C'est le cas par exemple de la dispense accordée aux organismes publics pour la dématérialisation des

[59] Délibération n° 2005-296 du 22 novembre 2005 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les membres des professions médicales et paramédicales exerçant à titre libéral à des fins de gestion de leur cabinet, *JORF* n°7 du 8 janvier 2006, texte n° 19.

marchés publics[60]. La CNIL peut également, dans le cas de traitement relevant d'un même organisme ou ayant des finalités identiques ou liées entre elles, autoriser les responsables du traitement à procéder à une déclaration unique[61].

57. Pour les données considérées comme étant plus sensibles, une autorisation préalable de la CNIL sera nécessaire. Ce régime particulier s'applique aux données sensibles citées aux III et IV l'article 8 de la loi[62], mais également : « *aux traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements, aux traitements portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, aux traitements automatisés susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire aux traitements automatisés ayant pour objet : l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents, l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes, les traitements portant sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques et ceux qui requièrent une consultation de ce répertoire sans inclure le numéro d'inscription à celui-ci des personnes, les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes, les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.* »

58. Contrairement à la procédure de déclaration normale, le traitement envisagé va faire l'objet d'un examen de la part de la CNIL qui dispose d'un délai de deux mois, renouvelable une fois sur décision motivée de son président, pour se prononcer et autoriser ou non la mise en œuvre du traitement. En l'absence de réponse de la part de la CNIL dans le délai imparti, la demande d'autorisation est réputée rejetée et le responsable du traitement pourra engager un recours en annulation auprès du Conseil d'Etat.

---

[60] Délibération n° 2005-003 du 13 janvier 2005 décidant la dispense de déclaration des traitements mis en œuvre par les organismes publics dans le cadre de la dématérialisation des marchés publics, *JORF* n° 55 du 6 mars 2005, texte n° 32.
[61] Article 24, II, de la loi Informatique et Libertés.
[62] *V. Infra.* n° 63.

59. La protection mise en place par la loi Informatique et Libertés passe également par la consécration de droits fondamentaux pour les personnes concernées par les données traitées. Ces droits, exposés au sein du chapitre V de la loi, sont au nombre de quatre : droit d'information, droit d'accès, droit de rectification et de radiation et le droit d'opposition. Le droit d'information, prévu à l'article 32 de la loi, consiste pour la personne concernée par les données, à être informée d'une manière générale sur le traitement dont ses données vont faire l'objet. Elle doit notamment être informée sur l'identité du responsable du traitement, de la finalité du traitement, du ou des destinataires des données, des droits qu'il détient en vertu de la loi Informatique et Libertés et, le cas échéant, du transfert des données au sein d'un état non membre de l'Union Européenne. Ce droit nous apparaît comme essentiel puisqu'il va permettre à la personne concernée par le traitement, d'une part de donner un consentement éclairé au traitement et d'autre part, d'être clairement informée des autres droits qu'elle détient à l'égard de ses données.

La loi Informatique et Libertés prévoit également le droit, pour toute personne physique, de s'opposer à ce que ses données fassent l'objet d'un traitement et ce, à condition d'avoir des raisons légitimes. L'opposition devra donc être motivée et l'appréciation du caractère légitime ou non de l'opposition reviendra donc au responsable du traitement. Cette notion de « motifs légitimes » n'est malheureusement pas définie dans les textes et ni la CNIL, ni le juge n'ont eu à se prononcer à ce sujet pour l'instant.

Le droit d'accès, posé à l'article 39 de la loi Informatique et Libertés, permet à toute personne physique justifiant de son identité d'interroger le responsable d'un traitement afin d'obtenir confirmation que ses données font ou ne font pas l'objet d'un traitement.

Enfin, il est prévu que toute personne physique ait droit d'exiger que ses données soient « *rectifiées, complétées, mises à jour, verrouillées, ou effacées* ». Toutefois, les données concernées doivent être inexactes, incomplètes, périmées ou encore équivoques ou tout simplement frappées d'une interdiction de traitement.

60. Avec la loi Informatique et Libertés, le législateur a donc essayé de mettre en place la protection des données à caractère personnel la plus complète possible, garantissant aux personnes concernées par un traitement de données, des droits fondamentaux, assurant un contrôle *a priori* et *a posteriori* des traitements effectués. Ces garanties ont d'ailleurs été

jugées comme présentant un caractère approprié par le Conseil d'Etat dans une décision rendue le 19 novembre 1992[63].

B. La protection spécifique des données de santé

61. Les données de santé sont des données à caractère personnel assez particulières. En effet, elles touchent de très près à l'intimité de la personne et leur communication rend la personne qu'elles concernent vulnérable. Cette particularité leur vaut d'appartenir à une catégorie spécifique de données, puisqu'elles sont considérées par la loi Informatique et Libertés comme étant des "données sensibles" (1). En complément des protections instaurées par la loi Informatique et Libertés, les données de santé bénéficient ainsi de protections qui leurs sont propres (2).

1) Les données de santé, des données sensibles

62. Bien qu'il soit depuis longtemps acquis que les données de santé sont des données particulièrement sensibles, la définition légale de la notion de données de santé n'est apparue que très récemment.

63. La loi Informatique et Libertés définit clairement la notion de données à caractère personnel comme étant « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». Toutefois, elle ne revient pas précisément sur la notion de données de santé. Elle se contente juste de préciser, dans son article 8, qu' « *il est interdit de collecter ou de traiter des données à caractère personnel […] qui sont relatives à la santé* ». La directive européenne de 1995 n'est pas beaucoup plus précise sur la notion de données de santé. C'est un arrêt de la CJCE, en date du 6 novembre 2003 qui a apporté les premières précisions sur cette notion.[64] En l'espèce, le Göta hovrätt (Suède) avait posé, par ordonnance du 23 février 2001, sept questions préjudicielles sur l'interprétation de la directive 95/46/CE. La quatrième de ces questions demandait à la Cour de préciser si « *l'indication, sur une page d'accueil, qu'un collègue de travail mentionné par*

[63] CE, 18 novembre 1992, LICRA, n° 115367, Rec., 1992 , p. 411 ; *AJDA*, 1993, p. 213.
[64] CJCE, 6 novembre 2003, aff.n°C-101/01, Suède c/ Lindqvist.

son nom s'est blessé au pied et est en congé de maladie partiel est-elle une donnée à caractère personnel relative à la santé qui, aux termes de l'article 8 paragraphe 1, ne peut faire l'objet d'un traitement ? ». Face à cette question, la CJCE va apporter une réponse simple : « *Eu égard à l'objet de cette directive, il convient de donner à l'expression "données de santé" employée à son article 8, paragraphe 1, une interprétation large de sorte qu'elle comprenne des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne* ». La CJCE se montre par conséquent assez large sur la définition de la notion de données de santé. Et elle n'est d'ailleurs pas la seule dans ce cas.

64. Dans sa transposition de la directive 95/46/CE, le Grand-Duché du Luxembourg, contrairement à la France, a défini les données relatives à la santé comme étant « *toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques* »[65]. La définition est légèrement plus large en ce qu'elle regroupe expressément les données génétiques. Cette intégration est compréhensible, bien que les données génétiques, qui regroupent les caractères héréditaires d'un individu, ne concernent pas à proprement parlé un aspect de la santé d'un individu, mais touchent en revanche indéniablement à son intimité.

65. Le Groupe de l'article 29[66] se montre également très large dans la définition qu'il donne de la notion. Ce groupe s'est penché à plusieurs reprises sur la problématique liée à la protection des données de santé. Ainsi, dans un document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques, adopté le 15 février 2007, le groupe de travail reprend la définition posée par l'arrêt Lindqvist et la complète en précisant que : « *cette définition s'applique également aux données à caractère personnel lorsqu'elles présentent un lien clair et étroit avec la description de l'état de santé d'une personne : les données sur la consommation de*

[65] Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, Art 2 g) du journal officiel du Grand-Duché du Luxembourg, « Recueil des législations », A n° 91, du 13 août 2002.

[66] Le groupe de l'article 29, ou Article 29 data protection working party est un organe consultatif européen indépendant sur la protection des données et de la vie privée établi en vertu de l'article 29 de la directive n° 95/46/CE. Ce groupe, consultatif et indépendant, est composé de représentants des autorités nationales chargées de la protection des données à caractère personnel, d'un représentant de l'autorité crée pour…et d'un représentant de la commission européenne. Ses missions sont définies à l'article 30 de la directive. Il s'agit principalement de donnée des avis sur les questions relatives à la protection des données à caractère personnel mais également promouvoir et contribuer à une application uniforme de la directive.

médicaments, d'alcool ou de drogue et les données génétiques sont incontestablement des données à caractère personnel relatives à la santé […] en outre, toutes autres données – par exemple des données administratives (numéro de sécurité sociale, date d'admission à l'hôpital) – contenues dans les documents médicaux relatifs au traitement d'un patient doivent être considérées comme sensibles ». Le Groupe de l'article 29 franchit un cap supplémentaire en intégrant les données administratives à la catégorie des données de santé, à partir du moment où celles-ci sont contenues dans les dossiers médicaux. Il justifie sa position au regard de la pertinence présumée de ces données dans le cadre de la prise en charge du patient. Nous pouvons noter ici le lien entre la définition de la notion de données de santé que tente d'esquisser le Groupe de l'article 29 et le champ couvert par le secret professionnel. En effet, l'article L. 1110-4 du Code de la santé publique prévoit que le secret « *couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé* ». Il nous semble dès lors raisonnable d'affirmer si ces données sont couvertes par le secret professionnel, c'est bien du fait de leur caractère sensible. Dès lors, la définition des données de santé ne peut pas être moins vaste que cela. A ce sujet d'ailleurs, le Groupe Européen d'Ethique, dans une décision rendue le 30 juillet 1999, avait défini le périmètre des données de santé comme englobant « *un large éventail d'informations qui, touchent à la vie privée de la personne concernée. Elles incluent non seulement les données médicales de base [...] mais aussi des données individuelles sensibles telles que celles relatives à l'état psychique de la personne, à ses antécédents familiaux, à ses habitudes de vie, y compris sa vie sexuelle, à sa situation sociale et économique, ainsi que des données de nature administrative* ».

66. Le règlement européen relatif à la protection des données personnelles[67], adopté en avril 2016, donne enfin une définition légale à la notion de donnée de santé. Ainsi, selon les dispositions de l'article 4 de ce règlement, les données concernant la santé sont définies comme « *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* ».

[67] Règlement 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 du 4 mai 2016.

67. Cette définition très succincte s'inscrit dans la lignée de celles proposées jusqu'alors dans le sens où elle se veut le plus large possible. Toutefois, nous pensons qu'il aurait été préférable d'inclure de manière explicite les données administratives, comme c'était le cas dans la définition avancée par le Groupe de l'article 29 ou encore par le Groupe Européen d'Ethique. Toutes les données relatives au patient et servant de manière directe ou non à sa prise en charge devraient pouvoir bénéficier de la même protection renforcée du fait de leur sensibilité mais également afin d'assurer une certaine cohérence.

68. Le caractère particulièrement sensible de ces données a amené le législateur à adopter des dispositions spécifiques à celles-ci. Ainsi, le traitement de ces données est, en principe, interdit : « *il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci*.»[68]

69. Toutefois, à chaque principe son exception et les dispositions de la loi Informatique et Libertés ne dérogent pas à la règle. Cette exception est d'ailleurs posée tout de suite après le principe.[69] En effet, le II de l'article 8 de la loi Informatique et Libertés dresse une liste de

---

[68] Article 8 de la loi Informatique et Libertés.

[69] L'article 8 II de la loi Informatique et Libertés dispose : *« Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I :*
1° *Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;*
2° *Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;*
3° *Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :*
- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ;
- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;
- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
4° *Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;*
5° *Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;*
6° *Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en oeuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du Code pénal ;*
7° *Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ;*

huit exceptions pour lesquelles le traitement d'une donnée *a priori* sensible peut toutefois être autorisé. Ainsi, même si les données sensibles sont frappées d'une interdiction de traitement, comme nous pourrons le constater dans la suite de notre réflexion, ce sont bien les exceptions qui trouveront à s'appliquer la majeure partie du temps.

2) Des mécanismes de protection propres aux données de santé

70. La loi Informatique et Libertés n'est pas le seul texte organisant la protection des données de santé et d'autres protections les concernant existent au sein du Code de la santé publique. Toutefois, bien que présentes au sein d'un même code, celles-ci sont éparses et il n'existe pas réellement de coordination entre les différents textes. Nous ne nous attarderons pas ici sur l'encadrement spécifique qui existe en matière d'hébergement des données de santé et de confidentialité, ces cas spécifiques faisant l'objet d'un développement ultérieur[70] et préférons concentrer notre réflexion sur les protections de droit commun relatives aux données de santé.

Deux dispositions doivent donc être étudiées : la protection des données assurée par le secret professionnel et le rôle joué par le médecin responsable de l'information médicale.

71. *« Il n'y a pas de soins sans confidences, de confidences sans confiance, de confiance sans secret »*[71]. Comme le rappelle Bernard HOERNI, le secret médical est le pilier de la relation entre le médecin et son patient car il permet de préserver le colloque singulier nécessaire à l'instauration d'une relation de confiance. La jurisprudence a très tôt affirmé le caractère absolu du secret médical. Dans une décision rendue le 9 décembre 1885, connue sous le nom de l'arrêt WATELET, la Cour de cassation avait décidé que l'obligation de secret professionnel s'imposait aux médecins comme un devoir de leur état, qualifiant cette obligation de générale et absolue, personne ne pouvant les en affranchir[72]. Aujourd'hui, l'obligation de secret médical a été introduite au Code de la santé publique et elle s'impose

---

8° *Les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX.* »

[70] *V. Infra*. n° 155 et s.

[71] HOERNI, Bernard. « Ethique et déontologie médicale », 2ème édition, *Masson*, Juin 2000.

[72] Cass. crim., 19 décembre 1885, Watelet, *Bull. cri*n° 363 et S. ; *V.* également en ce sens : Cass. Crim., 8 mai 1947, Decraene, *Bull. Crim*. n° 124.

aussi bien aux médecins, qu'à toutes les personnes intervenant dans la prise en charge du patient.

72. Ainsi, l'article 4 du Code de déontologie médicale, transposé à l'article R. 4127-4 du Code de la santé publique prévoit : « *le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris*.». La loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé[73] a renforcé le secret médical et l'a étendu à toutes les personnes participant de manière directe ou indirecte à la prise en charge du patient. Ainsi, l'article L. 1110-4 du Code de la santé publique prévoit : « *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 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 le concernant. Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues 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. […]* ». Ainsi, du secret médical, nous sommes passés au secret professionnel, dont la violation peut entrainer des sanctions civiles, disciplinaires et pénales. A ce titre, le Code pénal sanctionne la violation du secret professionnel d'un an emprisonnement et de 15 000 Euros d'amende.[74]

73. La protection apportée par le secret médical vient renforcer celle offerte par la loi Informatique et Libertés. Il faut toutefois s'attarder sur la différence qui existe entre la notion d'information concernant la personne, couverte par le secret professionnel selon les dispositions de l'article L. 1110-4 du Code de la santé publique et la notion de données à

[73] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* du 5 mars 2002, p. 4118.
[74] Article 226-13 du Code pénal.

caractère personnel relatives à la santé (ou données de santé) dont la protection est assurée par la loi Informatique et Libertés[75]. Il faut faire attention à ne pas aller trop vite et considérer comme référant à la même chose deux notions qui, en réalité, ne se recoupent pas totalement[76]. Une information peut être définie comme étant toute « *indication, renseignement, précision que l'on donne ou que l'on obtient sur quelqu'un ou sur quelque chose* »[77], tandis que la donnée est définie comme étant une *« représentation d'une information sous forme conventionnelle destinée à faciliter son traitement. »*[78]. La donnée est donc une information valorisée qui possède une valeur ajoutée d'ordre technologique[79]. Ainsi, alors que la simple information médicale ne sera protégée que par le secret professionnel (c'est le cas par exemple de l'information orale donnée par le patient à son médecin qui ne serait pas retranscrite au dossier médical), la donnée de santé se verra offrir une double protection : celle prévue par la loi Informatique et Libertés, d'une part, et celle assurée par l'obligation de secret professionnel, d'autre part. Cette double protection, véritable garantie pour le patient, peut toutefois s'avérer pesante pour le professionnel de santé, qui devra s'assurer que toutes les obligations vis-à-vis d'une seule et même donnée soient remplies, sous peine de voir sa responsabilité engagée.

74. L'autre protection majeure garantie aux données de santé est celle assurée par le médecin responsable de l'information médicale. Ce dispositif, prévu au Code de la santé publique, s'inscrit dans un cadre particulier qui est celui de l'utilisation des informations médicales dans un but d'analyse de l'activité : le Programme de Médicalisation des Systèmes d'Information, ou PMSI, instauré par l'ordonnance du 24 avril 1996[80].

75. Un « *praticien responsable de l'information médicale* » doit être désigné dans tout établissement de santé par le directeur général après avis de la commission médicale d'établissement.[81] Les conditions exactes de sa désignation et les modes d'organisation de la fonction auraient dû être fixées par un décret qui n'a pas été publié. Bien que ces modalités ne

---

[75] LAUDE, Anne. TABUTEAU, Didier. « Droit de la santé », *PUF*, 2007, p. 321.
[76] DE LAMBERTERIE, Isabelle. LUCAS, Henri-Jacques. « Informatique, libertés et recherche médicale », *CNRS éd.*, 2001, p. 68.
[77] Définition du dictionnaire Larousse.
[78] DE LAMBERTERIE, Isabelle. « Qu'est-ce qu'une donnée de santé », *RGDM*, n° spécial, 2004, p. 12.
[79] *Id*., p. 13.
[80] Ordonnance n° 96-346 du 24 avril 1996 portant réforme de l'hospitalisation publique et privée, *JORF* n°98 du 25 avril 1996, p. 6324.
[81] Article L. 6113-7 du Code de la santé publique.

nous semblent pas indispensables, les dispositions du Code de la santé publique étant suffisamment claires pour que les établissements de santé puissent prendre leurs dispositions quant à la nomination du praticien responsable de l'information médicale, nous ne pouvons que déplorer, encore une fois, le manque de rigueur du législateur, qui ne nous offre que des dispositions partielles sur un sujet pourtant important qu'est l'encadrement de l'information médicale.

76. La mission principale du médecin responsable de l'information médicale est de collecter les informations puis de traiter les données nécessaires à l'analyse de l'activité médicale et à sa facturation que doivent lui transmettre les praticiens hospitaliers. Divers textes précisent les autres missions de ce praticien responsable de l'information médicale : conseiller les praticiens pour la production des données et veiller à la qualité de ces données en les confrontant si nécessaire, avec les dossiers médicaux et les fichiers administratifs[82], assurer la sauvegarde et la copie des données puis leur conservation durant cinq ans[83], diffuser ces données auprès de la direction de l'établissement, du président de la Commission médicale d'établissement (CME) ou de la commission elle-même, selon des modalités arrêtées après avis de la CME[84]. Le médecin responsable de l'information médicale transmet à la direction de l'établissement ainsi qu'au président de la CME les informations nécessaires à l'analyse de l'activité de l'établissement, soit dans son ensemble, soit pour chacune des structures médicales, de manière systématique ou à leur demande, mais toujours dans des conditions garantissant la confidentialité des données et l'anonymat des patients. Il peut aussi transmettre ces informations aux praticiens ayant dispensés des soins. Le médecin responsable de l'information médicale doit être informé de l'objectif des traitements de l'information qui lui sont demandés. Il doit ensuite participer à l'interprétation de leurs résultats.

77. Dans le cadre des contrôles relatifs à la facturation, les médecins inspecteurs de santé publique et les médecins conseils des organismes d'assurance maladie ont accès aux fichiers concernant les informations d'activité et de facturation par l'intermédiaire du praticien

---

[82] Article R. 6113-4 du Code de la santé publique.

[83] Arrêté du 22 février 2008 relatif au recueil et au traitement des données d'activité médicale et des données de facturation correspondantes, produites par les établissements de santé publics ou privés ayant une activité en médecine, chirurgie, obstétrique et odontologie, et à la transmission d'informations issues de ce traitement dans les conditions définies à l'article L. 6113-8 du Code de la santé publique, *JORF* n°0051 du 29 février 2008, p. 3577.

[84] Article R. 6113-8 du Code de la santé publique.

responsable de l'information médicale. Ce dernier doit, dans le cadre d'un contrôle, informer les praticiens responsables des structures médicales concernées préalablement à toute confrontation d'un enregistrement de fichier avec un dossier médical. Il appartient également au praticien responsable de l'information médicale de conseiller le directeur général en ce qui concerne la durée de conservation des dossiers[85]. Ainsi, il doit être consulté par le directeur général avant que ce dernier décide d'éliminer un dossier médical dont le délai de conservation est dépassé. Il lui appartient également de donner son avis sur l'opportunité de fixer des durées de conservation excédant vingt ans pour certaines catégories de dossiers. En tant que garant de la protection des données nominatives, il reçoit les demandes des usagers concernant leur droit d'accès et de rectification prévu par la loi Informatique et Libertés du 6 janvier 1978 et conseille le directeur général en ce qui concerne les droits d'accès aux données médicales nominatives. Il est également consulté concernant les modalités d'attribution et de contrôle des autorisations d'accès.

78. Force est de constater que ce médecin responsable de l'information médicale bénéficie de nombreuses prérogatives afin de lui permettre de remplir au mieux son rôle de garant de la protection des données personnelles. Toutefois, cette fonction est souvent restreinte, au sein des établissements de santé, aux simples missions relatives au PMSI. Or, l'analyse des textes nous montre bien une volonté d'instaurer un "gardien" de l'information médicale, à la fois garant de la bonne application des dispositions de la loi Informatique et Libertés, mais également du respect du secret professionnel.

[85] Article R. 1112-7 du Code de la santé publique.

§2. Une protection à l'efficacité relative

79. La loi Informatique et Libertés a doté la CNIL de nombreux pouvoirs afin que celle-ci puisse mener à bien les missions de contrôle qui lui sont confiées. Toutefois, il convient de s'interroger sur l'efficacité de ces pouvoirs (A) tout comme sur les limites de la protection accordée aux données de santé (B).

A. Le contrôle et la sanction du non-respect de la loi Informatique et Libertés : des mesures disproportionnées ?

80. La CNIL s'est vue dotée par le législateur d'un statut particulier, accompagné des pouvoirs qu'il estimait nécessaire à la réalisation de ses missions (1). Il est également prévu que le non-respect des dispositions de la loi Informatique et Libertés entraine la mise en œuvre de sanctions qui nous semblent toutefois disproportionnées, et donc difficiles d'application (2).

1) La CNIL, une autorité administrative indépendante dotée d'un pouvoir de contrôle nécessaire

81. Le chapitre III de la loi Informatique et Libertés encadre le fonctionnement et l'organisation de la Commission Nationale de l'Informatique et des Libertés. Celle-ci fut la première a bénéficié du statut particulier d'Autorité Administrative Indépendante (AAI). Lors des débats relatifs à la loi de 1978, s'était en effet posée la question du statut à donner à ce qui aller devenir la CNIL. Initialement, il avait été envisagé de faire de la CNIL soit un établissement public sur lequel n'aurait pesé qu'une tutelle allégée, soit un simple service du Ministère de la justice. Mais le contexte particulier[86] dans lequel est née la loi Informatique et Libertés, et donc la CNIL, a justifié la création d'une nouvelle structure : les AAI. Toutefois, ce n'est que plus tard que cette dénomination spécifique est apparue. C'est le Conseil constitutionnel, dans une décision en date du 26 juillet 1984[87] et relative à la haute autorité

[86] *V. Supra.* n° 44.
[87] Conseil constitutionnel, décision n° 84-173 DC du 26 juillet 1984, *JORF* du 28 juillet 1984, p. 2496.

audiovisuelle, qui va pour la première fois mettre un nom sur le concept : « *la désignation d'une autorité administrative indépendante du gouvernement pour exercer une attribution aussi importante […] constitue une garantie fondamentale pour l'exercice d'une liberté publique.* ». La doctrine s'était cependant essayée à la théorisation du concept auparavant.[88] Les AAI ont été créées pour répondre principalement à trois objectifs[89] : le premier est d'offrir aux citoyens l'assurance d'une certaine impartialité en ce qui concerne les interventions de l'Etat. En effet, les AAI ont cette particularité de sembler « *parées dès leur naissance d'une onction qui les ferait bénéficier d'une irréfragable présomption d'impartialité* »[90]. Dans les domaines touchant de près aux droits et libertés fondamentaux, comme c'est le cas pour la protection des données à caractère personnel, l'Etat peut être réputé partial ; il lui appartient alors de confier ses responsabilités en la matière à des autorités extérieures et indépendantes, dont les avis et décisions ne seront pas remis en cause. La deuxième justification tient à la volonté d'associer des professionnels à la mise en place des règles applicables dans des domaines techniques. Enfin, la troisième justification avancée est la meilleure efficacité d'une AAI, notamment en matière de sanction, le juge pouvant sembler parfois plus lent à ce niveau, mais également en matière de prise de décision, le circuit étant plus simple qu'au sein d'une administration classique.

82. La volonté initiale du législateur, en créant la CNIL, n'était pas d'instaurer une nouvelle catégorie juridique, mais simplement de s'assurer que la commission qu'il allait créer ne serait pas une énième structure, dénuée de tout pouvoir. Selon les dispositions de la loi Informatique et Libertés, la CNIL dispose de missions spécifiques, qui pourront être menées à bien grâce aux pouvoirs que lui accorde la loi, l'ensemble étant défini au sein de l'article 11 de la loi.

83. La CNIL est avant toute chose investie d'une mission d'information et de conseil puisque qu'elle doit informer les citoyens et les responsables de traitements de leurs droits et obligations. Au titre de sa mission de conseil, elle doit également épauler les pouvoirs publics et les juridictions en répondant à leurs demandes d'avis. Cette mission l'amène par ailleurs à

---

[88] *V.* notamment en ce sens SABOURIN, Pierre. « Les autorités administratives indépendantes : une catégorie nouvelle », *AJDA*, 1983, pp. 275-295.
[89] « Considérations générales, les Autorités Administratives Indépendantes», Rapport public du Conseil d'Etat, 2001, p. 275.
[90] *Ibid.*

donner un avis sur tout projet de loi ou de décret portant sur la protection des personnes à l'égard des traitements automatisés. Elle peut aussi collaborer avec d'autres AAI en matière de protection de données mais également être associée à la préparation et à la définition de la position française en la matière. La CNIL constitue ainsi une réelle cellule d'appui et de conseil en matière de protection des données.

84. Sa deuxième mission consiste à assurer la protection des données à caractère personnel. Elle se doit donc de veiller à ce que les traitements de données soient mis en œuvre de manière conforme à la loi. Pour mener à bien cette mission, le législateur n'a pas hésité à doter la commission d'un double pouvoir de contrôle : contrôle *a priori* et contrôle *a posteriori*. Au titre de son pouvoir *a priori*, elle doit instruire les déclarations de traitement ainsi que les demandes d'autorisation ou d'avis qui lui sont soumises. Au titre de son pouvoir de contrôle *a posteriori*, elle est destinataire des réclamations, pétitions et plaintes relatives à la mise en œuvre des traitements, auxquelles elle décide des suites à donner. Elle dispose également d'un pouvoir d'enquête au sein des entreprises. Elle peut à ce titre diligenter des perquisitions. Cela lui permet de recueillir tout renseignement utile ou d'obtenir la communication de tout document qu'elle estimera nécessaire à la réalisation de sa mission.[91]. Elle possède un important pouvoir réglementaire en vertu duquel elle est habilitée à élaborer des normes simplifiées, mais également des règlements types et ce afin d'assurer la sécurité des systèmes. Toutefois, la CNIL n'a que très peu utilisé ce pouvoir, puisqu'un seul règlement de ce type a été établi jusqu'à aujourd'hui.[92]Enfin, elle bénéficie d'un pouvoir de sanction à l'encontre des responsables de traitements[93].

85. La CNIL dispose bien entendu de moyens propres afin de mener à bien l'ensemble des missions qui lui sont confiées, son budget relevant du budget de l'Etat. Toutefois, en 2008, face à la faiblesse de ses moyens, la commission a réfléchi à la possibilité d'instaurer un autre mode de financement. La CNIL avait donc présenté au Sénat en 2007 un projet de diversification des sources de financement de la commission[94], dans lequel il envisageait une

---

[91] DESGENSPASANAU, Guillaume. « La protection des données à caractère personnel », *op. cit.*, p. 63.
[92] Délibération CNIL n°81-094 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques.
[93] *V. Infra*, n° 86 et s.
[94] DÉTRAIGNE, Yves. ESCOFFIER, Anne-Marie. «La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information », Rapport d'information fait au nom de la commission des lois, n° 441, 27 mai 2009.

contribution de la part de chaque acteur générant des traitements de données à caractère personnel, tout en excluant des contributeurs les particuliers et le petits organismes. Toutefois, celui-ci n'a, à l'heure actuelle, pas abouti. Nous estimons que cette mesure, bien que permettant de renforcer les moyens de la CNIL pourrait être à double tranchant : d'un côté, certains organismes pourraient être tentés de ne pas déclarer leurs fichiers afin de ne pas avoir à s'acquitter de la redevance, mais d'un autre côté, nous pourrions assister à une plus grande implication des organismes contributeurs dans la protection des données. Dans tous les cas, il est vrai que le manque de moyens de la CNIL, face à l'augmentation constante du traitement des données à caractère personnel et du développement de nouvelles situations à risque (développement des procédés de biométrie notamment), pousse à réfléchir aux nouveaux modes de financement de cette commission.

Le pouvoir de contrôles accordé à la CNIL par la loi Informatique et Libertés est complété par un pouvoir de sanction qui présente cependant quelques limites.

2) La limite des sanctions prévues par les textes

86. Depuis la réforme de la loi Informatique et Libertés intervenue en 2004, la CNIL s'est vue accorder un pouvoir de sanction administrative, dispositif qui est venu compléter les sanctions pénales déjà en place.

L'ensemble des sanctions encourues en cas de non-respect de la loi Informatique et Libertés est décrit au sein de chapitre VII et VIII de la loi, traitant respectivement des sanctions prononcées par la CNIL et des sanctions pénales. Il existe une gradation dans les sanctions pouvant être mises en œuvre par la CNIL. Un premier niveau est prévu avec la possibilité de prononcer un avertissement ou une mise en demeure de faire cesser les manquements à l'encontre du responsable d'un traitement qui n'aurait pas respecté les obligations découlant de la loi Informatique et Libertés. Si le responsable ne se conforme pas à la mise en demeure et, après la mise en œuvre d'une procédure contradictoire, la CNIL pourra alors prononcer, à l'encontre du responsable du traitement défaillant, soit une sanction pécuniaire (sauf s'il s'agit d'un traitement mis en œuvre par l'Etat), soit une injonction de cesser le traitement ou un retrait de l'autorisation qui avait été délivrée. La loi prévoit également une procédure d'urgence qui permet à la CNIL, après une procédure contradictoire et dans l'hypothèse où le traitement porterait atteinte à l'identité humaine, aux droits de

l'homme, à la vie privée ou encore aux libertés individuelles ou publiques, de décider de l'interruption de la mise en œuvre du traitement pour une durée maximum de trois mois (sauf pour certains traitements spécifiques mis en œuvre par l'Etat), décider le verrouillage de certaines données à caractère personnel, pour une durée maximale de trois mois (sauf pour les traitements qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ou qui concernent la prévention, la recherche, la constatation ou la poursuite d'infractions pénales ; dans ce cas, la CNIL en informera le Premier Ministre qui prendra, le cas échéant, les mesures nécessaires pour faire cesser la violation constatée) ou enfin, en cas d'atteinte grave et immédiate aux droits et libertés, le Président de la CNIL peut demander, par le biais d'un référé auprès de la juridiction compétente, d'ordonner sous astreinte toutes les mesures de sécurité nécessaires à la sauvegarde de ces droits[95]. Ces décisions doivent être motivées et notifiées au responsable du traitement. Elles sont susceptibles de recours devant le Conseil d'Etat. Enfin, la CNIL peut décider de rendre publics ou non les avertissements qu'elle prononce ou, en ce qui concerne les autres sanctions, en cas de mauvaise foi du responsable du traitement, décider de les faire publier au sein de journaux ou tout autre support de son choix.

87. Les sanctions pénales réprimant les infractions aux dispositions de la loi Informatique et Libertés sont réprimées aux articles 226-16 à 226-24 du Code pénal[96]. D'une manière générale, nous pouvons constater que toutes les infractions à la loi Informatique et Libertés sont punissables d'une peine de cinq ans d'emprisonnement et de 300 000 Euros d'amende et, dans tous les cas, l'effacement des données à caractère personnel traitées de manière illégales peut être ordonné[97]. A noter que le fait d'entraver l'action de la CNIL est puni d'un an d'emprisonnement et 15 000 euros d'amende[98].

88. Les sanctions administratives pécuniaires, quant à elles, doivent être proportionnelles aux manquements constatés et prises en fonction de la gravité du manquement constaté. Elles ne peuvent excéder la somme de trois millions d'euros[99].

---

[95] Article 46 de la loi Informatique et Libertés.
[96] Article 50 de la loi Informatique et Libertés.
[97] Article 226-22-2 du Code Pénal.
[98] Article 51 de la loi Informatique et Libertés.
[99] Il est intéressant de préciser que ce plafond a été introduit par l'article 65 de la loi n°2016-1321 du 7 octobre 2016 pour une République numérique. Avant cela, les sanctions administratives pécuniaires étaient graduées et ne pouvaient dépasser la somme de 150 000 euros lors du premier manquement et 300 000 euros en cas de manquement réitéré.

89. Ces sanctions prévues par la loi soulèvent de nombreuses interrogations. La première est celle de savoir quelle peut être l'articulation entre sanctions pénales et sanctions administratives prononcées par la CNIL. En pratique, rien dans le texte n'empêche une saisine des deux juridictions de manière simultanée. Le parallèle ici peut être fait avec ce qui s'applique en matière de responsabilité médicale : la responsabilité pénale du praticien peut être mise en cause, sans que cela n'empêche le Conseil de l'Ordre de mettre en œuvre une procédure disciplinaire. Un seul bémol est apporté par le Conseil constitutionnel[100] à ce sujet : le cumul des sanctions prononcées ne peut pas dépasser le montant le plus élevé d'une des sanctions encourues. De même, la loi Informatique et Libertés elle-même prévoit que « *lorsque la Commission Nationale de l'Informatique et des Libertés a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou sur des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce* ».

90. La deuxième réflexion qu'il est utile d'aborder à ce stade concerne l'efficacité réelle des sanctions prévues. Pour cela, nous devons développer notre réflexion en deux temps : d'abord se pencher sur les sanctions pénales, et ensuite se focaliser sur le pouvoir de sanction propre à la CNIL.

91. Les sanctions pénales sont-elles efficaces ? Cela est fortement remis en question par la doctrine[101]. En effet, avant la réforme intervenue en 2004, le contraste entre la sévérité des textes et les condamnations prononcées étaient frappant. Ce constat avait d'ailleurs été effectué par Guy BRAIBANT dans son rapport remis au Premier Ministre en 1998 puisqu'il y précisait que : « *le régime répressif français en matière de fichiers informatiques – dont la cohérence avec d'autres dispositions du Code Pénal comparables est sujette à caution – se caractérise par une grande sévérité, dont le contraste avec une jurisprudence pusillanime est frappant* »[102]. La directive européenne de 1995 laissant carte blanche aux différents Etats en

---

[100] Décision du Conseil constitutionnel n° 89-260DC du 25 juillet 1989, Rec., p. 59. *V.* également en ce sens Décision du Conseil constitutionnel n° 97-395DC du 30 décembre 1997, Rec., p. 33.

[101] *V.* en ce sens LEPAGE, Agathe. « Loi du 6 août 2004. Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Communication commerce électronique*, 2005, n° 2, étude n° 9.

[102] BRAIBANT, Guy « Données personnelles et société de l'information : rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46», *La Documentation française*, 1998, p. 119.

ce qui concerne les sanctions à mettre en œuvre[103], le législateur aurait pu profiter de la réforme de 2004 pour refondre le régime de sanction pénale. Il aurait pu envisager par exemple, comme une partie de la doctrine pouvait l'évoquer, une dépénalisation[104], les sanctions pécuniaires prononcées par la CNIL se substituant aux sanctions pénales[105]. Le législateur aurait également pu suivre les préconisations de Guy BRAIBANT. Celui-ci, constatant l'absence d'une réelle politique pénale dans un domaine « *où les moyens d'investigation humain et matériels de la police judiciaire sont insuffisants et sous dimensionnés, eu égard à l'ampleur de l'activité économique liée à l'informatique* », proposait d'assouplir la répression en distinguant les cas où la violation des dispositions de la loi Informatique et Libertés était destinée à porter atteinte à la liberté des cas où il n'y avait qu'une violation des règles de forme. Dans la première hypothèse, la sanction aurait été une peine correctionnelle et dans la seconde, une peine contraventionnelle. Cette solution aurait permis de rendre la loi et la répression plus efficaces.

92. Toutefois, le législateur a choisi une autre direction lors de la réforme de 2004, en accordant, il est vrai, plus de pouvoirs à la CNIL, mais en n'apportant que peu de nouveautés en ce qui concerne les sanctions pénales. La preuve en est, le législateur se contente d'utiliser la technique du renvoi à la loi de 1978. Or, comme le souligne très bien Caroline ZORN-MACREZ, « *ce procédé, facteur d'inflation législative du fait de sa facilité, est également facteur d'instabilité juridique car il contribue à perdre dans ses méandres le législateur comme le citoyen* »[106]. Loin de la simplification prônée notamment par Guy BRAIBANT, certains auteurs y ont même vu un renforcement de la pénalisation[107], responsable d'une inefficacité des sanctions prévues du fait de leur disproportion. Car force est de constater que les peines actuellement prévues, trop sévères si ce n'est même disproportionnées, perdent de leur pouvoir dissuasif et donc de leur efficacité. A titre de comparaison, il est intéressant de signaler qu'alors que « *le fait, y compris par négligence, de procéder ou de faire procéder à*

---

[103] Directive n°95/46/CE du 24 octobre 1995, article 24 : « Les Etats membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive ».

[104] *V.* notamment en ce sens FRANCILLON, Jacques « Infractions relevant du droit de l'information et de la communication », *revue de science criminelle et de droit pénal comparé*, 1995, n° 1.

[105] BRAIBANT, Guy « Données personnelles et société de l'information : rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46», *op. cit*. p. 119.

[106] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *PUN*, 2010, p. 214.

[107] BRAIBANT, Guy « Données personnelles et société de l'information : rapport au Premier ministre sur la transposition en droit français de la directive numéro 95-46», *op. cit*. p. 119.

des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende », l'homicide involontaire est quant à lui puni de trois ans d'emprisonnement et de 45 000 euros d'amende[108]. Il est alors facilement compréhensible que le juge pénal, face à une infraction à la loi Informatique et Libertés, hésite à prononcer une peine trop lourde, alors que l'atteinte causée ne constitue ni une atteinte physique, ni une atteinte aux biens[109] et que le véritable préjudice subi par la victime sera difficile à chiffrer.

93. Nous sommes ici face à ce que Caroline ZORN-MACREZ considère comme « *un droit non-réaliste* »[110], difficilement susceptible d'être sanctionné. Tout repose alors sur l'efficacité de la CNIL et des sanctions qu'elle prononce. Le fait de disposer de pouvoirs de sanction n'est pas rare pour les autorités administratives de ce type. Le Conseil constitutionnel s'était d'ailleurs déjà prononcé sur la possibilité qu'une AAI puisse exercer un pouvoir de sanction, dans la mesure où la sanction susceptible d'être prononcée reste exclusive de toute privation de liberté et que l'exercice de ce pouvoir demeure assorti par la loi de mesures destinées à sauvegarder les droits et libertés constitutionnellement garantis.[111] Mais la CNIL a dû attendre la réforme de 2004 et le décret d'application du 20 octobre 2005[112] avant de pouvoir disposer de telles prérogatives. Et il a fallu attendre encore deux ans après l'adoption de cette réforme avant que la CNIL ne se décide à faire usage de son nouveau pouvoir[113] et prononcer sa première sanction pécuniaire[114]. Depuis, entre 2006 et 2015, la CNIL aura prononcé en tout 122 sanctions dont 58 sanctions pécuniaires[115]. Ce nombre qui peut nous paraitre assez bas s'explique par la procédure d'élaboration des sanctions elle-même. En effet, comme nous avons pu le constater précédemment, ce n'est que s'il ne se conforme pas à la mise en demeure prononcée à son encontre, et qu'il maintient son délit, que le responsable d'un traitement se verra sanctionné. A titre d'exemple, en 2011, 65 mises en demeures ont été

---

[108] Article 221-6 du Code Pénal.
[109] MATTATIA, François. « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi Informatique et Libertés ? », *Revue de science criminelle*, 2009, p. 317.
[110] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit.*, p. 216.
[111] Décision du Conseil constitutionnel n° 89-260 DC du 28 juillet 1989.
[112] Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004, *JORF* n° 247 du 22 octobre 2005, p. 16769.
[113] FOREST, David. « Pouvoirs de la CNIL : le réveil soudain de la belle endormie », *Recueil Dalloz*, 2007, p. 94.
[114] Délibération CNIL n°2006-173 du 28 juin 2006.
[115] Chiffres consultés le 3 mai 2016 sur [http://www.cnil.fr].

adoptées par la CNIL contre seulement 19 sanctions prononcées.[116]Ainsi, contrairement aux cas dans lesquels le traitement litigieux serait amené devant un tribunal, le responsable du traitement bénéficie d'une possibilité de régulariser sa situation.[117] Le pouvoir de sanction accordé à la CNIL nous apparaît donc être plus efficace et plus facilement applicable que devant une juridiction de droit commun.

En parallèle de ce pouvoir de sanction, la loi Informatique et Libertés instaure, comme nous l'avons vu, une protection spécifique aux données de santé. Cependant, dans les faits, celle-ci présente certaines limites.

B. La protection limitée des données de santé

94. La loi Informatique et Libertés se veut, aux premiers abords, protectrice des données de santé, réputées sensibles. Toutefois, celles-ci peuvent quand même faire l'objet d'un traitement automatisé (1). De même, le consentement de la personne concernée par les données n'a pas l'importance ni le poids que l'on pourrait attendre de lui (2).

1) Les limites de l'interdiction de traitement des données sensibles

95. En transposant la directive européenne 95/46/CE, le législateur a fait entrer les données de santé dans la catégorie des données sensibles, catégorie qui est, par principe, frappée d'une interdiction de traitement. Toutefois, à chaque principe son exception : l'article 8 II vient dresser une liste de plusieurs cas dans lesquels le traitement des données sensibles va être autorisé. Nos travaux portant plus particulièrement sur les données de santé, nous ne nous attarderons pas sur les dispositions qui ne s'appliquent pas à celles-ci.

96. Pas moins de six exceptions trouvent à s'appliquer aux données de santé. La première est énoncée au 1° du II de l'article 8 de la loi Informatique et Libertés : « *les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne* ».

[116] Rapport d'activité 2011 de la CNIL, p. 68.
[117] MATTATIA, Fabrice. « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi Informatique et Libertés ? », *Revue de science criminelle*, 2009, p. 317.

Cette première exception amène plusieurs réflexions. D'abord, la loi exige un consentement "exprès" de la part de la personne concernée par les données. Ainsi, les consentements présumés ne seront pas suffisants, contrairement à certaines hypothèses où seule la non opposition suffit. Concernant la forme, la loi n'impose pas d'obligation de consentement écrit mais, dans la pratique, il sera plus prudent pour le responsable du traitement d'obtenir une preuve du consentement de la personne concernée par les données, sous peine de se voir sanctionné pénalement[118].

97. Le consentement ne sera pour autant pas toujours suffisant à lever l'interdiction de traitement des données sensibles puisque la loi laisse la possibilité au législateur de prévoir que le consentement de la personne concernée par les données ne soit pas suffisant pour lever l'interdiction de traitement des données. Cette possibilité a été introduite par la directive européenne 95/46/CE en son article 8, II, point a : « *le paragraphe 1 ne s'applique pas lorsque la personne concernée a donné son consentement explicite à un tel traitement, sauf dans le cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée* ». Le législateur français a repris cette disposition telle quelle. Toutefois, il n'en n'a pas fait application concernant les données de santé. Or, cette interdiction de traiter des données sensibles malgré le consentement de la personne concernée aurait pu permettre d'instaurer une protection supplémentaire vis-à-vis de certaines situations susceptibles de représenter un risque pour la personne, sans que celle-ci ne puisse totalement s'en rendre compte. Cela aurait constitué une forme de garde-fou contre la personne elle-même. La CNIL, quant à elle, se montre réticente à l'utilisation du consentement de la personne comme unique justification du traitement des données, considérant que le consentement risque d'être parfois forcé et devenir, en quelques sortes, une *« solution de facilité* » pour le responsable du traitement[119]. Ainsi, nous estimons que cette possibilité aurait pu être utilisée notamment dans le cas des dossiers médicaux proposés par certaines sociétés[120]. En effet, nous pensons que les personnes ne mesurent pas toujours les conséquences du traitement de certaines de leurs données et qu'elles doivent donc bénéficier d'une protection supplémentaire.

---

[118] JOB, Jean-Marie. « La loi Informatiques et libertés et les données de santé », *RLDI*, n° 34, 2008, p. 87.
[119] *Ibid*.
[120] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *PUN*, 2010, p. 230.

98. La deuxième exception à l'interdiction de traitement des données de santé est posée au 2° du II de l'article 8 : « *les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle*.». Cette exception rejoint celle existant dans le cadre des soins et instaurée par la loi Kouchner de 2002 (l'article L. 1111-4 du Code de la santé publique prévoit que : « *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. Lorsque la personne est hors d'état d'exprimer sa volonté, aucune intervention ou investigation ne peut être réalisée, sauf urgence ou impossibilité* »). La notion de "sauvegarde de la vie de la personne concernée" a été préférée à celle "d'intérêt vital" qui était utilisée dans la directive européenne. Comme le souligne à juste titre Alex TÜRK dans son rapport[121], la notion d'intérêt vital est la traduction littérale de l'expression anglaise "vital interest", terme ambigu en ce qu'il peut désigner également un intérêt essentiel qui ne se rattache pas pour autant à la survie de la personne. L'urgence dispense donc d'obtenir le consentement de la personne dans l'hypothèse où le traitement serait nécessaire à la sauvegarde de la vie de la personne concernée par les données. Cette exception est en réalité double, ce qui rend son application très limitée[122]. De plus, comme le souligne Jean-Marie JOB, il s'agit de situations qui sont déjà couvertes par la troisième dérogation, beaucoup plus générale[123].

99. La troisième exception concerne les « *traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du Code pénal* » (article 8, II 6°). Pour que cette exception puisse s'appliquer, deux conditions cumulatives doivent être respectées : le traitement doit répondre à une finalité spécifique et être mis en œuvre par un professionnel de santé ou tout autre professionnel tenu au secret professionnel. Cette condition permet ainsi de s'assurer que les données qui seront traitées dans ce cadre, seront soumises à une autre

[121] TÜRK, Alex. « Rapport fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *Sénat*, 2003, p. 57.
[122] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit.*, p. 236.
[123] JOB, Jean-Marie. « La loi Informatique et Libertés et les données de santé », *op. cit.*, p. 87.

protection, celle du secret professionnel. Cette exception renvoie à la relation patient / médecin classique, au cours de laquelle le patient communique un certain nombre d'informations à son médecin, nécessaires à sa prise en charge.[124]. Comme le soulignait le sénateur Alex TÜRK, cette exception permet de compenser le fait que les données de santé soient, de par leur qualification de données sensibles, interdites de traitement, tout en offrant un cadre strict et sécurisé pour la personne concernée par les données traitées.[125]

100. La quatrième exception est beaucoup plus spécifique, puisque le 8° du II de l'article 8 vise « *les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX* ». Cette disposition concerne les traitements mis en œuvre dans le cadre des recherches médicales, qui sont soumis à une procédure particulière décrite au sein du chapitre IX de la loi Informatique et Libertés.

101. La cinquième exception vise également un cas très spécifique, puisque le III de l'article 8 de la loi dispose: « *si les données à caractère personnel visées au I sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitement selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables* ». Les données doivent donc être anomymisées, c'est-à-dire transformées afin qu'il ne soit plus possible de les relier, même indirectement, à la personne concernée[126] : on parlera alors d'anonymisation irréversible. Celle-ci doit intervenir "à bref délai" : cette notion n'est pas définie par la loi Informatique et Libertés et il appartiendra donc à la CNIL, lors de l'étude de la demande d'autorisation, d'apprécier le délai proposé par le responsable du traitement. Comme il est précisé, cette exception ne s'applique pas dans le cadre de la recherche médicale, mais trouvera à s'appliquer notamment dans le cadre de traitements mis en œuvre par des entreprises privées du secteur de la santé, comme, par exemple, les mutuelles.

---

[124] DE LAMBERTERIE, Isabelle. «La place du consentement dans la collecte et le traitement des informations sensibles. La situation en France », *RGDM*, n° 13, 2004, p. 62.
[125] TÜRK. Alex, « Rapport fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée Nationale, relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *op. cit.*, p. 63.
[126] JOB, Jean-Marie. « La loi Informatique et Libertés et les données de santé », *op. cit.*, p. 88.

102. Enfin, la loi Informatique et Libertés, dans son article 8, IV prévoit que les données sensibles pourront faire l'objet d'un traitement si celui-ci est justifié par l'intérêt public et après autorisation de la CNIL[127]. Cette exception ouvre de nombreuses possibilités et trouve à s'appliquer dans des situations diverses. La loi ne définit pas précisément cette notion d'intérêt public. Nous adhérons néanmoins à la définition proposée par Caroline ZORN-MACREZ[128], et à la définition du vocabulaire juridique de Gérard CORNU ; « *ce qui est à l'avantage de tous* ».[129]La directive européenne vient nous apporter quelques précisions quant aux situations pouvant bénéficier de cette exception. Ainsi, elle cite les domaines de la santé publique et de la protection sociale.[130] On peut penser par exemple à la télétransmission des feuilles de soins prévue à l'article L. 161-29 du Code de la Sécurité Sociale[131].

Ainsi, les responsables de traitement disposent de plusieurs exceptions leur permettant de mettre en œuvre un traitement portant sur des données de santé. Au final, ces exceptions, de par leur nombre et leur champ d'application, font du principe d'interdiction la véritable exception.

2) Le consentement mis à mal

103. La condition du consentement préalable au traitement des données est posée à l'article 7 de la loi Informatique et Libertés. Cette nécessité n'existait pas dans la version antérieure de la loi. En effet, initialement, elle ne prévoyait qu'une possibilité d'opposition de la personne concernée par les données[132]. La loi de 2004 modifiant la loi initiale fait désormais du consentement une des conditions permettant la mise en œuvre d'un traitement automatisé de données personnelles. Cependant, le consentement n'est envisagé que comme une alternative parmi d'autres à disposition du responsable du traitement pour légitimer son traitement et non

---

[127] Article 8, IV : « *ne sont pas soumis à l'interdiction de traitement prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I de l'article 25 ou au II de l'article 26* ».
[128] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit*., p. 238.
[129] CORNU, Gérard. « Vocabulaire juridique », *PUF, coll. « Quadrige Dicos Poche »*, 8éme éd., 2007.
[130] La directive 95/46/CE prévoit, en son considérant 34: « Les Etats membres doivent également être autorisés à déroger à l'interdiction de traiter les catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale ».
[131] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit*., p. 239.
[132] Article 26 de la loi Informatique et Libertés.

pas une condition nécessaire[133] (l'article 7 prévoit : *« un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes […]* »). Ainsi, nonobstant le consentement de la personne concernée, le traitement pourra quand même être licite s'il remplit une des autres conditions énoncées à l'article 7.

104. La qualité et la forme du consentement ne sont, quant à elles, pas précisées. Contrairement à ce qui est prévu en matière de données sensibles, le législateur n'exige pas de consentement exprès. Ainsi, il pourrait être possible de présumer qu'une simple non opposition pourrait être suffisante. Toutefois, il ne nous semble pas que cela soit la volonté du législateur. Le Groupe de travail de l'article 29 s'est penché sur la question et a apporté quelques pistes de réflexions[134]. Ainsi, le consentement de la personne concernée par les données doit être un consentement éclairé et, comme le précise la directive européenne en son article 2, il doit être une « *manifestation de volonté, libre, spécifique et informée* ».

105. Le consentement ne bénéficie pas d'un poids important dans le traitement des données à caractère personnel, dans la mesure où d'autres hypothèses vont venir légitimer le traitement des données, sans que le consentement de la personne ne soit nécessaire. Il s'agit du respect d'une obligation légale incombant au responsable du traitement (c'est le cas, par exemple, de la mise en place d'un dossier médical, rendu obligatoire par l'article R. 1112-2 du Code de la Santé Publique), de la sauvegarde de la vie de la personne concernée, de l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement, de l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ou enfin de la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou son destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

106. Il est intéressant ici de s'arrêter sur la dernière exception : l'intérêt légitime du responsable du traitement. Nous ne pouvons que déplorer cette disposition qui nous apparaît

---

[133] DE LAMBERTERIE, Isabelle. « La place du consentement dans la collecte et le traitement des informations sensibles. La situation en France », *op. cit.*, p. 61.

[134] Groupe de travail « article 29 » sur la protection des données, « Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (D.M.E) », *Commission européenne*, 2007.

trop large. En effet, la loi ne propose aucune définition de ce que pourrait être "l'intérêt légitime". Pour sa part, la directive européenne se contente dans son considérant 30 de donner quelques exemples tels que la gestion courante des entreprises, la prospection commerciale ou encore la prospection par une association caritative. Force est de constater que cette exception donne au responsable du traitement une marge de manœuvre assez large, avec pour seules limites le respect de l'intérêt ou des droits de la personne concernée. Alex TÜRK avait déploré dans son rapport le caractère très général de cette dérogation « *d'une portée exceptionnellement large* » qui selon lui, « *fragilise substantiellement la portée du principe du consentement de la personne, qui ne saurait donc être considéré comme constituant la règle en matière de traitement des données.* ». Il appartient donc à la CNIL, grâce à ses pouvoirs de contrôle, de s'assurer que l'équilibre entre l'intérêt légitime du responsable du traitement et le respect des droits de la personne concernée est établi.

107. Ces exceptions, et notamment la dernière, fragilisent fortement le consentement de la personne concernée par les données et sa valeur s'en trouve amoindrie. Dans les domaines relatifs au traitement des données de santé, rares seront les hypothèses où le consentement du patient sera nécessaire. En effet, à titre d'exemple, la constitution d'un dossier médical à l'hôpital répond à une obligation légale (exception n° 1). D'une manière générale, les traitements des données de santé par un établissement de santé découlent directement de sa mission de service public qui est le soin (exception n° 3) mais permettent également la sauvegarde de la vie de la personne concernée (exception n° 2).

De même, si nous poussons notre raisonnement, les compagnies d'assurance pourraient invoquer un intérêt légitime à la collecte et au traitement de données de santé, ce qui pourrait s'avérer réellement préjudiciable pour le patient.

Conclusion de la Section

108. La France s'est très tôt sentie concernée par la problématique du développement de l'informatique et des traitements automatisés des données à caractère personnel. Sa législation Informatique et Libertés essaie d'instaurer un cadre se voulant le plus protecteur possible pour les données personnelles. Les données de santé, considérées comme des données sensibles, bénéficient, en théorie, d'une protection renforcée au titre de la loi Informatique et Libertés, mais également au titre de dispositions du Code de la Santé Publique, la plus importante d'entre elles étant, bien entendu, le secret professionnel.
Toutefois, une étude approfondie des dispositions de la loi Informatique et Libertés nous a permis d'établir que le principe d'interdiction de traitement des données sensibles était fortement fragilisé par les nombreuses exceptions qui y sont prévues. De même, le consentement de la personne concernée par les données n'a pas autant d'importance qu'on aurait pu l'espérer.

Ces données de santé faisant l'objet d'un traitement vont ensuite être partagées par les différents professionnels intervenant dans la prise en charge du patient. Il est donc important de s'arrêter sur l'encadrement réservé au partage de ces données sensibles.

Section 2. Les modalités de partage des données relatives au patient.

109. Les données relatives à un patient, qu'il s'agisse de données de santé ou tout simplement de données administratives, sont nécessaires à sa bonne prise en charge, que ce soit pour la prévention, le diagnostic, le soin ou encore pour la recherche médicale. Ces données sont donc, comme nous l'avons vu précédemment, collectées, conservées et ensuite partagées entre les différents professionnels qui en auraient besoin. L'utilisation désormais quasi systématique des technologies d'information et de communication améliore et facilite ce partage. En effet, grâce à l'informatisation des données, le partage se fait plus rapidement et il est plus complet. La consultation des dossiers médicaux dans leur version informatisée est également plus simple. Toutefois, ces données sont des données sensibles et surtout confidentielles. Leur partage ne peut donc pas avoir lieu sans que certaines dispositions soient prises, notamment en ce qui concerne la sécurité des données. Force est de constater que les règles existantes en la matière sont des règles d'ordre général, qui ne s'adaptent pas toujours correctement aux spécificités des technologies d'information et de communication. L'encadrement du partage des données du patient doit prendre en compte deux dimensions : la sécurisation physique des données et l'encadrement du partage en tant que tel, de manière à délimiter quand, avec qui et sous quelles conditions les données peuvent être partagées. C'est bien cette dernière notion qui va particulièrement nous intéresser ici. En la matière, il n'existe pas de règle spécifique régissant l'encadrement du partage des données de santé par le biais des TIC. Il faut donc se tourner, une fois de plus, vers les règles générales applicables en la matière (paragraphe I), règles générales qui peuvent se montrer parfois limitées. En matière de recherche médicale toutefois, un corpus de règles spécifiques à la matière existe (paragraphe II), qui demeure néanmoins incomplet.

§1. Les règles générales

110. L'encadrement du partage des données de santé nous pousse à nous demander quelles données peuvent être partagées et avec qui. Cette question nous oblige donc à réfléchir dans un premier temps à la notion de propriété des données (A). On peut constater que, même s'il n'existe pas aujourd'hui de réponse claire et définitive sur la question, plusieurs pistes de

réflexion s'offrent à nous. Or, des droits attachés aux données de santé et au dossier médical vont découler certaines règles relatives à leur partage (B).

A. La délicate question de la propriété des données de santé

111. Avant de savoir comment peuvent être utilisées les données de santé, et notamment les conditions de leur partage, il est intéressant de chercher d'abord à savoir qui possède des droits sur ces données. En effet, la question de la propriété des données médicales se pose très souvent. Les patients, d'un côté, estiment que les données les concernent et sont donc leur propriété (1). Les professionnels de santé, à l'inverse, pensent parfois qu'ils possèdent un droit sur ces données qu'ils ont recueillies, formalisées et conservées (2)

1) La recherche d'une qualification du droit des individus sur leurs données

112. Afin de comprendre comment peuvent se partager les données de santé, et notamment qui peut décider quelles données sont partagées avec quelles personnes, il faut commencer par rechercher quels droits possèdent les individus sur leurs données. Car il n'est pas rare d'entendre un patient réclamer l'intégralité de son dossier médical, non pas parce que la loi lui octroie un droit d'accès[135], mais surtout parce qu'il considère son dossier médical comme étant un bien dont il serait le propriétaire.

113. D'une manière générale, la recherche de la qualification du droit que détient l'individu vis-à-vis de ses données fait l'objet d'un vieux débat au sein de la doctrine. En effet, la question qui nous intéresse, à savoir quels droits existent sur l'information de santé, s'inscrit dans un débat beaucoup plus large qui est celui du statut de l'information[136]. Nous ne nous attarderons toutefois pas ici sur le concept large d'information qui peut désigner tout autant les idées d'une personne que les informations plus générales sur un événement. Nous

---

[135] L'article L. 1111-7 Code de la santé Publique dispose : « *Toute personne a accès à l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit, par des professionnels et établissements de santé, qui sont formalisées ou ont fait l'objet d'échanges écrits entre professionnels de santé, notamment des résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en oeuvre, feuilles de surveillance, correspondances entre professionnels de santé, à l'exception des informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant un tel tiers.* ».

[136] MALLET-POUJOL, Nathalie. « Appropriation de l'information : l'éternelle chimère », *Dalloz*, 1997.

préférons nous concentrer sur l'information personnelle en tant que donnée relative à la personne.

114. Face à un risque de marchandisation de l'information personnelle, notamment dans un but de prospection, certains auteurs ont souhaité s'orienter vers le droit de propriété, en préconisant une appropriation de l'information personnelle[137]. Cette théorie, soutenue notamment par L.HUNTER et J.RULE, a été développée afin que chaque individu puisse être propriétaire des droits d'exploitation commerciale des renseignements le concernant[138]. Elle présente l'avantage d'offrir à la personne un droit de contrôle absolu sur ces données et sur l'utilisation qui peut en être faite. Toutefois, ce raisonnement semble, pour certains auteurs, impossible à maintenir. Ainsi, Nathalie MALLET-POUJOL, qualifie cette théorie d' « *excessivement dangereuse* » en ce qu'elle instaure pour l'individu une possibilité de disposer de l'information qui le concerne « *quand seule la jouissance de cette information est véritablement en jeu* » ce qui, pour reprendre ses termes, « *hypothèque le principe de dignité de la personne* »[139]. Pour illustrer ses propos, l'auteur reprend à juste titre l'exemple de l'information génétique et cite le raisonnement développé par Loïc CADIET[140] à ce sujet. Pour l'auteur, l'information génétique, de par son caractère intrinsèquement lié à la personne doit être considérée comme étant un élément du corps humain à part entière. L'information génétique relèverait donc de la catégorie des personnes et bénéficierait, à ce titre, des mêmes droits. L'information génétique, au même titre que le corps humain, se verrait donc appliquer le principe de non-patrimonialité.[141]

115. Cette proximité des liens entre la personne et ses informations n'est pas toujours aussi tranchée que dans le cas des données génétiques. Toutefois, certaines informations peuvent être facilement assimilées à la personne. C'est le cas du nom, qui, comme le dit si bien CAPITANT, est une émanation de la personne[142]. Ainsi, nous estimons qu'il en va de même

---

[137] MALLET-POUJOL, Nathalie. « Droit à et droit sur l'information de santé », *RGDM*, 2007, pp. 77-95.
[138] L, HUNTER. J, RULE. « Vers un droit de propriété des renseignements personnels », *Communication au congrès de l'association canadienne française pour l'avancement de la science*, Montréal, 1994.
[139] MALLET-POUJOL, Nathalie. « Appropriation de l'information : l'éternelle chimère », *op. cit.*
[140] CADIET, Loïc. « La notion d'information génétique en droit français », *in* La génétique humaine, de l'information à l'informatisation, *Ed. Thémis/Litec diffusion*, 1992, p.52. Cité par MALLET-POUJOL. Nathalie, « Appropriation de l'information : l'éternelle chimère », *op. cit.*
[141] Article 16-1 du Code Civil.
[142] CAPITANT, « Introduction à l'étude du droit », 3éme Ed., Paris, 1902, p. 97, cité par MALLET-POUJOL, Nathalie. « Appropriation de l'information : l'éternelle chimère », *op. cit.*

pour les données de santé d'une personne qui, comme nous avons pu le voir précédemment, touchent de très près à son intimité. Dès lors, les informations personnelles doivent donc être considérées comme étant des choses hors commerce. En effet, nous adhérons à la conception de Nathalie MALLET-POUJOL qui considère qu'un rapport propriétaire / objet de propriété de la part d'un individu sur ses données personnelles est inenvisageable car cela reviendrait à remettre en cause la dignité même de la personne. Le droit de l'individu sur ses données personnelles entrerait donc dans la classification des droits de la personnalité.[143] De fait, la question ici n'est pas tant de protéger les données personnelles que l'individu lui-même.

116. Quand on se penche sur la question du droit des personnes sur leurs données, il est également intéressant de s'arrêter sur le principe d'autodétermination informelle. Ce concept est né d'une décision du tribunal fédéral d'Allemagne, qui, en 1983[144], est venu préciser que le traitement de données personnelles nécessitait une justification. Le droit à l'autodétermination informelle ou « *Recht auf informationelle Selbstbestimmung* » est apparu avec cette décision, le tribunal fédéral allemand en faisant un droit fondamental de la personne humaine. Le droit à l'autodétermination informelle peut être défini comme étant le droit pour une personne de maîtriser pleinement les informations la concernant en décidant notamment à qui ces informations pourront être transmises. Il est également défini par certains auteurs comme « *le droit de tout individu à maîtriser l'image qu'il donne de lui-même dans la société* ».[145] Ce droit à l'autodétermination informelle se retrouve dans la loi Informatique et Libertés avec le principe posé à l'article 7 selon lequel tout traitement de données à caractère personnel doit avoir reçu le consentement préalable de la personne concernée. Toutefois, comme nous avons pu le voir précédemment, cette règle connaît quelques exceptions qui viennent fragiliser le poids du consentement et donc ce droit à l'autodétermination informelle. Il existe des cas dans lesquels l'individu verra ses données faire l'objet d'un traitement sans qu'il ne puisse en décider autrement.[146]

117. La théorie de l'autodétermination informelle présente l'avantage, comme le souligne Caroline ZORN-MACREZ[147], de rendre l'individu responsable des décisions qu'il prendra

---

[143] MALLET-POUJOL, Nathalie. « Appropriation de l'information : l'éternelle chimère », *op. cit.*
[144] Tribunal constitutionnel allemand, 15 octobre 1983, cité par ZORN-MACREZ, Caroline, « Données de santé et secret partagé », *op. cit.* p. 231, note 2.
[145] POULLET, Yves. LEONARD, Thierry. « Les libertés comme fondement de la protection des données nominatives », *in* La vie privée, une liberté parmi les autres ?, *Larcier*, Bruxelles, 1992, p. 233.
[146] *V. Infra.*, n° 230.
[147] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit.*, p. 233.

concernant ses données, celles-ci étant totalement en sa maîtrise. Toutefois, nous estimons qu'une application absolue de ce principe pourrait s'avérer trop dangereuse, notamment en ce qui concerne des données sensibles telles que les données de santé, les individus n'ayant pas toujours conscience des conséquences du partage ou de la communication de leurs données.

118. Nous estimons qu'il est inconcevable d'envisager les patients comme étant propriétaires de leurs données médicales. Le droit de propriété ne peut s'appliquer à des données aussi sensibles que les données de santé sans que cela ne porte atteinte à la dignité de la personne concernée. Tout au plus disposent-ils d'une certaine maîtrise sur leur utilisation. Cependant, cette maîtrise de l'individu sur l'utilisation qui peut être faite de ses données de santé est relative, et le jeu des principes et des exceptions à l'interdiction de traitement des données de santé[148] fait que les seuls cas dans lesquels l'individu pourra décider s'il souhaite ou non partager ses données seront des cas dans lesquels il aurait été préférable, selon nous, que le législateur intervienne afin de rendre l'autodétermination informelle de l'individu inapplicable.[149]

2) Tentative de qualification du droit des professionnels de santé sur le dossier médical

119. Si les patients ne disposent pas d'un droit de propriété sur leurs données médicales, qu'en est-il des professionnels de santé et des établissements de santé, qui alimentent les dossiers médicaux ? A l'origine, le dossier médical n'était constitué que de quelques notes sur des fiches cartonnées que le médecin de famille conservait précieusement en son cabinet. La pratique a évolué et la technique aussi. Les établissements de santé ont été légalement tenus de constituer un dossier médical[150]. Ainsi, depuis quelques années, les systèmes d'information hospitaliers se développent et avec eux, les dossiers médicaux informatisés. Des simples fiches, nous sommes passés à des dossiers informatisés et structurés, contenant de nombreuses informations sur le patient. La question se pose alors de savoir si les professionnels de santé, qui alimentent les dossiers médicaux, ou les établissements de santé, qui mettent en place et conservent ces dossiers, vont bénéficier de droits particuliers sur ces derniers.

---

[148] *V. infra.* n° 95 à 102.

[149] Comme nous l'avons vu précédemment, la loi Informatique et Libertés laisse au législateur la possibilité de prévoir des cas où même le consentement de la personne concernée par les données ne pourra pas venir lever l'interdiction de traitement dont fait l'objet les données sensibles.

[150] L'article R. 1112-2 du Code de la santé Publique dispose : « *un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé.* ».

120. Le Code de la santé publique n'apporte pas réellement de précisions à ce sujet (mis à part l'article R. 4127-45 relatif au dossier professionnel ou fiche d'observation tenu par le médecin)[151]. Il nous faut donc faire appel à une autre branche du droit, en l'occurrence le droit de la propriété intellectuelle, pour tenter de qualifier les droits des professionnels et des établissements de santé sur les dossiers médicaux.

121. Le dossier médical, en tant que recueil formalisé d'un ensemble de données, peut-il être considéré comme une base de données et bénéficier à ce titre de la protection spécifique mise en place par le Code de la propriété intellectuelle ? Et si tel est le cas, qui, des praticiens alimentant le dossier ou de l'établissement, serait gardien de la structure même du dossier ?
La base de données est définie par le Code de la propriété intellectuelle comme « *un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par d'autres moyens* ».[152] A ce titre, il est donc possible d'envisager le dossier médical comme étant une base de données, celui-ci étant bien un recueil de données qui sont accessibles de manière individuelle. Une nuance pourrait être apportée sur la question de savoir si ces données sont bien disposées de manière systématique, à savoir selon un ordre déterminé à l'avance ou encore de façon méthodique, c'est-à-dire selon un ensemble ordonné de manière logique[153]. Le Code de la Santé Publique n'impose pas, il est vrai, de classification spécifique du dossier médical. Toutefois, l'article R. 1112-2 du même code détaille le contenu, *a minima*, du dossier médical, et des recommandations de l'Agence Nationale d'Accréditation et d'Evaluation en Santé (ANAES) relatives au contenu du dossier médical ont été publiées[154]. Le dossier médical nous semble donc correspondre suffisamment à la définition du Code de la propriété intellectuelle pour être qualifié de base de données.

---

[151] Cet article prévoit : « *Indépendamment du dossier médical prévu par la loi, le médecin tient, pour chaque patient, une fiche d'observations qui lui est personnelle […] les notes personnelles du médecin ne sont ni transmissibles ni accessibles au patient et aux tiers* ». Toutefois, cette disposition ne concerne que le cas particulier des notes personnelles du médecin et non l'ensemble du dossier médical.
[152] Article L. 112-3 Code de la propriété intellectuelle.
[153] Selon la définition du dictionnaire Larousse.
[154] Agence Nationale d'Accréditation et d'Evaluation en Santé, « Dossier du patient : amélioration de la qualité de la tenue et du contenu, réglementation et recommandations », juin 2003, disponible sur [http://www.has-sante.fr]. Consulté le 5 mai 2017.

122. Les bases de données bénéficient de la protection relative aux droits d'auteurs ainsi que d'une protection *sui generis*, posée au titre IV du Code de la propriété intellectuelle et relative aux droits des producteurs des bases de données. Ce droit s'exerce d'ailleurs indépendamment des droits d'auteurs ou d'autres droits qui pourraient s'exercer sur la base de données.

123. Le droit d'auteur va protéger plus particulièrement la structure de la base de données et, pour en bénéficier, celle-ci devra présenter un critère d'originalité. Il faut ainsi apporter la preuve que la seule forme de la base de données est originale. Par exemple, il est nécessaire de démontrer que « *le choix et la disposition sont originaux* »[155]. Dans le cas des dossiers médicaux informatisés, la structure même du dossier va dépendre du logiciel de gestion utilisé par l'établissement de santé. Or, dans la majorité des cas, ce logiciel va être la propriété d'une société prestataire, sauf à envisager que l'établissement de santé ait créé son propre logiciel.

Cela nous paraît difficilement envisageable et il faut donc recentrer notre réflexion sur la protection *sui generis* des bases de données. Celle-ci va bénéficier au producteur de la base de données, qui est défini à l'article L. 341-1 du Code de la Propriété Intellectuelle comme étant « *la personne qui prend l'initiative et le risque des investissements correspondants* ». Il peut alors bénéficier *« d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel* ». Le producteur reconnu d'une base de données se verra ainsi donner la possibilité d'interdire : *« l'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ; la réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme* ».[156]

Ainsi, la question qui se pose à nous est celle de savoir qui, à l'hôpital, prend l'initiative et le risque des investissements correspondants à la création de la base de données ? Une chose est certaine, les professionnels de santé ne peuvent en aucun cas être considérés comme les producteurs de la base de données, dans la mesure où ce ne sont pas eux qui

[155] TGI Paris, 3e ch., 1ére sect., 13 avril 2010, n°09/03970, Sté Optima on line, JurisData n° 2010-010806.
[156] Article L. 342-1 du Code de la propriété intellectuelle,

pourront attester d'un investissement, financier, humain ou matériel[157]. L'établissement de santé peut-il alors être considéré comme le producteur du dossier médical, base de données ? Le Code de la propriété intellectuelle précise que le producteur de la base prend l'initiative et le risque des investissements. Or, la mise en place d'un dossier médical pour chaque patient étant une obligation légale, peut-on réellement parler d'initiative à proprement parler ? De même que les investissements financiers mis en œuvre pour le développement des dossiers médicaux informatisés ne se feront pas entièrement sur les deniers de l'établissement, celui-ci bénéficiant de fonds publics dispensés dans le cadre de plans tels que le plan Hôpital 2012 ou encore le programme Hôpital numérique. Dès lors, on ne peut pas considérer que l'établissement de santé réponde aux critères du producteur de bases de données.

124. Ni les établissements de santé, ni les professionnels de santé ne disposent donc d'un droit de propriété intellectuelle sur les dossiers médicaux. Toutefois, les règles relatives aux archives hospitalières nous apportent des précisions quant aux droits que possèdent les établissements de santé sur les dossiers médicaux.

L'arrêté du 11 mars 1968 portant règlement des archives hospitalières définit le contenu des archives hospitalières comme étant « *l'ensemble des titres concernant les biens, droits et obligations des établissements publics hospitaliers […] y compris les registres et papiers émanant de l'administration et des services médicaux et chirurgicaux de ces divers établissements* »[158]. Ainsi, selon les termes de cet arrêté, les dossiers médicaux font partie intégrante des archives hospitalières. Aucune disposition relative aux archives publiques ou aux archives hospitalières ne vient préciser que les établissements publics soient propriétaires de leurs archives. Toutefois, l'arrêté du 11 mars 1968 précise en son article 3 que le directeur de l'établissement détient la garde et la responsabilité des archives hospitalières. Dès lors, l'établissement de santé peut être considéré comme étant responsable du dossier médical, qu'il se doit de conserver sous sa protection, mais en aucun cas propriétaire.[159]

---

[157] Nous tenons à rappeler ici que notre travail est accès sur l'utilisation des TIC et non sur la création du dossier médical informatisé en établissements de santé. Notre réflexion différerait certainement dans le cas des dossiers médicaux en cabinet de ville.

[158] Arrêté du 11 mars 1968 portant règlement des archives hospitalières, *JORF* du 25 octobre 1968, p. 10039.

[159] GENOT-POK, Isabelle. « Des archives publiques aux archives hospitalières : points de droit », *Actualités JuriSanté*, n° 69, 2010, p. 6.

B. La difficile application des règles relatives au secret partagé

125. Le partage des données du patient va être nécessaire dans l'intérêt du patient, afin d'assurer la continuité des soins et la coordination de sa prisE en charge. Pour cela, le législateur a aménagé des dérogations au secret professionnel (1) afin de permettre et simplifier le partage des données entre professionnels. Toutefois, l'intégration des TIC dans la pratique courante vient compliquer l'application concrète des règles théoriques (2).

1) Le secret partagé, une dérogation au secret professionnel strictement encadrée

126. La notion de secret partagé n'est pas une notion récente. Très tôt, la jurisprudence a développé ce concept nécessaire à la bonne prise en charge du patient. Dès 1953[160], le Conseil d'Etat reconnaissait la possibilité du partage des données médicales à condition que celui-ci soit nécessaire à la continuité de la prise en charge du patient[161]. Toutefois, la jurisprudence restait imprécise, voire parfois équivoque[162], et le secret partagé ne bénéficiait pas de base légale suffisante à son bon développement. La loi du 4 mars 2002, en introduisant l'article L. 1110-4 au Code de la santé publique présente l'intérêt de remédier à cette situation en inscrivant dans un cadre précis le partage de données au sein d'une équipe de soins. Cet article, modifié depuis, disposait alors : « *Lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe* ». Ce texte présentait néanmoins, jusque très récemment, une lacune importante : aucune définition précise n'était apportée concernant la notion d'équipe de soins. Certains auteurs considéraient même la notion comme étant une « *coquille vide* »[163], qui ne renvoyait à rien de précis, la composition de chaque équipe devant être étudiée au cas par cas afin de conserver une souplesse d'action. D'autres considéraient que l'équipe de soins devait obligatoirement être composée de professionnels effectuant des actes de soins et donc de professionnels de santé ayant compétence légalement reconnue pour effectuer ce type de soins[164]. Cette définition était, selon nous, trop réductrice. De fait, il est

---

[160] CE, sect. Soc., 2 juin 1953, Bull. ord. Méd. 1952-1954, p. 194.
[161] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit*., p. 119.
[162] JONAS, Carol. « La loi du 4 mars 2002 et la pratique médicale quotidienne : apports et incertitudes », *Médecine et droit*, n° 56, 2002.
[163] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit*., p. 119.
[164] BOILEAU Chrystelle. « L'équipe médicale : une existence évidente pour le professionnel de santé, mais discutable pour le juriste », *RGDM*, 2004, n° 14, p. 34.

important de ne pas restreindre la composition de l'équipe de soins aux seuls professionnels de santé *stricto sensu*. En effet, certains professionnels de santé n'effectuent pas de soins (comme les ambulanciers) et certains soins ne sont pas dispensés par des professionnels de santé[165]. Comme le souligne à juste titre Caroline ZORN-MACREZ[166], il est plus important de se concentrer sur le contenu des échanges qui interviennent entre les différents professionnels, plutôt que sur la qualité de ces derniers. La notion d'équipe de soins doit donc s'entendre de manière large et certains professionnels, à l'instar des assistantes sociales, doivent pouvoir faire partie pleinement d'une équipe de soins, et donc partager les données de santé d'un patient, si la prise en charge de celui-ci le nécessite.

127. C'est ce que le législateur a entendu faire en définissant, dans le cadre de la loi de modernisation de notre système de santé[167], la notion de l'équipe de soins.

Désormais, l'article L. 1110-4 est modifié et prévoit, en son point III : « *lorsque ces professionnels appartiennent à la même équipe de soins, au sens de l'article L. 1110-12, ils peuvent partager les informations concernant une même personne qui sont strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social. Ces informations sont réputées confiées par la personne à l'ensemble de l'équipe* ».
L'article L. 1110-12 quant à lui dispose : « *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 ;

---

[165] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit.*, p. 126.
[166] ZORN-MACREZ, Caroline. « Chronique martienne des données de santé numérisées. Brèves observations sur une réglementation surréaliste », *RDS*, n° 36, 2010, p. 336.
[167] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016.

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 ».

128. Preuve que cette notion est difficile à cerner, le texte nous apparaît comme étant rédigé de manière complexe, proposant, finalement, plusieurs définitions dans la définition générale de l'équipe de soins. Cependant, cet article s'inscrit bien dans le sens prévu initialement par les motifs de la loi, à savoir, la promotion d'une prise en charge décloisonnée entre les différents acteurs intervenant dans la prise en charge d'un patient, les professionnels des secteurs sanitaire et médico-social y étant directement intégrés. Par ailleurs, le partage des données de santé en ville ou dans le cadre d'une collaboration ville / hôpital doit satisfaire à d'autres conditions, elles aussi exposées au sein de l'article L. 1110-4 du Code de la santé publique : « *un professionnel peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social […]Le partage, entre des professionnels ne faisant pas partie de la même équipe de soins, d'informations nécessaires à la prise en charge d'une personne requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée, dans des conditions définies par décret pris après avis de la Commission nationale de l'informatique et des libertés* ». Dans ce cas, le consentement préalable du patient est nécessaire avant tout partage d'informations. Nous sommes ici dans une hypothèse où l'information relative au patient va sortir du cadre strict et délimité de l'équipe de soins. Les données vont être communiquées, dans ce cas, à un professionnel extérieur à l'équipe, voire à l'établissement. Contrairement à l'ancienne rédaction de l'article L. 1110-4, qui, jusqu'en janvier 2016, prévoyait une non opposition de la part des patients avant tout échange de données le concernant[168], le Code de la santé publique prévoit désormais la nécessité d'un consentement dûment recueilli et donc, formalisé. Les professionnels prenant en charge le

[168] BOSSI, Jeanne. « Le cadre juridique du partage d'information dans les domaines sanitaires et médicosocial. Etat des lieux et perspectives. », *Médecine et droit*, 2013, p. 6.

patient et souhaitant partager ses données avec un autre professionnel devront donc s'assurer de dispenser une information claire au patient afin de lui laisser l'opportunité de consentir, ou non, à cet échange. Bien que cette disposition aille dans le sens d'un renforcement du secret professionnel, il nous faut cependant déplorer, en pratique, l'aspect contraignant pour les professionnels de la nécessité de recueillir le consentement systématique avant tout échange de données.

2) Les limites de l'application du secret partagé aux TIC

129. L'application des règles relatives au secret partagé ne pose pas réellement problème quand il s'agit pour deux professionnels d'échanger à l'oral. Toutefois, l'exercice se complique dès lors que l'utilisation des TIC entre en jeu. En effet, dans le cas du dossier médical informatisé par exemple, il va falloir s'assurer que seule l'équipe de soins, au sens de l'article L. 1110-4 du Code de la santé publique, puisse accéder aux données du patient. Il va donc être nécessaire que le professionnel s'identifie dans un premier temps, puis s'authentifie ensuite. Il s'agit bien ici de deux actions différentes : une au cours de laquelle le professionnel va décliner son identité et une autre qui va permettre au professionnel de prouver qu'il est bien celui qu'il prétend être.

130. Pour ce faire a été créée la Carte de Professionnel de Santé (CPS). Beaucoup plus répandue chez les professionnels libéraux, cette carte peine toutefois à se développer dans le secteur hospitalier. La CPS, qui contient les données d'identification de son porteur ainsi que ses conditions d'exercice, permet à son détenteur de s'authentifier et de signer électroniquement les différentes opérations qu'il effectue (par exemple la rédaction d'un compte rendu d'hospitalisation). Initialement mise en place pour l'authentification des professionnels de santé dans le cadre de la transmission dématérialisée des feuilles de soins[169], son utilisation a ensuite été élargie à toutes les transmissions de données de santé par voie électronique. Le décret confidentialité du 15 mai 2007[170] ajoute donc au Code de la santé

[169] L'article L. 161-33 du Code de la Sécurité Sociale dispose : « Dans le cas de transmission électronique par les professionnels, organismes ou établissements dispensant des actes ou prestations remboursables par l'assurance maladie, l'identification de l'émetteur, son authentification et la sécurisation des échanges sont assurées par une carte électronique individuelle, appelée carte de professionnel de santé ».

[170] Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le Code de la santé publique, *JORF* 113 du 17 mai 2007, p. 9362.

publique un article R. 1110-3 qui prévoit qu': « *en cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du Code de la sécurité sociale est obligatoire.* ». Cette carte est actuellement distribuée par l'Agence des Systèmes d'Information Partagées en santé (ASIP santé).

131. Plusieurs bémols doivent être apportés à ce système *a priori* sécurisé. Le premier tient à son manque de diffusion au sein des établissements de santé. En effet, à l'heure actuelle, selon les chiffres de l'ASIP santé[171], sur les 592 828 cartes CPS en circulation, seulement 120 408 ont été distribuées au sein des établissements de santé. Il devient alors compliqué, pour les professionnels de ces établissements, de respecter les obligations instaurées par le décret confidentialité dans le cas du partage de données de santé par voie électronique. De plus, ces cartes sont uniquement à destination des professions règlementées au titre du chapitre IV du Code de la Santé Publique. Or, en établissement de santé, le partage de données n'est pas restreint à ces professions[172]. Pour pallier ce problème, l'ASIP santé a mis en place des cartes de la famille de la CPS. On trouve ainsi la CDE (carte de directeur d'établissement), destinée aux directeurs d'établissement de santé. Le directeur peut également déléguer ces tâches en désignant des mandataires délégués. De même, a été créée la CPE (carte de personnel d'établissement) destinée aux salariés non professionnels de santé, des structures libérales et des établissements de santé. Là encore, ces cartes ne sont pas encore suffisamment répandues au sein des établissements de santé pour permettre d'assurer la sécurité prévue par les textes (sur les 497 590 cartes CPE, 203 987 étaient distribuées en secteur hospitalier au 20 février 2017).[173]

132. Les freins à l'application des règles en matière de partage des données de santé, dans le cadre de l'utilisation des TIC, sont dûs principalement aux limites de la technologie actuelle en matière de traçabilité des accès ou, pour être plus précis, aux difficultés, pour les établissements, de disposer d'un système à la fois performant et en conformité avec des textes parfois utopistes. A ce sujet, nous pouvons reprendre une expression de Caroline ZORN-

[171] Chiffres disponibles sur [http://esante.gouv.fr]. Consultés le 15 mai 2017.
[172] *V. Supra.* n° 127.
[173] Chiffres disponibles sur [http://esante.gouv.fr]. Consultés le 15 mai 2017.

MACREZ, qui illustre parfaitement le problème actuel, en parlant de « *secret partagé coincé dans la bulle informatique* »[174].

§2. Le cas particulier de la recherche médicale : des règles de protection spécifiques

133. La spécificité de la recherche médicale a amené le législateur à intégrer, au sein de la loi Informatique et Libertés, des dispositions propres au traitement de données à caractère personnel dans le cadre de la recherche médicale.

Avant d'étudier de manière précise ces dispositions (B), il est important de nous arrêter sur la particularité de la recherche médicale et du cadre qui l'entoure, cadre pouvant parfois se montrer complexe à appréhender, et ce malgré une réforme récente (A). L'étude de l'ensemble de ces dispositions nous permettra de nous interroger sur la force de la protection accordée aux données de santé issues de la recherche (C).

A. Le cadre juridique des recherches impliquant la personne humaine

134. La difficulté principale rencontrée lors de l'étude et l'application des règles en matière de partage des données dans le cadre de la recherche médicale provient du manque de lisibilité des textes encadrant la recherche médicale. En effet, la recherche médicale est strictement réglementée par différentes lois, codifiées au sein du Code de la santé publique tandis que l'encadrement des traitements de données dans ce cadre, fait l'objet, comme nous venons de le voir, de dispositions spécifiques au sein de la loi Informatique et Libertés. Pour certains auteurs, nous sommes ici confrontés à une dualité de qualification[175] et le responsable d'un traitement va devoir commencer par qualifier juridiquement sa recherche, avant de pouvoir chercher à trouver quelles seront les démarches à effectuer en vue d'encadrer son traitement de données à caractère personnel.

---

[174] ZORN-MACREZ, Caroline. « Chronique martienne des données de santé numérisées. Brèves observations sur une réglementation surréaliste », *Revue droit et santé*, n° 36, 2010, p. 335.
[175] BAHR, Anne. BULACH, Claudette. FABER, Stéphanie « Comment appliquer la loi Informatique et Libertés à la recherche médicale ? », *op. cit*., p 49.

135. Cette démarche constitue une première difficulté. En effet, les recherches médicales sont encadrées par différents textes. Jusque 2012, la recherche médicale était encadrée, pour l'essentiel, par la loi n° 88-1138 du 20 décembre 1988 relative à la protection des personnes se prêtant à des recherches biomédicales, connue sous le nom de loi "Huriet-Sérusclat"[176]. Cette loi a défini pour la première fois les recherches biomédicales comme étant des « es*sais ou expérimentations organisés et pratiqués sur l'être humain en vue du développement des connaissances biologiques ou médicales* ». Plusieurs modifications ont ensuite été apportées, notamment par la loi n° 2004-806 du 9 août 2004, relative à la politique de santé publique[177], qui a transposé les dispositions de la directive 2001/20/CE du 4 avril 2001 relative à l'application de bonnes pratiques cliniques dans la conduite d'essais cliniques de médicaments à usage humain. A ces dispositions s'ajoutaient celles contenues au sein des lois bioéthiques et notamment la loi n° 2004-800 du 6 août 2004 relative à la bioéthique[178], révisée par la loi n° 2001-814 du 7 juillet 2011[179]. En effet, ces lois, dont le contenu a été codifié au sein du Code de la santé publique, encadrent les dons des éléments et produits du corps humain. Ainsi, dans le cadre d'une recherche non interventionnelle portant sur une collection biologique d'échantillons humains, le promoteur de la recherche devait effectuer, d'une part, les démarches relatives à la mise en œuvre de la recherche en elle-même et, d'autre part, celles relatives à la mise en place de la collection d'échantillons. Or les différents dispositifs sont difficiles à mettre en œuvre car il n'existe pas de réelle coordination et le chercheur se retrouve alors face à « *une multiplicité des guichets d'autorisation et d'enregistrement* »[180].

136. Le manque de cohérence des différents textes ainsi que leur caractère incomplet ont été de nombreuses fois critiqués par la doctrine[181] et c'est pourquoi un travail de refonte de la législation applicable avait été mis en œuvre, celui-ci ayant abouti à l'adoption de la loi n°

---

[176] Loi n°88-1138 du 20 décembre 1988 dite Huriet relative à la protection des personnes qui se prêtent à des recherches biomédicales, *JORF* du 22 décembre 1988, p. 16032.
[177] Loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique, *JORF* n°185 du 11 août 2004, p. 14277.
[178] Loi n° 2004-800 du 6 août 2004 relative à la bioéthique, *JORF* n°182 du 7 août 2004, p. 14040.
[179] Loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique, *JORF* n°0157 du 8 juillet 2011, p. 11826.
[180] CHEMTOB-CONCE, Marie-Christine. CAILLEUX, Anne. « L'impact des nouvelles dispositions de la loi relative aux recherches impliquant la personne humaine », *médecine et droit*, 2013, pp. 30-35.
[181] *V.* notamment en ce sens BOYER-BEVIERE, Bénédicte « Les principales réformes de la loi n° 2011-300 du 5 mars 2012 sur les recherches impliquant la personne humaine, *RGDM*, n° 44, 2012, pp. 225-238. ; LEMAIRE, François. « Pourquoi faut-il encore réformer la législation de la recherche biomédicale ? », *Médecine et droit*, 2011 ; LAIGNEAU, Jean-François. « Sécurité et développement des recherches : de la loi Bertrand à la loi Jardé », *médecine et droit*, 2012.

2012-300 du 5 mars 2012 sur les recherches impliquant la personne humaine[182], plus communément appelée loi "JARDE". Cependant, le décret d'application de cette loi, longtemps attendu, n'a été publié qu'en novembre 2016[183].

137. Cette loi a permis d'unifier le cadre juridique applicable à la recherche médicale et ce, notamment, afin de simplifier les démarches des chercheurs. En effet, face au « *mille-feuille législatif* »[184] que constituent les différentes lois encadrant la recherche, le législateur a souhaité offrir à la recherche médicale un cadre juridique plus lisible et surtout plus équilibré. Olivier JARDE avait notamment reproché l'excès de réglementation qui existait pour certaines recherches, tandis que d'autres étaient menées dans « *quasi-vide juridique* »[185]. La refonte de la réglementation a donc consisté en la mise en place de différentes catégories de recherches disposant d'un cadre juridique commun. Désormais, trois catégories de recherches cohabitent : les recherches interventionnelles qui comportent une intervention sur la personne non justifiée par sa prise en charge habituelle, les recherches interventionnelles qui ne portent pas sur des médicaments et qui ne comportent que des risques et des contraintes minimes et les recherches non interventionnelles dont tous les actes sont pratiqués et les produits utilisés de manière habituelle. Pour ces trois types de recherches, la loi propose un cadre juridique minimum applicable dans tous les cas. Ainsi, toutes les recherches devront faire l'objet d'un avis du comité de protection des personnes. Cela permettra notamment à certains chercheurs de publier leurs résultats plus facilement[186].

138. Toutefois, ces nouvelles dispositions ne font pas l'unanimité au sein de la doctrine. Si certains félicitent le législateur pour les efforts de simplification accomplis par la loi JARDE et soulignent l'impact positif que ces dispositifs pourraient avoir sur le développement de la

---

[182] Loi n° 2012-300 du 5 mars 2012 sur les recherches impliquant la personne humaine *JORF* n° 0056 du 6 mars 2012, p. 4138, texte n° 1.
[183] Décret n° 2016-1537 relatif aux recherches impliquant la personne humaine, *JORF* n° 0267 du 17 novembre 2016.
[184] JARDE, Olivier. « Rapport fait au nom de la commission des affaires sociales sur la proposition de loi, modifiée par le Sénat, relative aux recherches cliniques ou non interventionnelles impliquant la personne humaine », *Assemblée Nationale*, 7 avril 2000.
[185] LAIGNEAU, Jean-François. « Sécurité et développement des recherches : de la loi Bertrand à la loi Jardé » *op. cit.*, p. 166.
[186] BOYER-BEVIERE, Bénédicte. « Les principales réformes de la loi n° 2012-300 du 5 mars 2012 sur les recherches impliquant la personne humaine », *RGDM*, 2012, n° 44

recherche[187], d'autres au contraire n'hésitent pas à critiquer avec véhémence cette loi qui n'est « *pas plus digeste et compréhensible* »[188] que les précédents textes, dénonçant une « *pathétique obscurité des textes* »[189].

Au-delà du cadre organisant les modalités de mise en œuvre d'une recherche impliquant la personne humaine, la particulière sensibilité du sujet a amené le législateur à prévoir un cadre spécifique applicable aux données de santé faisant l'objet d'un traitement automatisé dans ce contexte.

B. L'encadrement particulier des traitements des données de santé dans le cadre de la recherche

139. Conscient du domaine délicat de la recherche et de l'importance d'éviter les déviances et les abus, le législateur a très tôt encadré l'utilisation et le partage des données de santé dans le cadre de la recherche. Ainsi, la loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[190] est venue compléter la loi Informatique et Libertés afin d'y intégrer un chapitre consacré aux traitements de données à caractère personnel dans le domaine de la recherche médicale. Troisième volet du triptyque relatif à la bioéthique[191], cette loi a fait l'objet d'une longue maturation et était très attendue des acteurs de la recherche médicale.[192]

140. Plus récemment, la loi de modernisation de notre système de santé a modifié le cadre applicable aux traitements des données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, refondant ainsi le chapitre IX de la loi Informatique et Libertés, qui pose les principes applicables aux traitement de données à caractère personnel dans le cadre

---

[187] *V.* en ce sens Marie CHEMTOB-CONCE, Marie-Christine. CAILLEUX, Anne. « L'impact des nouvelles dispositions de la loi relative aux recherches impliquant la personne humaine », *op. cit.*, p. 30.
[188] LEROYER, Anne-Marie. « Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine », *RTD Civ.*, 2012, p. 384.
[189] *Ibid*.
[190] Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n°152 du 2 juillet 1994, p. 9559.
[191] TÜRK, Alex. « Rapport au nom de la Commission des lois », *Sénat*, 1993/1994, p. 87.
[192] MARLIAC-NEGRIER, Claire. « La protection des données nominatives informatiques en matière de recherche médicale » Tome 1, *Presses universitaires d'Aix-Marseille*, 2001, p. 106.

de la recherche (1). Par ailleurs, la CNIL a modifié sa méthodologie de référence applicable aux recherches biomédicales (MR001) et en a adopté une nouvelle (MR003) (2) simplifiant ainsi les démarches pour les chercheurs souhaitant mettre en place un traitement de données.

1) Les principes applicables aux traitements de données à caractère personnel dans le cadre de la recherche médicale

141. Par principe, les traitements ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation dans le domaine de la santé, doivent être autorisés par la CNIL. L'autorité prend sa décision après avoir recueilli d'une part l'avis du Comité de Protection des Personnes (CPP) en ce qui concerne les recherches impliquant la personne humaine telles que définies à l'article L. 1121-1 du Code de la santé publique ou du Comité d'Expertise pour les Recherches, les Etudes et les Evaluations dans le domaine de la Santé (CEREES) pour les demandes relatives à des recherches n'impliquant pas la personne humaine ou relatives à des études ou des évaluations. Ce comité, dont la composition exacte a été précisée par décret[193], doit rendre son avis dans un délai d'un mois à compter de sa saisine, délai qui peut être ramené à quinze jours en cas d'urgence. Cet avis portera sur « *la méthodologie retenue, sur la nécessité du recours à des données à caractère personnel, sur la pertinence de celles-ci par rapport à la finalité du traitement et, s'il y a lieu, sur la qualité scientifique du projet* ». Le comité va apporter une caution éthique au projet de recherche.

142. A noter que ce comité vient remplacer l'ancien Comité Consultatif sur le Traitement de l'Information en matière de Recherche dans le domaine de la Santé (CCTIRS), qui avec la loi de modernisation de notre système de santé, disparaît. Cette suppression du CCTIRS au profit d'un comité rebaptisé mais ayant les mêmes missions peut intriguer. Cependant, le décret n° 2016-1872 du 26 décembre 2016[194], qui vient préciser le fonctionnement du CEREES, tend à démontrer que le législateur a souhaité organiser celui-ci de manière plus précise.

---

[193] Décret n° 2016-1872 du 26 décembre 2016 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF* n°0301 du 28 décembre 2016, texte n° 34.
[194] *Ibid.*

143. A ces formalités administratives, le chapitre IX de la loi Informatique et Libertés ajoute d'autres obligations à la charge du responsable du traitement. Ainsi, une liste d'informations à fournir préalablement à la collecte des données et de manière individuelle aux personnes concernées est dressée à l'article 57 de la loi Informatique et Libertés[195]. Cette obligation d'information n'est pas absolue et deux exceptions sont prévues : la première concerne l'impossibilité de retrouver le patient encas de recherche rétrospective ; la seconde concerne l'hypothèse dans laquelle le médecin traitant estime pour des raisons légitimes que le patient doit être laissé dans l'ignorance du diagnostic.

144. A ce sujet, il est intéressant de signaler que ces dispositions sont aujourd'hui en contradiction avec la réforme du Code de déontologie intervenue le 7 mai 2012[196]. En effet, le Code de déontologie prévoyait en son article 35 la possibilité pour le médecin, de tenir un patient dans l'ignorance d'un diagnostic ou d'un pronostic graves et ce, pour des raisons légitimes qu'il appréciait en conscience. En prévoyant une possibilité de non divulgation de l'information par le praticien, le Code de déontologie était en opposition avec l'article L. 1111-2 du Code de la Santé Publique qui ne prévoit que trois exceptions à l'obligation d'information : l'urgence, l'impossibilité d'informer, la volonté du patient d'être tenu dans l'ignorance. Cette possibilité est désormais supprimée et remplacée par la disposition suivante : « *toutefois, lorsqu'une personne demande à être tenue dans l'ignorance d'un diagnostic ou pronostic, sa volonté doit être respectée, sauf si des tiers sont exposés à un risque de contamination* ». Dès lors, il est légitime de se demander quelles vont être les dispositions qui prévalent.

De notre point de vue, le Code de déontologie a été modifié afin d'être mis en conformité avec les dispositions du Code de la santé publique et renforcer ainsi le droit à l'information des patients. Dans cette optique, cette possibilité de tenir le patient dans

---

[195] Cet article dispose : « *Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :*
1° De la nature des informations transmises ;
2° De la finalité du traitement de données ;
3° Des personnes physiques ou morales destinataires des données ;
4° Du droit d'accès et de rectification institué aux articles 39 et 40 ;
5° Du droit d'opposition institué aux premier et troisième alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement. »

[196] Décret n° 2012-694 du 7 mai 2012 portant modification du Code de déontologie médicale, *JORF* n°0108 du 8 mai 2012, p. 8479.

l'ignorance d'un diagnostic ne devrait plus exister non plus dans le cadre de la recherche médicale, sauf à admettre que la recherche puisse bénéficier d'un cadre plus souple du fait des buts poursuivis. Or, nous estimons que les données du patient et, d'une manière plus générale, les droits du patients, doivent être protégés de la même manière, que le patient soit pris en charge dans le cadre d'une activité de soins et de diagnostic ou dans le cadre d'une recherche médicale.

145. Parmi les obligations incombant au responsable du traitement, se trouve l'obligation d'anonymiser les données à caractère personnel, obligation à laquelle il ne peut plus être dérogé[197]. Enfin, il faut souligner que la loi Informatique et Libertés soumet toutes les personnes, amenées à mettre en œuvre les traitements ou ayant accès aux données sur lesquelles celui-ci porte, au secret professionnel tel que défini à l'article 226-13 du Code pénal. L'ensemble de ces démarches constituent les formalités préalables à la mise en place Cependant, des formalités simplifiées existent, par le biais des méthodologies de référence.

2) Les Méthodologies de Références MR001 et MR003

146. La version initiale de la loi du 1er juillet 1994 prévoyait la possibilité pour le Président du CCTIRS de mettre en œuvre une procédure simplifiée[198] applicable aux traitements de données à caractère personnel ayant pour finalité la recherche en santé. Toutefois, ces dispositions ne contenaient pas plus de précisions quant aux recherches concernées ou aux modalités de mise en œuvre de cette procédure simplifiée.[199] Néanmoins, la CNIL et le CCTIRS avaient adopté un régime simplifié de déclaration des essais cliniques en 1998[200]. Cette procédure simplifiée était applicable aux recherches entrant dans le champ d'application

---

[197] L'article 55 de la loi Informatique et Libertés, dans sa version antérieure au 26 janvier 2016, prévoyait : « *lorsque ces données permettent l'identification des personnes, elles doivent être codées avant leur transmission. Toutefois, il peut être dérogé à cette obligation lorsque le traitement de données est associé à des études de pharmacovigilance ou à des protocoles de recherche réalisés dans le cadre d'études coopératives nationales ou internationales ; il peut également y être dérogé si une particularité de la recherche l'exige. La demande d'autorisation comporte la justification scientifique et technique de la dérogation et l'indication de la période nécessaire à la recherche.* ». Ces dispositions ont été supprimées par la loi de modernisation de notre système de santé.

[198] L'ancienne version de l'article 40-1 loi Informatique et Libertés alinéa 3 prévoyait la chose suivante : « *le président du comité consultatif peut mettre en œuvre une procédure simplifiée* ».

[199] PERRAY, Romain. « Traitement de données personnelles dans le cadre de recherches médicales : vers un allégement des formalités », *Revue Lamy droit de l'immatériel*, 2007, n° 24, pp. 64-66.

[200] Procédure simplifiée adoptée par le Comité consultatif le 3 février 1998 relative aux traitements informatiques de données nominatives collectées dans le cadre de recherches biomédicales.

de la loi du 20 décembre 1988 modifiée sur la protection des personnes qui se prêtent à des recherches biomédicales.

147. La loi du 6 août 2004 modifiant la loi Informatique et Libertés initiale dans un premier temps, puis la loi de modernisation de notre système de santé plus récemment, ont précisé cette possibilité d'instaurer des procédures simplifiées. L'article 54, IV précise désormais : « *pour les catégories les plus usuelles de traitements automatisés de données de santé à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé, la Commission nationale de l'informatique et des libertés peut homologuer et publier des méthodologies de référence destinées à simplifier la procédure d'examen. Celles-ci sont établies en concertation avec le comité d'expertise et des organismes publics et privés représentatifs des acteurs concernés* ». Ces procédures vont permettre aux responsables de traitement, en souscrivant à un engagement de conformité vis-à-vis d'une méthodologie de référence, d'éviter de formuler une demande d'autorisation auprès de la CNIL. Dans ce cas les traitements peuvent être mis en œuvre dès lors qu'ils respectent les conditions fixées par la Méthodologie de Référence (conditions en termes de sécurité du traitement notamment mais également en termes de durée de conservation des données).

148. Conformément à ces dispositions, la CNIL avait donc adopté, en 2006, une méthodologie de référence applicable aux traitements de données personnelles mis en œuvre dans le cadre des recherches biomédicales[201]. L'adoption de cette méthodologie de référence a été justifiée par le fait que les recherches biomédicales sont déjà encadrées de manière stricte et selon des méthodologies standardisées. La MR-001, qui a été récemment modifiée par la délibération CNIL n° 2016-262 du 21 juillet 2016[202], s'applique aux essais cliniques de médicaments, à l'exception des essais cliniques dits "par grappe"[203], aux recherches biomédicales, aux recherches interventionnelles qui comportent une intervention sur la

[201] Méthodologie de référence MR-001 pour les traitements de données personnelles opérées dans le cadre des recherches biomédicales.

[202] Délibération n° 2016-262 du 21 juillet 2016 portant modification de la méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales (MR-001), *JORF* n°0189 du 14 août 2016, texte n° 76.

[203] GIRAUDEAU, Bruno. «L'essai clinique randomisé par grappes », disponible sur [http://ipubli-inserm.inist.fr]. Consulté le 22 février 2017. Pour l'auteur « *un essai clinique randomisé par grappes (cluster randomization trial) est un essai dans lequel on ne randomise pas individuellement des sujets, mais des groupes de sujets qu'on appelle des « grappes » (clusters). Ces unités de randomisation peuvent être des hôpitaux, des médecins, des familles, des villages, des entreprises, autant d'unités "sociales" pour lesquelles les sujets qui composent une unité ne peuvent être considérés comme indépendants les uns des autres* ».

personne non justifiée par sa prise en charge habituelle, aux recherches interventionnelles, qui ne portent pas sur des médicaments et qui ne comportent que des risques et des contraintes minimes (la liste de ces recherche a été fixée par un arrêté en date du 3 mai 2017[204]) et les recherches nécessitant la réalisation d'un examen des caractéristiques génétiques.
La Méthodologie de Référence n°3 (MR003) quant à elle a été adoptée avec la délibération CNIL du 21 juillet 2016 et publiée le 14 août 2016[205]. Elle s'applique aux essais cliniques de médicaments dits "par grappe", les recherches visant à évaluer les soins courants et les recherches non interventionnelles.

Le législateur a donc prévu plusieurs dispositions venant encadrer l'utilisation des données de santé dans le cadre de la recherche médicale. Cependant, il apparait opportun de s'interroger sur la force de cette protection.

C. Les données de santé utilisées dans le cadre de la recherche, des données moins bien protégées ?

149. Les données de santé, du fait de leur statut de données sensibles, bénéficient d'une protection spécifique. Ainsi, les données utilisées dans le cadre des recherches médicales étant également des données de santé au sens de la définition que nous avons pu étudier précédemment[206], devraient bénéficier du même degré de protection. Force est de constater que cela n'est toujours pas le cas. En effet, afin de faciliter le travail des chercheurs, certaines mesures dérogatoires ont été établies, qui fragilisent la protection instaurée autour des données de santé utilisées dans le cadre de la recherche.

150. La première protection écornée est celle relative au secret médical. Les règles de droit commun applicables en matière de secret partagé ne permettent normalement pas aux médecins cliniciens de partager leurs données avec des médecins chercheurs ceux-ci ne

[204] Arrêté du 3 mai 2017 fixant la liste des recherches mentionnées au 2° de l'article L. 1121-1 du Code de la santé publique, *JORF* n°0107 du 6 mai 2017, texte n° 30.
[205] Délibération n° 2016-263 du 21 juillet 2016 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement exprès ou écrit de la personne concernée (MR-003), *JORF* n° 0189 du 14 août 2016, texte n° 77.
[206] *V. Supra*. n° 63 à 69.

faisant pas partie de l'équipe de soins[207]. L'article 55 de la loi Informatique et Libertés vient donc instaurer une exception au secret professionnel, précisant que « *nonobstant les règles relatives au secret professionnel, les membres des professions de santé peuvent transmettre les données à caractère personnel qu'ils détiennent dans le cadre d'un traitement de données autorisé en application de l'article 53* ». Il peut donc être dérogé au secret professionnel s'il s'agit pour des professionnels de partager des données de santé, initialement collectées afin d'assurer la prise en charge du patient, mais dont les chercheurs pourraient avoir besoin dans le cadre de recherches rétrospectives. Il est utile de préciser que cette utilisation secondaire des données n'est pas contraire, dans ce cas, au principe de finalité posée par l'article 6 de la loi, puisque ce même article prévoit qu'un traitement ultérieur à des fins de recherche scientifique est possible si celui est réalisé dans le respect de certaines dispositions prévues par la loi, et notamment celles du chapitre IX, relatif au traitement des données à caractère personnel ayant pour fin la recherche dans le domaine de la santé.

151. L'article 55 essaie toutefois de compenser cette dérogation au secret professionnel en instaurant une anonymisation obligatoire de ces données : « *Lorsque ces données permettent l'identification des personnes, leur transmission doit être effectuée dans des conditions de nature à garantir leur confidentialité.*». Cela permet de justifier l'exception au secret professionnel, dans la mesure où les données transmises ne seront plus des données personnelles. A noter que jusqu'au 27 janvier 2016, date d'entrée en vigueur de la loi de modernisation de notre système de santé, l'article 55 prévoyait deux exceptions à cette obligation d'anonymisation : lorsque le traitement de données était associé à des études de pharmacovigilance ou si une particularité de la recherche l'exigeait. Avec la loi de modernisation de notre système de santé, ces dérogations ont disparu.

152. L'autre protection importante dont les données de santé issues de la recherche ne bénéficient pas est celle relative à l'hébergement agréé. En effet, face à l'augmentation de la dématérialisation des données de santé, les établissements de santé ainsi que les professionnels de santé n'ont pas eu d'autre choix que d'externaliser le stockage de ces données. Afin de sécuriser cette pratique, la loi du 4 mars 2002 a donc instauré un cadre spécifique relatif à l'hébergement des données de santé. Ainsi, l'article L. 1111-8 du Code de

[207] *V. Supra*. n° 127.

la santé publique dispose que « *toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime* ». Nous n'entrerons pas dans les détails des questions que peut poser l'hébergement des données de santé, celles-ci faisant l'objet d'un développement ultérieur. Nous préférons nous pencher ici sur la question des données visées par ces dispositions.

En effet, l'article L. 1111-8 du Code de la santé publique vise les données de santé recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins. Ainsi, les données collectées dans le cadre de recherches biomédicales ne sont pas directement visées par le texte. Faut-il considérer que celles-ci ne doivent pas être hébergées obligatoirement auprès d'un hébergeur agréé ? Où s'agit-il d'un oubli malheureux de la part du législateur ? Les travaux parlementaires ne nous éclairent pas à ce sujet. L'application *stricto sensu* de l'article L. 1111-8 du Code de la Santé Publique nous amènerait donc à considérer que les données collectées dans le but d'effectuer une recherche médicale, qui n'est ni un acte de prévention, ni de diagnostic, ni de soin, n'auraient pas à être hébergées chez un hébergeur agréé. Pour la CNIL, cette position se justifie par le fait que ces données auraient un caractère indirectement identifiant[208]. Toutefois, comme nous venons de l'établir précédemment, cela n'est toujours pas le cas. La secrétaire générale de l'ASIP santé de l'époque, Jeanne BOSSI a apporté une précision lors d'une présentation relative au décret hébergeur en expliquant que « *le champ d'application de la procédure d'agrément s'applique à toute base de données recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins : recherche, secteur assurantiel* »[209]. Mais, contrairement à ce qu'avancent certains auteurs, nous ne pensons pas que cette indication signifie que toutes les données de santé, quelles qu'elles soient doivent être conservées chez un hébergeur agréé. La situation avancée par Jeanne BOSSI fait uniquement référence aux données qui auraient dans un premier temps été recueillies pour des activités de soin, de prévention ou de diagnostic,

[208] BRAC DE LA PERRIERE, Marguerite. FERRE, Elise. « L'hébergement des données de santé, des textes à la pratique », *Gaz. Pal.*, 2011, n° 204, p. 21.
[209] Présentation disponible sur [http://www.sante.gouv.fr]. Consultée le 15 mai 2017.

puis récupérées ensuite à des fins d'utilisation secondaires. Cela révèle au contraire que, selon le type de recherche, les données de santé seront soumises à une protection différente : les données de santé utilisées dans le cadre de recherches rétrospectives seront mieux protégées, car initialement collectées dans le cadre visé à l'article L. 1111-8, que celles collectées dans le seul but d'effectuer une recherche médicale.

Nous estimons qu'il est dommage que les données issues de la recherche ne soient pas concernées par ces dispositions car elles ne sont en aucun cas moins sensibles que d'autres. Nous pensons donc qu'une évolution de la réglementation en ce sens devrait avoir lieu.

Conclusion de la section

153. Pour assurer la qualité et la continuité des soins de leurs patients, les professionnels de santé doivent régulièrement partager les données de santé qui les concernent. Ce partage ne peut se faire dans n'importe quelles conditions et le législateur a entendu l'encadrer.
Dans le cadre du soin tout d'abord, en introduisant notamment la notion de secret partagé, mais en permettant également aux professionnels de santé qui n'appartiendraient pas à une même équipe de soins, de partager des données concernant leur patient, sous certaines conditions.

Dans le cadre de la recherche médicale ensuite, pour lequel un corpus législatif et règlementaire strict existe afin de permettre le partage et l'utilisation de données de santé à caractère personnel dans ce contexte particulier.

Conclusion du chapitre

154. Dans le cadre de l'introduction des TIC dans la pratique médicale, les traitements informatisés des données de santé se sont considérablement développés. Dans ce contexte, une protection toute particulière doit être garantie à ces données, considérées comme sensibles par la loi Informatique et Libertés. C'est justement cette loi qui constitue le premier pilier de cette protection. De fait, ce texte de droit commun consacre des dispositions spécifiques aux traitements de données de santé qui devront être mis en place avant tout traitement automatisé. Toutefois, cette protection peut apparaitre comme étant limitée, les nombreuses exceptions à l'interdiction de traitement des données de santé fragilisant le dispositif en place. Par ailleurs, le législateur a entendu encadrer strictement les modalités de partage de ces données particulières. Ainsi, le secret professionnel, obligation prévue par de nombreux textes, devient le second pilier de la protection offerte aux données de santé. Cependant, l'application de ces règles, dans le cadre de l'utilisation des TIC, peut parfois s'avérer délicate. Enfin, le cas particulier des données de santé utilisées dans le cadre de la recherche n'a pas été oublié et fait l'objet de dispositions législatives spécifiques. Cependant, ces données peuvent apparaitre parfois moins bien protégées que les données de santé recueillies dans le cadre du soin.

Une fois les données de santé ayant fait l'objet d'un traitement automatisé sur support informatique, celles-ci vont devoir être conservées et éventuellement partagées par le biais des TIC. Le législateur a souhaité, dans ce cadre, mettre en place une réglementation propre aux TIC en santé.

Chapitre 2

Les modalités de conservation et de communication des informations relatives aux patients

« *La notion même d'équipe suppose le partage de l'information, dans le respect des droits des patients. C'est pourquoi le plus grand risque serait aujourd'hui de continuer à déployer des systèmes d'information non communiquants* »[210].

155. Comme le souligne judicieusement le Dr Jacques LUCAS[211], en matière de soins, la prise en charge en équipe prévaut désormais. Celle-ci se développe notamment par le biais de l'utilisation des TIC dans la pratique quotidienne. Le partage sécurisé des données de santé informatisées, ainsi que leur conservation, sont donc devenus un enjeu majeur.

156. Bien que certains puissent voir dans le développement de l'informatisation en médecine un risque d'aller à l'encontre de l'humanisme qui caractérise le métier de médecin[212], il n'en reste pas moins une formidable avancée pour les professionnels de santé comme pour les patients. Car force est de constater que l'introduction des TIC dans la pratique médicale permet d'améliorer la coordination des soins par le biais de la mise en place d'une communication facilitée des informations en santé.

Tout comme il existe un cadre relatif à la collecte et au traitement informatisé des données de santé, leur archivage et leur communication par voie informatique sont également encadrés. Or, ce cadre est multiple. En effet, les données de santé produites par les établissements publics de santé, qu'elles soient informatisées ou non, vont être considérées comme des archives publiques et, à ce titre, leur archivage sera soumis aux dispositions du Code du patrimoine (Section I Cependant, de par leur informatisation, l'hébergement et la communication de ces données de santé, archives publiques, vont devoir être soumis au

---

[210] Livre blanc de l'Association française des hébergeurs agréés de données de santé, 2014, consultable sur [http://www.dsih.fr], p. 13.
[211] Le Docteur Jacques LUCAS est Vice-Président du Conseil National de l'Ordre des Médecins.
[212] FAROUDJA, Jean-Marie. « Questions sur l'informatisation des dossiers médicaux, le partage et l'hébergement des données », rapport de la commission nationale permanente, adopté lors des assises du Conseil National de l'ordre des médecins du 18 juin 2005, p. 3.

respect de dispositions particulières. Pourtant, comme nous le verrons, ces dispositions nous apparaissent, à l'heure actuelle, quelque peu limitées (Section II)

Section 1. La conservation des données de santé en tant qu'archives hospitalières

157. Les données de santé recueillies à l'occasion d'un acte médical vont être précieusement conservées au sein de son dossier médical afin, notamment, d'assurer la continuité des soins du patient. A l'hôpital, la conservation des données de santé est soumise à une réglementation stricte et précise qui peut parfois paraître complexe à articuler. En effet, les textes applicables en la matière sont multiples et les obligations pesant sur les établissements de santé, tout aussi nombreuses.

Les données de santé produites par les établissements publics de santé vont être qualifiées d'archives hospitalières et, à ce titre, être régies par des dispositions du Code du patrimoine (Paragraphe 1). Toutefois, du fait de leur sensibilité toute particulière, les données de santé ne peuvent pas être conservées et stockées sans s'assurer au préalable de la mise en place de dispositifs permettant de préserver leur sécurité et leur confidentialité (Paragraphe 2).

§1. Les règles spécifiques aux archives publiques

158. La loi n° 2008-696 du 15 juillet 2008[213] modifie l'encadrement relatif aux archives publiques. Cette loi, qui s'inscrivait dans un mouvement de transparence engagé par le législateur français depuis plusieurs années[214], avait pour but d'améliorer la protection des archives et d'en faciliter l'accès.

Les dossiers médicaux produits par les établissements publics de santé, personnes morales de droit public, entrent dans la catégorie des archives publiques. L'ensemble des dispositions qui les concerne, et notamment la loi de 2008, va donc trouver à s'appliquer à ces dossiers (A).

---

[213] Loi n° 2008-696 du 15 juillet 2008 relative aux archives, *JORF* n°0164 du 16 juillet 2008, p. 11322.
[214] GARREC, René. « Rapport sur le projet de loi relatif aux archives », rapport fait au nom de la commission des lois, *Sénat*, n° 146, 19 décembre 2007.

Les dossiers médicaux restent cependant soumis à une réglementation spécifique prévue par le Code de la santé publique. Cela a pour conséquence de provoquer des oppositions entre les différentes règles d'application, mais également des difficultés d'interprétation (B).

A. Les conséquences de la qualification d'archives publiques.

159. Le Code du patrimoine définit de manière exhaustive quels sont les documents qui relèvent des archives publiques (1). Ces définitions emportent plusieurs conséquences juridiques, notamment en matière de durée de conservation et de modalités d'élimination des documents (2), mais également en matière d'archivage électronique des données de santé (3).

1) Définitions légales

160. L'archivage peut être défini comme « *l'action de conserver et de classer des documents ne présentant plus un intérêt immédiat* »[215]. L'hébergement, quant à lui, consiste, en informatique, en l'action « d'accueillir sur un serveur un service ou des pages Web pour les rendre accessibles aux utilisateurs »[216]. En ce qui concerne plus spécifiquement l'hébergement des données de santé, cela consiste donc à leur fournir un site de sauvegarde.
Notre exercice de définition doit être poussé un peu plus loin et il est nécessaire de se pencher plus attentivement sur la notion d'archive. C'est la loi du 3 janvier 1979 sur les archives[217] qui a donné pour la première fois, dans son article initial, une définition générale de ce que sont les archives. Ainsi, aux termes du Code du patrimoine, « *les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, dans l'exercice de leur activité*».[218] Comme le souligne Catherine MORIN-DESAILLY, ce n'est donc pas l'ancienneté du document qui fait de lui une archive[219].

---

[215] Définition du dictionnaire Larousse.
[216] *Ibid*.
[217] Loi n°79-18 du 3 janvier 1979 sur les archives, *JORF* du 5 janvier 1979, p. 43.
[218] Article L. 211-1 du Code du patrimoine.
[219] MORIN-DESAILLY, Catherine. « Avis sur le projet de loi relatif aux archives », avis rendu au nom de la commission des affaires culturelles, *Sénat*, n° 147, 19 décembre 2007, p. 10.

161. Le législateur distingue les archives publiques des archives privées et les définit comme « *les documents qui procèdent de l'activité, dans le cadre de leur mission de service public, de l'Etat, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public ou des personnes de droit privé chargées d'une telle mission* »[220]

Le législateur fait la distinction entre trois âges des archives publiques[221] : l'âge courant, qui correspond à la période pendant laquelle les données sont à la disposition des personnes qui les ont collectées ; l'âge intermédiaire, qui correspond à la période pendant laquelle les données ne sont plus utilisées, mais sont toutefois conservées par l'administration, notamment pour des raisons de preuve ou de suivi ; l'âge définitif, qui concerne une petite partie des archives publiques qui, même si elles ne présentent plus d'intérêt pour l'administration qui les a produites, conservent néanmoins un intérêt historique, scientifique ou patrimonial[222].

Cette distinction est cruciale puisque de l'âge des archives vont dépendre ensuite leur modalités pratiques de conservation (notamment en termes de durée) et de leur destruction.

162. Il est important de souligner que le législateur a créé des sous-catégories d'archives publiques, parmi lesquelles se trouvent les archives hospitalières. Ces dernières sont réglementées par l'arrêté du 11 mars 1968[223] qui précise, en son article 1 que : « *les archives hospitalières consistent dans l'ensemble des titres concernant les biens, droits et obligations des établissements publics hospitaliers énumérés à l'article 1er du décret n° 957 du 3 août 1959 des établissements de soins et des établissements de cure, y compris les registres et papiers émanant de l'administration et des services médicaux et chirurgicaux de ces divers établissements* ». Dès lors, tout document répondant à cette définition se verra appliquer les règles prescrites par l'arrêté du 11 mars 1968. Traditionnellement, une distinction est faite

[220] Article L. 211-4 du Code du patrimoine.
[221] Décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques, *JORF* du 5 décembre 1979, p. 3056 et Décret n° 2009-1124 du 17 septembre 2009 modifiant le décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques, *JORF* n°0216 du 18 septembre 2009, p. 15251.
[222] BANAT-BERGER, Françoise. « Archives et protection des données personnelles », *RLDI*, 2013, n°95, p. 93.
[223] Arrêté du 11 mars 1968, *JORF* du 25 octobre 1968, p. 10039.

entre, d'une part, les archives hospitalières qualifiées d'administratives et d'autre part celles qualifiées d'archives médicales. Enfin, notre exercice de définition peut être conclu avec la précision suivante : le législateur ne fait pas de différence selon les supports retenus pour l'archivage. Ainsi, les documents numériques, audiovisuels, les bases de données, constituent des archives au même titre que les documents papiers.

2) Conséquences juridiques

163. La qualification d'archives publiques, et plus particulièrement celle d'archives hospitalières, va avoir des conséquences juridiques en matière de durée de conservation des données (a), et en matière d'élimination des données (b).

a) Les conséquences relatives à la durée de conservation des données

164. Les archives publiques sont, comme nous l'avons vu précédemment, encadrées par des textes précis. En ce qui concerne leur durée de conservation, le jeu de l'application des différents textes, de la loi à la simple circulaire, peut paraître un peu perturbant, d'autant plus que certains desdits textes sont anciens.

165. La qualification d'archives publiques entraîne, avant toute chose, l'obligation de conserver ces données. En effet, l'article L. 211-2 du Code du patrimoine dispose que « *la conservation de ces documents est organisée dans l'intérêt du 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* ». En ce qui concerne plus précisément les archives hospitalières, les délais de conservation vont résulter à la fois des textes relatifs aux archives publiques, des textes relatifs à la conservation du dossier médical et de textes réglementaires complémentaires intervenus pour fixer la durée de conservation de certaines catégories de données de santé. L'arrêté du 11 mars 1968 classe, dans son annexe, les archives hospitalières en différentes catégories, auxquelles sont associées des durées de conservation. Ainsi, à titre d'exemple, dans la série "Q", qui concerne la population "malades hospitalisés", on trouve notamment les registres d'entrées et de sorties, qui doivent être conservés indéfiniment, tandis que dans la série "K", qui concerne le personnel, on trouve les mouvements du personnel administratif, qui doivent être conservés cinq ans. Les archives

hospitalières dites "administratives" ont vu, quant à elles, leur durée de conservation précisée par plusieurs circulaires, publiées entre 1993 et 1994[224].

166. Plus récemment, la loi du 4 mars 2002[225] a introduit une durée légale de conservation du dossier médical[226]. Ces règles sont édictées à l'article R. 1112-7 du Code de la santé publique. Par principe, le dossier médical est conservé pendant une durée de vingt ans, à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein. Pour un patient mineur, si la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, celle-ci est prorogée jusqu'à cette date. Enfin, pour les patients décédés, le dossier est conservé pendant une durée de dix ans à compter de la date du décès.

A noter que ces délais sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité de l'établissement public de santé ou de professionnels de santé, en raison de leurs interventions au sein de l'établissement. Enfin, certaines données de santé, comme les données relatives aux transfusions sanguines ou les données relatives à l'aide médicale à la procréation, auront une durée de conservation différente de celles du dossier médical traditionnel.

167. Le but ici n'est pas de dresser une liste exhaustive des délais de conservation de chaque type de données. Nous souhaitions simplement souligner qu'en tant qu'archives publiques, les archives hospitalières doivent répondre à une obligation de conservation dont le délai dépend de la nature des informations archivées. Or, en la matière, force est de constater qu'il existe presque autant de délais différents qu'il y a de types de documents. Une harmonisation et, surtout, une mise à jour de l'ensemble de ces délais serait souhaitable. En effet, à l'heure actuelle, du fait de cette obligation de conservation, mais également du

---

[224] Circulaire AD 93-4 du 14 mai1993, Archives des établissements publics d'hospitalisation ; Circulaire AD 94-2 du 18 janvier 1994, Tri et conservation des archives des établissements publics de santé : documents produits après 1968 par les services administratifs chargés de la gestion des hospitalisations et consultations ; Circulaire AD 94-6 du 18 juillet 1994, Tri et conservation des archives des établissements publics de santé : documents produits après 1968 par les services chargés de la gestion du personnel et de la formation ; Circulaire AD 94-11 du 20 octobre 1994, Tri et conservation des documents produits après 1968 par les établissements publics de santé : archives de l'administration générale de l'établissement (Série L de l'instruction annexée à l'arrêté du 11 mars 1968).

[225] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* du 5 mars 2002, p. 4118.

[226] Le dossier médical est défini à l'article R. 1112-2 du Code de la santé publique.

passage, parfois difficile[227], du papier au numérique, les établissements publics de santé doivent faire face à des difficultés de stockage, qu'elles soient physiques ou techniques. De même, comme nous le verrons ultérieurement, les supports de conservation informatique proposés actuellement ne garantissent pas la pérennité nécessaire pour répondre aux délais légaux de conservation. Les établissements se trouvent donc régulièrement dans l'obligation, pour plus de sécurité, de conserver les versions papiers, en plus des versions informatiques de certains documents, afin de satisfaire aux obligations légales.

En matière d'archivage des documents hospitaliers, un travail relatif au cadre légal, qui prendrait en compte les nouvelles contraintes techniques auxquelles doivent faire face les établissements publics de santé, devrait donc être initié par le législateur.

b) Les conséquences relatives à la suppression des données

168. En matière d'élimination des archives hospitalières, il nous plaît à emprunter l'expression de Caroline ZORN-MACREZ, qui nous parle de « *paradoxe de la suppression* »[228]. En effet, dans ce domaine, plusieurs dispositions vont venir se superposer, voire s'opposer, créant alors de grandes difficultés d'interprétation des textes.

169. Classiquement, les archives publiques qui ont atteint le troisième âge peuvent faire l'objet d'une destruction, sous réserve du respect de certaines conditions strictes, prévues au Code du patrimoine. Une destruction des archives en dehors de ces règles entraîne la responsabilité de l'établissement. C'est d'ailleurs ce qu'a rappelé la Cour administrative d'appel de Marseille dans une décision du 25 juin 2009[229]. En l'espèce, un centre hospitalier n'était pas en mesure de communiquer à un usager, et ce malgré un avis de la CADA en ce sens, les bandes d'enregistrement du SAMU, celles-ci ayant été détruites. Le centre hospitalier estimait qu'aucune faute ne pouvait lui être reprochée, aucun texte législatif ou réglementaire n'imposant la conservation de ces bandes.

La Cour d'appel de Marseille a considéré que l'enregistrement des échanges téléphoniques entre le médecin régulateur du SAMU et ses interlocuteurs constituait un

---

[227] *V. infra.*, n° 191 et s.
[228] ZORN-MACREZ, Caroline. « Chroniques martiennes des données de santé numérisées », *RDS*, n° 36, juillet 2010, p. 340.
[229] CAA Marseille, 25 juin 2009, n° 07MA02024.

document produit par l'hôpital dans l'exercice de ses activités et répondait donc à la définition des archives publiques. Dès lors, la destruction des enregistrements étant intervenue en dehors de prescriptions prévues au sein de l'article 16 du décret n° 79-1037 du 3 décembre 1979, la destruction devait être considérée comme fautive, peu importe si celle-ci présentait un caractère intentionnel ou non. D'une manière générale, comme le rappelle une instruction ministérielle du 14 août 2007[230], l'élimination des archives publiques est subordonnée au visa du directeur des archives départementales territorialement compétent, qui peut choisir d'en conserver certaines de manière définitive afin de documenter la recherche.Toutefois, l'établissement public de santé a toujours la possibilité de choisir de conserver les archives, même si la direction départementale des archives préconise leur élimination[231].

170. En ce qui concerne le cas plus spécifique des archives médicales, l'article R. 1112-7 du Code de la santé publique prévoit que : « *la décision d'élimination est prise par le directeur de l'établissement après avis du médecin responsable de l'information médicale. Dans les établissements publics de santé et les établissements de santé privés participant à l'exécution du service public hospitalier, cette 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* »
La question qui pourrait se poser ici, et qui n'est pas directement encadrée par les textes, est l'hypothèse dans laquelle un patient, en raison du droit à l'oubli dont il dispose, demanderait l'élimination de son dossier médical et ce, dans sa totalité.

171. A ce sujet, il est avant tout nécessaire de tenter de définir ce qu'est le droit à l'oubli. Actuellement, il n'en n'existe aucune définition. Des infractions sont bien prévues par le Code pénal en cas de conservation « *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 adressé à la CNIL* »[232]. De même, l'article 40 de la loi Informatique et Libertés prévoit bien, pour toute personne concernée par un traitement automatisé de données à caractère personnel, le droit d'obtenir que soient effacées les données personnelles la

[230] Instruction interministerielle N°DHOS/E1/DAF/DPACI/ 2007/322 et N°DAF/DPACI/RES/2007/014 du 14 août 2007 relative à la conservation du dossier médical, non parue au *JORF*.
[231] GARREC, René. « Rapport sur le projet de loi relatif aux archives », Rapport fait au nom de la commission des lois, *Sénat*, *op. cit*.
[232] Article 226-20 du Code pénal.

concernant et qui seraient inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Enfin, plus récemment, le règlement européen a prévu, dans son article 17, la possibilité pour une personne dont les données à caractère personnel feraient l'objet d'un traitement, d'obtenir l'effacement de ces données dans les meilleurs délais mais dans la limite de certaines hypothèses strictement prévues[233].

172. Toutefois, il ne s'agit jamais d'une possibilité pure et simple d'obtenir l'élimination complète d'un traitement automatisé. Au mieux, le patient dispose-t-il d'un droit à rectification au sujet de données erronées. Mais à qui appartient alors la possibilité d'apprécier si une donnée de santé est erronée ? La loi Informatique et Libertés répond à cette question puisque, toujours dans son article 40, elle précise qu'il appartient au responsable de traitement, en cas de contestation de la demande de rectification ou de suppression de données, d'apporter la preuve que ces données ne sont pas fausses, sauf s'il est établi que les données ont été communiquées par l'intéressé ou avec son accord. De plus, la création d'un dossier médical étant une obligation légale pour l'établissement, et la loi spéciale dérogeant au droit général, une telle demande nous semble impossible à autoriser. Pourtant la CNIL, qui a déjà eu à se prononcer sur une telle demande, s'est montrée favorable à l'application stricte de l'article 40. Ainsi, elle a considéré comme étant légitime, la demande d'un patient qui exigeait que soit effacé l'ensemble des documents conservés sur support informatique et concernant ses différentes hospitalisations. Le patient invoquait le fait qu'il était atteint d'une affection qu'il ne souhaitait pas révéler à sa famille et il craignait qu'un membre de sa famille,

---

[233] L'article 17 du règlement européen prévoit : « *La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:*
a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;
b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement;
c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;
d) les données à caractère personnel ont fait l'objet d'un traitement illicite;
e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;
f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1. »

médecin dans l'hôpital où il était pris en charge, consulte le système informatique et découvre ainsi sa pathologie[234].

173. Bien qu'il faille remarquer ici qu'il ne s'agissait pas d'une demande d'élimination portant sur l'intégralité du dossier médical, l'avis de la CNIL, sur ce sujet, nous paraît néanmoins dangereux à plusieurs titres. D'une part, nous estimons que la CNIL remet en question l'efficacité des règles relatives au secret professionnel. En effet, la décision de supprimer des données de santé, par anticipation sur un éventuel accès frauduleux à celles-ci, laisse à penser que la CNIL n'a pas confiance dans les règles existantes en matière de partage de l'information médicale, règles qui s'appliquent aux professionnels de santé. La CNIL semble oublier qu'en matière de secret professionnel, les même règles sont opposables, qu'il soit question de données de santé papier ou informatisées. D'autre part, accepter la suppression de données informatisées, au motif que l'établissement public de santé possède toujours la possibilité de les conserver sur support papier, va à l'encontre du mouvement actuel qui tend à une informatisation complète des dossiers médicaux. Ce genre de situation se révèle donc très bloquant pour les établissements publics de santé, freinant considérablement le développement des TIC dans la pratique médicale.

Or, de telles demandes ne peuvent que se multiplier dans les années à venir, sous la double pression de la peur de l'outil informatique et de la crainte de l'ouverture à tous des archives, dont le délai de conservation serait écoulé. Nous pensons que la CNIL, bien que garante des droits des personnes dont les données font l'objet d'un traitement informatisé, devrait toutefois faciliter l'instauration d'un climat de confiance de l'outil informatique.

B. Archives publiques, archives hospitalières et secret médical : des règles parfois en opposition

174. Suite à la loi du 15 juillet 2008[235] réformant les règles relatives aux archives, des interrogations quant à la communicabilité des archives hospitalières et donc des dossiers médicaux ont vu le jour. Ce questionnement fait suite à une disposition issue de cette loi et

[234] Quinzième rapport d'activité de la CNIL, 1995, cité par SAMARCQ, Nicolas. BRIOIS, Sébastien. « Données de santé à caractère personnel : les enjeux de la diffusion des TIC », *Expertises*, 2010, p. 385.
[235] Loi n° 2008-696 du 15 juillet 2008 relative aux archives, *JORF* n°0164 du 16 juillet 2008, p. 11322.

codifiée au Code du patrimoine à l'article L. 213-2. Ce texte dispose que « *les archives publiques sont communicables de plein droit à l'expiration d'un délai de (…) vingt-cinq ans à compter du décès de l'intéressé, pour les documents dont la communication porte atteinte au secret médical* ». Le texte ajoute que « *si la date du décès n'est pas connue, le délai est de cent vingt ans à compter de la date de naissance de la personne en cause* ». Face à cette disposition, le directeur du centre hospitalier de Lorquin a saisi la CADA, afin d'obtenir un conseil concernant l'application de ces dispositions aux dossiers médicaux.

175. Dans un conseil rendu le 16 avril 2009[236], la CADA tient le raisonnement suivant : en application de l'article L. 211-4 du Code du patrimoine, les documents des établissements publics de santé sont des archives publiques, archives qui, au titre de l'article L. 213-2 du même code, sont communicables de plein droit vingt-cinq ans à compter du décès de l'intéressé pour les documents dont la communication porte atteinte au secret médical ou cent vingt ans, à compter de la date de naissance de la personne en cause. Elle poursuit son raisonnement en précisant que les dossiers médicaux ayant le caractère d'archives publiques, sont donc librement communicables dans les conditions prévues à l'article L. 212-2 du Code du patrimoine. La CADA ajoute enfin que le dernier alinéa de l'article L. 1110-4 du Code de la santé publique[237], qui encadre les modalités de communications des informations d'une personne décédée à ses ayants droit, n'est alors plus applicable. Selon la CADA, les dossiers médicaux, passé un certain délai, pourraient donc être librement communicables à n'importe quelle personne qui en formulerait la demande. Face à cet avis, la DHOS a, via une circulaire du 21 août 2009[238], rappelé l'état du droit en matière de communication des informations de santé relatives à une personne décédée ayant été hospitalisée dans un établissement public de santé ou un établissement privé, chargé d'une mission de service public. La DHOS préconise aux établissements de santé l'organisation de l'élimination des dossiers médicaux et ce, « *avec une particulière attention* ». En effet, par le truchement des articles du Code du patrimoine précités et des dispositions du Code de la santé publique relatives à la durée de

[236] CADA, conseil n° 20091205, séance du 16 avril 2009.

[237] Cet alinéa dispose : « *le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès* ».

[238] Circulaire n° DHOS/E1/2009/271 du 21 août 2009 relative à la communicabilité des informations de santé concernant une personne décédée ayant été hospitalisée dans un établissement public de santé ou un établissement de santé privé chargé d'une mission de service public, non publiée au *JORF*.

conservation des dossiers médicaux, la DHOS estime que l'élimination systématique des dossiers médicaux évitera leur communication au public.

176. Comme une partie de la doctrine, nous pensons que cette nouvelle disposition introduite par la loi de 2008 relative aux archives, ne s'applique pas aux dossiers médicaux. De fait, bien qu'il soit exact que les dossiers médicaux soient des archives publiques au sens de l'article L. 213-4 du Code du patrimoine, ce sont également, et avant tout, des documents administratifs au sens de la loi du 17 juillet 1978, portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal[239], aujourd'hui codifié au Code des relations entre le public et les administrations. Ainsi, la lecture attentive des articles L. 311-5 à L. 311-8 de ce code nous permet de tenir une position différente de celle de la CADA et la DHOS. Ces articles distinguent trois catégories de documents administratifs : les documents non communicables, les documents communicables uniquement à l'intéressé et enfin les documents non communicables qui peuvent néanmoins l'être à titre d'exception et notamment, dans les conditions et délais prévus aux articles L. 213-1 et L. 213-2 du Code du patrimoine. Ainsi, une interprétation stricte de ces dispositions[240] nous permet d'affirmer que seuls les documents dont la liste est dressée à l'article L 311-5 du Code des relations entre le public et les administrations seraient exceptionnellement communicables dans les délais et conditions prévus à l'article L. 213-2 du Code du patrimoine. Or, les dossiers médicaux sont considérés, aux termes de l'article L. 311-6 du Code des relations entre le public et les administrations, comme uniquement communicables aux personnes intéressées. Ceci est d'ailleurs en adéquation avec les dispositions de l'article L. 1111-7 du Code de la santé publique, relatives à l'accès à son dossier médical par l'usager, article d'ailleurs expressément cité par les dispositions de la loi.
Dans cette hypothèse, les documents « *dont la communication porte atteinte au secret médical* » seraient tous ceux détenus par l'établissement de santé mais non présents au dossier médical. A titre d'exemple, il est possible de citer les documents de facturation ou encore les carnets de rendez-vous.

[239] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, *JORF* du 18 juillet 1978, p. 2851.
[240] BEAUJEAN, Isabelle. « L'inquiétant devenir des dossiers patients conservés par les établissements publics de santé au-delà de 25 ans.», *RDS*, n° 45, 2012, p. 236.

177. Cette circulaire, étonnante en plusieurs points, n'a toutefois suscité que peu de commentaires au sein de la doctrine. Ceux qui existent sont assez tranchés. Certains estiment que cette circulaire relève « *d'un emballement rocambolesque* », critiquent le raisonnement de la DHOS et estiment qu'il y a « *urgence à ne pas appliquer cette recommandation* »[241]. D'autres affirment tout simplement que « *la position de la CADA et de la DHOS semble critiquable* », précisant qu'en tout état de cause, l'avis de la CADA et la circulaire interprétative de la DHOS ne revêtent aucunement un caractère obligatoire.[242]
Au-delà des règles applicables aux archives publiques, l'utilisation des TIC en matière de conservation des données de santé a amené le législateur à créer un cadre spécifique relatif à l'hébergement de ces données sensibles.

§2. La conservation à l'ère des TIC : le cadre de l'hébergement des données de santé

178. La conservation des données de santé sur support informatique doit respecter un cadre réglementaire précis, instauré par le législateur dans un souci de protéger à la fois la confidentialité et la sécurité de ces données. Ainsi, l'hébergement des données de santé, et notamment l'hébergement externalisé auprès de tiers, répond à un cadre strict (A), instauré depuis plusieurs années et récemment rénové.

Toutefois, la problématique majeure aujourd'hui reste l'opposition de la technique et de son évolution, aux règles juridiques (B).

A. L'hébergement des données de santé : de l'agrément à la certification

179. L'activité d'hébergement de données de santé est strictement encadrée depuis plusieurs années. Les règles instaurées ont toutefois mis du temps, avant d'être pleinement applicables, (1) et l'agrément, dont la procédure est vite apparue comme lourde (2), a été

---

[241] ZORN-MACREZ, Caroline. « Les dossiers médicaux des défunts : des archives publiques non communicables », *RLDI*, n° 56, 2010, p. 63.
[242] BEAUJEAN, Isabelle. « L'inquiétant devenir des dossiers des patients conservés par les établissements publics de santé au-delà du délai de 25 ans », *op. cit.*, p. 36.

remplacé par une certification, instaurée par la loi de modernisation de notre système de santé[243], et complétée par une ordonnance de janvier 2017[244] (3).

1) Des règles à la mise en place laborieuse

180. La possibilité, pour un établissement ou un professionnel de santé, d'externaliser l'hébergement des données de santé informatisées auprès d'un tiers agréé, a été instaurée par la loi du 4 mars 2002[245]. Celle-ci a inséré au Code de la santé publique un article L. 1111-8 qui prévoit[246] les dispositions suivantes : « *toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime* ». Il est intéressant de préciser que jusque très récemment, le texte visait expressément les établissements de santé et les professionnels de santé ou la personne concernée par les données, comme débiteurs de cette obligation d'héberger les données auprès d'un tiers agréé. Depuis la loi de modernisation de notre santé, cette obligation incombe aux « *personnes physiques ou morales à l'origine de la production ou du recueil desdites données* » et porte sur les données de santé ainsi que sur les données relatives au suivi social ou médico-social d'une personne. La formulation finalement retenue est donc plus vaste.

181. Cette disposition du Code de la santé publique, qui a fait l'objet de sept modifications successives entre 2002 et 2016, est complétée par le décret du 4 janvier 2006[247]. Celui-ci précise les modalités propres au dossier de demande d'agrément, au comité d'agrément ainsi qu'au modèle du contrat qui doit être signé entre l'hébergeur et l'établissement de santé ou le

---

[243] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte 1.

[244] Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, *JORF* n°0011 du 13 janvier 2017, texte n° 17.

[245] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* du 5 mars 2002, p. 4118.

[246] L'article L. 1111-8 du Code de la santé publique a été modifié par l'article 96 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[247] Décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le Code de la santé publique, *JORF* n°4 du 5 janvier 2006, p. 174.

professionnel de santé qui externalise les données de santé recueillies. Or, la mise en place de ces dispositions n'a pas été simple. En effet, le décret prévoyait initialement une mise en œuvre des modalités pratiques d'agrément des hébergeurs au 1er janvier 2007. Toutefois, la loi du 30 janvier 2007[248] suspend la procédure d'agrément des hébergeurs et ce, pour une période de 2 ans à compter du 2 février 2007. En effet, l'article 25 IV de la loi prévoyait : « *sauf lorsqu'elle s'applique à des demandes d'agrément portant sur l'hébergement des dossiers médicaux personnels prévus à l'article L. 161-36-1 du Code de la sécurité sociale, la procédure d'agrément prévue à l'article L. 1111-8 du Code de la santé publique est suspendue pendant une période de deux ans à compter de la publication de la présente loi* ». La raison principale de cette suspension était la nécessité, pour assurer une bonne mise en œuvre de ces dispositions, d'adopter au préalable des référentiels de sécurité et d'interopérabilité, la procédure d'agrément étant difficile à mettre en œuvre tant que ces référentiels, permettant aux candidats d'obtenir une certification auprès d'organismes accrédités, n'étaient pas adoptés[249]. Là encore, le législateur a montré son incapacité à réagir suffisamment rapidement face au développement des technologies et le décalage entre technologie et encadrement juridique a conduit, pendant deux années, à un flou règlementaire dangereux pour les données sensibles que sont les données santé. A noter que durant cette période de suspension, les hébergeurs étaient tenus de satisfaire aux dispositions de la loi Informatique et Liberté et, à ce titre, obtenir un avis favorable de la CNIL[250].

182. C'est le GIP-DMP[251] qui a été chargé, pendant cette période, de définir le référentiel de constitution des dossiers de demande d'agrément. Cette élaboration a été effectuée en concertation avec les opérateurs, les industriels et les maîtrises d'ouvrages régionales du secteur de la santé. L'objectif affiché de ce référentiel était d'assurer aux candidats à l'hébergement « *un traitement équitable et efficace lors de leurs candidatures* »[252], mais également « *de traduire de façon concrète les exigences d'un texte réglementaire long et*

---

[248] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le Code de la santé publique, *JORF* n°27 du 1 février 2007, p. 1937.

[249] BALLET, Philippe. « Où en est la procédure d'agrément des hébergeurs de données de santé à caractère personnel ? », *Gaz. Pal.*, n° 109, 2007, p. 20.

[250] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le Code de la santé publique, *JORF* n°27 du 1 février 2007, p. 1937, texte n° 1.

[251] Aujourd'hui devenu l'Agence des Systèmes d'Information Partagée en santé (ASIP Santé).

[252] BOSSI, Jeanne. « Le rôle de l'Agence des systèmes d'information partagés de santé dans la procédure d'agrément », *Actualités Jurisanté*, n° 74, juillet 2011, p. 9.

compliqué »[253]. A la reprise de la procédure d'agrément, les hébergeurs ont été tenus de déposer un dossier de demande d'agrément, et d'obtenir celui-ci afin de pouvoir maintenir leur activité. A l'heure actuelle[254], une centaine d'agréments ont été délivrés par le comité. Ceux-ci concernent parfois une même société, qui propose plusieurs types d'activité d'hébergement différents. L'activité du comité est néanmoins amenée à disparaitre, puisque l'ordonnance du 12 janvier 2017[255] substitue à la procédure d'agrément, une procédure de certification.

2) L'agrément des hébergeurs : une procédure critiquée

La procédure d'agrément des hébergeurs est décrite très précisément au sein du décret dit "hébergeur" (a). Celle-ci présente un certain nombre de lacunes (b), sources de critiques régulières.

a) Points essentiels de la procédure

183. Le but principal de la procédure instaurée par le décret du 4 janvier 2006 est d'organiser et d'encadrer le dépôt, la conservation et la restitution des données de santé à caractère personnel et ce, dans des conditions qui vont permettre de garantir la confidentialité et la sécurité des données. De ce fait, le décret hébergeur a mis en place une procédure stricte et formalisée, applicable à toute personne ou entreprise, dès lors qu'elle conserve des données de santé de personnes pour lesquelles elles n'interviennent pas dans la prise en charge médicale. La procédure se déroule en plusieurs temps. Le dossier de demande d'agrément, formalisé selon le référentiel de constitution des dossiers mis en place par l'ASIP santé, sera d'abord soumis à la CNIL, qui dispose d'un délai de deux mois renouvelable une fois, afin d'apprécier « *les garanties présentées par le candidat en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données* »[256]. La demande est ensuite transmise, avec l'avis de la CNIL le cas échéant, au comité d'agrément des hébergeurs[257], qui dispose d'un délai d'un mois, renouvelable une fois,

---

[253] *Ibid.*

[254] Chiffres en date du 25 novembre 2016, vérifiés sur le site de l'ASIP santé : [http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees]

[255] Article 1er de l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, *JORF* n°0011 du 13 janvier 2017, texte n° 17.

[256] Article R. 1111-10 du Code de la santé publique.

[257] Ce comité, placé auprès du ministre chargé de la santé a été créé par le décret de janvier 2006. Ces membres, qui sont nommés pour 5 ans par arrêté du ministre en charge de la santé, sont les suivants : un membre de

pour rendre un avis sur le dossier de candidature à l'agrément. Sur demande du secrétaire général du Ministère chargé des Affaires Sociale, l'ASIP Santé a été chargée d'instruire préalablement les dossiers de demandes d'agrément, afin de faciliter le travail du Comité. Ainsi, un comité d'instruction, interne à l'ASIP Santé, a été mis en place en 2009, ayant pour mission de rédiger un rapport ainsi que des recommandations globales, qui sont transmis ensuite au comité d'agrément. Enfin, une fois l'avis du comité rendu, le ministre chargé de la santé dispose d'un délai de deux mois pour prendre sa décision. Passé ce délai, la demande est réputée rejetée.

184. Une fois agréés, les hébergeurs s'engagent à rendre chaque année un rapport d'auto-évaluation. Cette procédure, qui repose principalement sur une relation de confiance, est toutefois complétée par de possibles contrôles de la CNIL. A titre d'exemple, en 2011, la CNIL a prononcé un avertissement à l'encontre d'un hébergeur de données de santé, suite à une déclaration mensongère, contenue dans son dossier de demande d'agrément. En l'espèce, la société prétendait chiffrer les données médicales hébergées, par le biais d'un procédé de "chiffrage fort"[258] ce qui n'était pas le cas. Lors d'un contrôle sur place réalisé en 2011, la CNIL a constaté que les données n'étaient pas chiffrées et qu'elles étaient de plus accessibles aux administrateurs informatiques de la société. Dans l'avis rendu par la CNIL, celle-ci s'est prononcée sur les garanties présentées par le candidat en matière de sécurité des données de santé faisant l'objet d'un traitement informatisé et avait estimé que l'hébergeur ne respectait pas l'obligation posée à l'article 6-1 de la loi Informatique et Liberté, à savoir traiter les données de manière licite.

b) Une procédure remise en cause

La procédure d'agrément des hébergeurs de données de santé a fait l'objet de plusieurs critiques.

---

l'inspection des affaires sociales, de représentant des associations compétentes en matière de santé, 2 représentants des professionnels de santé et de 3 personnalités qualifiées dans les domaines de l'éthique et du droit, de la sécurité des systèmes d'information et dans le domaine économique et financier.

[258] Le chiffrement est une des quatre fonctions assurées par la cryptologie. Le chiffrement de données consiste à rendre illisibles et inaccessibles ces données. Seules les personnes détenant une clé spécifique pourront alors accéder aux données. Il existe plusieurs techniques de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

185. La première concerne bien évidemment les délais de procédure. Ceux-ci peuvent en effet sembler assez longs, la procédure officielle pouvant durer entre cinq et huit mois, sans compter la procédure d'instruction préalable des dossiers par le comité d'instruction de l'ASIP Santé. En août 2011, le comité d'agrément des hébergeurs a rendu son premier rapport d'activité, couvrant les années 2006 à 2011. Après avoir rappelé le cadre et le déroulement de la procédure, le comité dresse un bilan de son activité. Il en ressort que cet encadrement et la démarche d'agrément sont globalement perçus de manière positive par les professionnels du secteur. Toutefois, le comité d'agrément pointe du doigt le fait que les expertises menées par l'ASIP Santé d'une part, et par la CNIL, d'autre part, portent en partie sur des points identiques. Cela génère des coûts importants, en termes de ressources humaines et financières. Le comité d'agrément souligne également que les hébergeurs doivent faire face à une contrainte pratique supplémentaire qui est celle des dates de réunion du comité d'agrément et des séances de la CNIL. Cette volonté d'alléger la procédure afin de la rendre plus fluide, nous paraît être effectivement une solution pragmatique à adopter rapidement. Enfin, le comité d'agrément s'interroge, à juste titre, sur « *le type d'écosystème qui va se mettre en place si les procédures d'agrément se complexifient* »[259], précisant que l'activité d'hébergement des données de santé pourrait alors être de fait réservée aux sociétés industrielles de grande taille, éloignées du patient et de ses problématiques.

186. L'autre critique qui peut être formulée à l'encontre du décret hébergeur, concerne l'absence d'adéquation entre les textes juridiques et les aspects techniques d'aujourd'hui. En effet, comme le souligne la secrétaire générale de l'ASIP Santé[260], les modèles pris par le législateur dans le décret de 2006 ne reflètent pas la réalité concrète et opérationnelle des offres actuelles sur le marché, et certaines exigences juridiques sont de fait inadaptées aux caractéristiques des technologies actuelles. Le risque principal de cette inadéquation serait, selon l'auteur, d'amener l'ASIP Santé à étudier des demandes d'agrément portant sur une application métier spécifique qui manipule des données de santé, alors que seul l'hébergement de ces données est soumis à agrément. De même, les documents qui, selon le décret, doivent accompagner le dossier d'agrément, ne sont pas toujours pertinents. A titre d'exemple, la nature des documents réclamés afin de vérifier la capacité financière de l'hébergeur ne permet

[259] Premier rapport d'activité du comité d'agrément des hébergeurs : 2006-2011, p. 27.
[260] BOSSI, Jeanne. « Le rôle de l'Agence des systèmes d'information partagés en santé dans la procédure d'agrément », *op. cit.*, p. 13.

pas, toujours selon Jeanne BOSSI, d'avoir une vision précise et nette de la véritable situation financière du candidat. Le décret dispose en effet que le candidat à un agrément fournisse : « *un document présentant les comptes prévisionnels de l'activité d'hébergement et, éventuellement, les trois derniers bilans et la composition de l'actionnariat du demandeur, ainsi que, dans le cas d'une demande de renouvellement, les comptes de résultat et bilans liés à cette activité d'hébergement depuis le dernier agrément* »[261].

187. D'une manière générale, nous adhérons à la vision pragmatique de la secrétaire générale de l'ASIP Santé : alors que le décret hébergeur expose les objectifs à atteindre par les hébergeurs, il appartient aux référentiels d'exposer les moyens à mettre en œuvre pour les atteindre. C'est pourquoi Jeanne BOSSI avait proposé de revoir le décret hébergeur, en prévoyant notamment, un renvoi systématique aux référentiels afin que le texte ne devienne pas rapidement obsolète. Une des solutions avancée à la fois par le comité d'agrément des hébergeurs dans son premier rapport d'activité, et rappelée dans le second[262], mais également par la secrétaire générale de l'ASIP Santé, était de s'orienter vers une procédure de certification menée par des organismes accrédités, en s'inspirant notamment de ce qui peut exister dans le domaine bancaire. C'est d'ailleurs dans cette direction que s'est orienté le législateur, avec la loi de modernisation de notre système de santé et l'ordonnance n°2017-27 du 12 janvier 2017, relative à l'hébergement des données de santé à caractère personnel.[263]

c) L'adoption définitive d'une procédure de certification

188. L'article 204 de la loi de modernisation de notre système de santé prévoit que dans les 12 mois suivant la promulgation de la loi, le gouvernement est autorisé à prendre par voie d'ordonnance plusieurs mesures visant, entre autres, à : « *remplacer l'agrément prévu au même article L. 1111-8 par une évaluation de conformité technique réalisée par un organisme certificateur accrédité par l'instance nationale d'accréditation mentionnée à l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie ou par l'organisme compétent d'un autre Etat membre de l'Union européenne. Cette certification de conformité porte notamment sur le contrôle des procédures, de l'organisation et des moyens*

[261] *Ibid.*
[262] Rapport d'activité 2013-2013 du Comité d'Agrément des Hébergeurs, consultable en ligne sur [http://esante.gouv.fr]. Consulté le 15 mai 2017.
[263] Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, *JORF* n°0011 du 13 janvier 2017, texte n° 17.

matériels et humains ainsi que sur les modalités de qualification des applications hébergées ».

189. L'ordonnance du 12 janvier 2017 a instauré cette procédure de certification, en remplacement de la procédure d'agrément telle qu'elle existait. Désormais, les prestataires de service d'hébergement externalisé de données de santé devront être certifiés par des organismes de certification accrédités par l'instance française d'accréditation ou l'instance nationale d'accréditation d'un autre Etat de l'Union européenne. Un décret pris en Conseil d'Etat doit encore venir préciser les conditions dans lesquelles seront délivrés ces certificats. Cependant, l'ordonnance n'est pas applicable immédiatement. En effet, le législateur a prévu un temps de transition pendant lequel la procédure d'agrément reste applicable. Ainsi, par principe, l'ordonnance entrera en vigueur à une date fixée par décret et au plus tard au 1er janvier 2019. Dans l'intervalle, les demandes d'agrément ou de renouvellement d'agrément, déposées avant l'entrée en vigueur de l'ordonnance, continuent d'être étudiées au titre de l'agrément. Par ailleurs, les organismes agréés conservent le bénéfice de leur agrément jusqu'à leur terme. Si celui-ci arrive à échéance dans les douze mois suivant l'entrée en vigueur de l'ordonnance, ils disposeront d'un certain délai, fixé par décret, pour se mettre en conformité et obtenir une certification.

190. Cette nouvelle procédure devra permettre « d'accroître la sécurité des données de santé hébergées en complétant les audits documentaires par des audits sur site, de réduire les délais d'instruction des demandes des hébergeurs, aujourd'hui trop importants, et de faire bénéficier les acteurs concernés de la visibilité du dispositif à l'international par une référence à des certifications ISO largement répandues à l'échelle européenne et mondiale »[264].

B. La reprise de l'existant : l'éventualité de la numérisation des dossiers papier.

191. La numérisation éventuelle des anciens dossiers papier est une hypothèse qui illustre bien l'opposition qui peut exister entre les contraintes techniques et les contraintes juridiques. Ainsi, cette hypothèse ne pourra être envisagée qu'à certaines conditions strictes (1) et

[264] Rapport au Président de la République relatif à l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, *JORF* n° 0011 du 13 janvier 2017, texte n° 16.

soulèvera en tout état de cause la question du devenir des dossiers papiers (2), dont la portée n'est pas négligeable.

1) Les conditions de la numérisation des dossiers existants

192. Face au développement massif des dossiers médicaux informatisés, une question majeure se pose : que va-t-il advenir du dossier papier ? Comme nous l'avons vu, la conservation des dossiers médicaux, qu'ils soient papiers ou électroniques, est soumise à des conditions de délais strictes. Ainsi, pour que les dossiers soient parfaitement complets, et les règles respectées, deux choix s'offrent à l'établissement public de santé : soit conserver en parallèle un dossier papier et un dossier informatisé, soit numériser l'ensemble des dossiers papier afin de les intégrer au dossier informatique.

193. La première solution est, dans les faits, la plus simple, mais néanmoins la plus encombrante pour les établissements de santé. De plus, elle ne se révèle pas la plus pratique pour les professionnels de santé, obligés de consulter les deux dossiers médicaux afin d'obtenir tous les éléments relatifs au patient. Enfin, cette solution est contraire à la logique actuelle qui tend à une informatisation complète des archives hospitalières de tout type, pour des raisons pratiques mais également de développement durable. La seconde solution permettrait un passage définitif au dossier informatisé. Toutefois, cette reprise de l'existant via une numérisation de l'ensemble des dossiers papier présente des difficultés à la fois techniques et juridiques.

194. Du point de vue technique, il faut reconnaître que cette opération va se révéler fastidieuse, voire irréalisable dans certains établissements publics de santé, au vu de la quantité de documents que représentent les dossiers médicaux. De plus, il va être nécessaire de stocker tous ces documents numérisés sur des serveurs, ce qui induit une capacité de stockage en interne ou externalisée conséquente et donc un coût supplémentaire. D'un point de vue juridique, une question intéressante doit être soulevée : quelle sera la valeur de ce document numérisé ? Pendant longtemps, la réponse à cette question était quelque peu incertaine, et il était nécessaire de se tourner vers les règles de droit commun pour tenter d'y

répondre (a). Mais récemment, l'ordonnance n°2017-29 du 12 janvier 2017[265], prise en application de l'article 204 de la loi de modernisation de notre système de santé[266], est venue y apporter une réponse précise (b).

a) Les règles applicables en droit commun

195. Pour répondre à cette interrogation, il nous faut d'abord nous tourner vers les textes applicables en matière de droit de la preuve, dans la mesure où l'écrit électronique n'est envisagé par le législateur que sous l'angle probatoire. La validité comme preuve juridique d'un document numérique est reconnue depuis 2000. C'est la loi n° 2000-230[267] qui est venue modifier le Code civil. Celui-ci prévoit désormais que « *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* »[268]. Deux conditions cumulatives sont posées par le législateur. Dans un premier temps, la personne de qui émane le document, doit pouvoir être identifiée. Pour cela, la personne a la possibilité de signer électroniquement le document. La signature électronique est prévue à l'article 1367 du Code civil : « *la signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle 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'Etat* ». Il s'agit en pratique d'un procédé, retenu pour garantir l'authenticité des documents numériques, et reposant sur un procédé cryptographique[269]. En matière de données de santé, cette signature est apposée par le biais de la Carte de Professionnel de Santé (CPS), délivrée

---

[265] 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, *JORF* n° 0011, 13 janvier 2017, texte n° 21.

[266] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n° 0022, 27 janvier 2016, texte n° 1.

[267] 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 du 14 mars 2000, p. 3968.

[268] Article 1366 du Code civil.

[269] Pour plus de détails sur la signature électronique, voir le Mémento édité par le bureau conseil de la Direction Centrale de la Sécurité des Systèmes d'Information et consultable en ligne sur : [http://www.ssi.gouv.fr]. Consulté le 15 mai 2017.

par l'ASIP Santé[270]. La carte CPS est une carte qui contient les données d'identification du professionnel qui en est le porteur (identité, numéro RPPS, modalités d'exercice). Cette carte permet aux professionnels de santé, entres autres, d'apposer leur signature électronique sur les documents qu'ils produisent.

196. La seconde condition posée à l'article 1366 du Code civil est celle de l'intégrité du document. Cette notion, qui n'est pas définie par la loi, mérite que nous la précisions. Garantir l'intégrité d'un document consiste à s'assurer qu'il ne soit pas altéré[271], que ce soit par le biais d'une manipulation ultérieure, ou par une dégradation de son support de conservation et donc de sa lisibilité. L'information doit être maintenue dans son intégralité. De même, le support de conservation doit apporter les garanties nécessaires en termes de pérennité : l'information ne doit pas être modifiée ou pire, disparaître. Finalement, l'intégrité d'un document dépend beaucoup de la qualité de son archivage. Il est donc nécessaire de mettre en place un processus fiable de gestion du cycle de vie du document[272].

197. Toutefois, ces conditions de validité ne s'appliquent qu'aux documents créés électroniquement, et non pas aux documents papier originaux, dont une copie serait ensuite conservée sur informatique, par le biais de la numérisation. Qu'en est-il de ces documents ? En matière de force probante d'une copie, l'article 1379 dispose que : « *la copie fiable a la même force probante que l'original. La fiabilité est laissée à l'appréciation du juge. Néanmoins est réputée fiable la copie exécutoire ou authentique d'un écrit authentique. 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'État. Si l'original subsiste, sa présentation peut toujours être exigée* ».

198. En ce qui concerne plus particulièrement les copies numérisées, la Cour de cassation avait déjà, en 2008, apporté un éclairage sur le sujet. Dans un arrêt en date du 4 décembre 2008[273], la Haute juridiction précisait la chose suivante : « *lorsqu'une partie n'a pas conservé*

---

[270] *V. Infra*. n° 244.
[271] RAYNOUARD, Arnaud. « Le droit de l'écrit électronique », *LPA*, 2001, n° 65, p. 15.
[272] RENARD, Isabelle. « Preuve informatique – valeur juridique du document numérique », *Expertises*, 2010, p. 215.
[273] Cass. 2ème civ, 4 décembre 2008, n° 07-17622.

l'original d'un document, la preuve de son existence peut-être rapportée par la présentation d'une copie qui doit en être la reproduction non seulement fidèle mais durable […] L'écrit sous forme électronique ne vaut preuve qu'à condition que son auteur puisse être dûment identifié et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». En l'espèce, la CPAM de la Marne avait, pour apporter la preuve de la délivrance d'une information, produit ce qu'elle présentait comme étant la copie informatique d'un courrier. La Cour de Cassation a cassé la décision d'appel, rappelant alors les critères permettant d'accepter une copie électronique comme élément de preuve. Les premiers critères posés par la Cour avait trait à la copie en elle-même, qui se devait d'être la reproduction fidèle et durable de l'original. Rien d'exceptionnel dans ces critères qui sont ceux opposables à n'importe quelle copie, qu'elle soit papier ou électronique. Nous rappellerons simplement qu'une copie fidèle signifie que celle-ci doit être l'exacte reproduction de l'original (par exemple, si le document original était signé manuellement, cette signature doit apparaitre sur la copie). En ce sens, la numérisation d'un document papier permettait de remplir ce critère de copie fidèle. Les seconds critères concernaient plus particulièrement, quant à eux, la copie sous forme électronique. Celle-ci doit permettre d'identifier son auteur et doit être conservée dans des conditions permettant de garantir son intégrité. Concernant l'indentification de l'auteur du document, ce qui importait était finalement de savoir à qui il pouvait être imputable. Se posait alors la question de savoir si cela impliquait que le document soit forcément "signé". Pour certains auteurs, ce n'était pas le cas, un simple papier à en-tête ou logo distinctif permettant de savoir de qui émane le document[274].

199. Cependant, ce raisonnement montrait vite ses limites selon nous. En effet, il est aujourd'hui très simple de falsifier un logo ou un papier à en-tête, surtout quand il s'agit d'un document électronique. Le décret n° 2016-1673 du 5 décembre 2016[275] relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du Code civil pose de manière précise et définitive les critères que doivent remplir les copies numériques pour être considérées comme fiables. Ainsi, selon les dispositions de l'article 1er du décret, « *est présumée fiable, au sens du deuxième alinéa de l'article 1379 du Code civil, la copie résultant :*

[274] RENARD, Isabelle, « Preuve informatique – valeur juridique du document numérique », *op. cit.*, p. 215.
[275] 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 du 6 décembre 2016, texte n° 61.

- soit d'un procédé de reproduction qui entraîne une modification irréversible du support de la copie ;
- soit, en cas de reproduction par voie électronique, d'un procédé qui répond aux conditions prévues aux articles 2 à 6 du présent décret ».

200. Les articles 2 à 6 du décret fixent des conditions très strictes. Le texte exige que le procédé de reproduction par voie électronique permette d'apporter des informations liées à la copie afin de l'identifier. Le contexte de numérisation et la date de création de la copie doivent être précisés. Par ailleurs, l'intégrité de la copie doit être attestée « *par une empreinte digitale qui garantit que toute modification ultérieure de la copie à laquelle elle est attachée est détectable* ». Pour ce faire, le texte exige que les établissements de santé fassent le choix entre un système d'horodatage qualifié, d'un cachet électronique qualifié ou d'une signature électronique, tel que prévu par le 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. Enfin, « *la copie électronique est conservée dans des conditions propres à éviter toute altération de sa forme ou de son contenu. 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 de la copie* ». Cette dernière disposition présente l'intérêt d'être, selon nous, parfaitement adaptée aux contraintes des techniques informatiques actuelles. En effet, aujourd'hui, peu de techniques sont suffisamment fiables pour permettre de garantir une conservation intègre et durable des documents électroniques[276]. Ainsi, en précisant que les opérations « *requises pour assurer la lisibilité de la copie électronique dans le temps* » n'altèrent pas la fiabilité de la copie, le législateur permet d'envisager la mise en place des opérations de conversion des formats informatiques, au gré des évolutions techniques, sans que cela n'entache la valeur probante de la copie.

201. La numérisation de l'ensemble des dossiers médicaux papier afin de les intégrer aux dossiers informatisés serait donc juridiquement possible, sous réserve de se plier à un certain

[276] En pratique, il est conseillé d'utiliser des disques WORM (Write Once Read Many), qui sont réinscriptibles. C'est le cas par exemple des disques optiques numérisés. Il faut également privilégier des formats électroniques standardisés du type XLM, PDF ou TIFF.

nombre de contraintes strictes. Toutefois, en pratique, il s'agit d'un chantier très important pour les établissements publics de santé, qui induit un coût financier et humain non négligeable. A noter qu'une ordonnance de janvier 2017[277], prise en application de l'article 204 de la loi de modernisation de notre système de santé, a définitivement acté, au sein du Code de la santé publique, la possibilité pour des documents contenant des données de santé, d'être numérisés tout en conservant une force probante[278]. Cependant, le législateur ne fait que rappeler, au sein du Code de la santé publique les dispositions du Code civil. Aucune nouveauté ni simplification donc, mais la précision que ces dispositions du droit commun s'appliquent bel et bien aux documents comportant des données de santé.

2) Le devenir des dossiers papier numérisés

202. Une fois les dossiers médicaux papier numérisés, ceux-ci deviennent redondants avec le dossier informatisé. Une suppression de ceux-ci est-elle pour autant envisageable ? Cette question, qui est commune à de nombreuses administrations, a été fréquemment posée aux Archives départementales. Les Archives de France avaient ainsi, dans un premier temps, posé un cadre de commun à l'élimination anticipée d'archives publiques papier qui auraient été numérisées (a). Cependant, face aux nombreuses demandes des établissements de santé, en faveur notamment d'un cadre plus adapté, le législateur s'est emparé du sujet (b).

a) La réponse des Archives de France

203. C'est par le biais d'une instruction de 2005[279] relative aux modalités de délivrance du visa d'élimination des documents papiers transférés sur support numérique ou micrographique que les Archives de France ont apporté une première réponse à la question du devenir du papier numérisé. Cette instruction rappelait la nécessité, pour l'administration qui souhaitait détruire ses archives papiers avant la fin de leur durée de conservation, d'obtenir une autorisation d'élimination de la part de la direction départementale des archives, et ce, même

[277] 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, *JORF* n°0011 du 13 janvier 2017, texte n° 21.

[278] Le nouvel article L. 1111-26 du Code de la santé publique prévoit que « *la copie numérique d'un document mentionné à l'article L. 1111-25, remplissant les conditions de fiabilité prévues par le deuxième alinéa de l'article 1379 du Code civil, a la même force probante que le document original sur support papier*. »

[279] Instruction DITN/DPACI/RES/2005/001 du 14 janvier 2005 sur les modalités de délivrance du visa d'élimination des documents papiers transférés sur support numérique ou micrographique, Archives de France, non publiée au *JORF*.

si une copie a été réalisée sur un autre support. Cette instruction précisait les cas (au nombre de trois) dans lesquels cette autorisation pouvait être délivrée. Le premier cas concernait les documents qui sont normalement éliminables au terme de leur durée d'utilité administrative. Dans ce cas, un visa d'élimination anticipé pouvait être accordé. Le deuxième cas concernait les documents qui devaient être conservés en totalité, et de manière définitive, au terme de leur durée d'utilité administrative : pour ces documents, les documents papier, une fois numérisés, pouvaient être versés aux archives départementales de manière anticipée, si leur conservation posait « *des problèmes particulièrement aigus* » à l'administration concernée. Enfin, si les documents concernés étaient normalement soumis au tri par échantillonnage, une combinaison des deux précédentes règles devait alors s'appliquer : une autorisation d'élimination anticipée pouvait être délivrée pour les documents normalement éliminables à terme, tandis que l'échantillon retenu était conservé en version papier et pouvait être déposé aux archives départementales au besoin.

204. Dans tous les cas, l'autorisation d'élimination anticipée devait être assortie de recommandations. Il était notamment recommandé à l'administration de réaliser, avant d'envisager la destruction des archives papier, une analyse juridique. Celle-ci avait pour but de déterminer les potentiels besoins en matière de preuve, les risques de contentieux et donc chercher à savoir si les copies numérisées qu'elle souhaitait réaliser, respectaient les critères nécessaires afin de conserver une valeur probante suffisante. Les Archives de France précisaient que, pour assurer une meilleure sécurité juridique, il pouvait éventuellement être nécessaire de conserver certaines archives papiers et ce, jusqu'à la fin de leur durée d'utilité administrative. Les Archives de France conseillaient enfin aux administrations qui s'orientaient vers une numérisation de l'ensemble de leurs archives papier, de suivre une procédure rigoureuse garantissant la qualité de leur démarche.

205. Plusieurs possibilités s'offraient alors aux administrations. Celles-ci pouvaient appliquer les principes posés par Dominique PONSOT dans son rapport intitulé « Valeur juridique des documents conservés sur support photographique ou numérique »[280] : opérer dans un cadre systématique, c'est-à-dire traiter de la même façon tous les documents appartenant à la même catégorie et/ou remplissant la même fonction probatoire, dater la copie,

[280] PONSOT, Dominique, « Valeur juridique des documents conservés sur support photographique ou numérique », Rapport de septembre 1995, *La Documentation française*, p. 37.

s'assurer d'effectuer une copie reproduisant le plus grand nombre de caractéristiques physiques du document (par exemple les annotations manuscrites), et enfin, dans le but de se pré-constituer une preuve de l'opération réalisée, présenter de manière précise le processus de numérisation mis en place. Les administrations pouvaient aussi s'inspirer de normes existantes. En la matière, on trouvait par exemple la norme AFNOR NF Z 42-013, intitulée « *recommandations relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes* ».

La suppression des archives papier qui auraient été numérisées était donc possible. Cependant, les établissements publics de santé devaient rester prudents et réalistes face aux exigences posées par les Archives de France. La loi de modernisation de notre système de santé s'est depuis penchée sur le sujet.

b) Les apports de la loi de modernisation de notre système de santé

206. L'article 204 de la loi de modernisation de notre système de santé prévoyait la possibilité pour le gouvernement de légiférer par voie d'ordonnance afin d' « *encadrer les conditions de destruction des dossiers médicaux conservés sous une autre forme que numérique quand ils ont fait l'objet d'une numérisation et préciser les conditions permettant de garantir une valeur probante aux données et documents de santé constitués sous forme numérique* ». L'ordonnance en question a été adoptée en janvier 2017[281] et vient ainsi encadrer la destruction des documents papiers numérisés. Ce texte insère, au sein du Code de la santé publique, une nouvelle section intitulée « conditions de reconnaissance de force probante des documents comportant des données de santé à caractère personnes créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique ». Ainsi, il est désormais possible, « *lorsqu'une copie fiable a été réalisée* »[282] de détruire un document original avant la fin de sa durée légale de conservation. A noter toutefois que pour les documents qui relèvent du champ des archives publiques, l'autorisation de destruction sera toujours soumise au visa de l'administration des archives.

[281] 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, *JORF* n°0011 du 13 janvier 2017, texte n° 21.
[282] Article L. 1111-26 du Code de la santé publique.

Conclusion de la section

207. Même informatisées, les données de santé conservent le statut d'archives hospitalières et, à ce titre, leur archivage doit respecter la réglementation en la matière et notamment, les dispositions du Code du patrimoine. Ces règles ont des conséquences, à la fois sur la gestion de la vie courante des archives numériques, mais également en ce qui concerne leur éventuelle élimination. Nous pouvons, par ailleurs, regretter les difficultés d'interprétation de certaines de ces règles, qui sont parfois contradictoires avec les règles classiques relatives à la gestion des données de santé, telles que celles qui ont trait au secret médical, fragilisant ainsi la sécurité et la confidentialité des données de santé.

208. La conservation des données de santé informatisées a fait, quant à elle, l'objet d'une réelle réflexion de la part du législateur, conscient des enjeux qui entourent la sécurité et la confidentialité de ces données. Cela a abouti aux différents textes et référentiels qui encadrent et organisent aujourd'hui l'hébergement des données de santé. Ce cadre n'est toutefois pas parfait et certains ajustements permettraient d'en améliorer l'efficacité. A l'heure actuelle, un des enjeux essentiels de la conservation informatisée des données de santé reste l'adéquation entre le développement de la technique et l'encadrement juridique mis en place.

Section 2. Hébergement et communication des données : un cadre limité

209. L'analyse des textes actuels encadrant l'hébergement et la communication électronique des données de santé nous amène à conclure que, malheureusement, ceux-ci se montrent trop limités. D'une part, le choix d'un hébergement externalisé des données de santé amène les établissements à se poser plusieurs questions juridiques, pas toutes résolues par le corpus de textes relatif à l'hébergement agréé (Paragraphe 1). D'autre part, l'encadrement actuel de la communication par voie électronique des données de santé n'est que partiellement en place et donc difficilement applicable (Paragraphe 2).

§1. L'hébergement des données de santé, un cadre incomplet

210. L'article L. 1111-8 du Code de la santé publique, complété par le décret dit "hébergeur", instaure un cadre strict relatif à l'hébergement des données de santé. Toutefois, la création et le développement de cette nouvelle activité posent, en pratique, de nombreuses questions, qui ne sont pas directement résolues par ces textes. Ainsi, le choix de l'hébergeur soulève des problématiques concrètes qui ne peuvent être résolues qu'en faisant appel à d'autres règles de droit (A). De même, à la lecture des textes encadrant l'hébergement des données de santé, il est légitime de se poser la question de la réelle place accordée au patient et à ses droits (B).

A. Choix de l'hébergeur et questions en suspens

211. Aujourd'hui, les établissements de santé peuvent faire le choix d'être leur propre hébergeur de données de santé ou de confier cette charge à un tiers. Cependant, les choses se compliquent quand ce tiers est un autre établissement de santé (1). Par ailleurs, si l'établissement fait le choix de confier ses données à un tiers, il devra alors se soumettre à d'autres règles en plus de celles strictement applicables à l'hébergement externalisé des données de santé (2).

1) L'hypothèse d'un établissement de santé hébergeur de données

212. Un établissement de santé, qui choisirait d'être son propre hébergeur de données, n'a pas à obtenir d'agrément. En effet, l'article L. 1111-8 du Code de la santé publique est très clair à ce sujet et le périmètre de l'agrément (et, à compter du 1er janvier 2019, de la certification) ne concerne que les cas dans lesquels les données ont été déposées auprès de personnes tiers. Mais *quid* dans le cas où un établissement de santé hébergerait les données d'un autre établissement ou un autre professionnel ? Cette hypothèse existe par exemple dans le cas de mise en place de réseaux de télémédecine. En toute logique, l'établissement devenant un tiers hébergeur devra donc répondre aux obligations posées par l'article L. 1111-8 du Code de la santé publique ainsi que celles du décret "hébergeur". Cependant, une autre question se pose alors, celle de la possibilité juridique, pour un établissement de santé, d'assurer des missions de tiers hébergeur de données de santé. En effet, les établissements publics de santé sont soumis au principe de spécialité et sont donc tenus de limiter leurs activités aux missions qui leur ont été fixées par la loi. Il ne leur est donc pas possible, en théorie, de sortir du champ de compétence qui leur a été attribué. L'hébergement de données de santé d'autres établissements pourrait-il entrer dans les compétences d'un établissement public de santé ?

213. Les missions des établissements de santé sont prévues à l'article L. 6111-1 du Code de la santé publique[283] et l'hébergement de données de santé pour le compte d'un autre établissement public ou privé de santé ne fait pas partie de la liste exhaustive dressée par l'article. Toutefois, l'article L. 6145-7 du Code de la santé publique prévoit quant à lui la possibilité pour un établissement public de santé, sans porter atteinte au principe de spécialité, d'effectuer des prestations de service à titre subsidiaire. Reste à savoir ce que recouvre cette notion de prestation réalisé à titre subsidiaire.

---

[283] *« Les établissements de santé publics, privés et privés d'intérêt collectif assurent, dans les conditions prévues par le présent Code, le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes. Ils délivrent les soins avec hébergement, sous forme ambulatoire ou à domicile, le domicile pouvant s'entendre du lieu de résidence ou d'un établissement avec hébergement relevant du Code de l'action sociale et des familles. Ils participent à la coordination des soins en relation avec les membres des professions de santé exerçant en pratique de ville et les établissements et services médico-sociaux, dans le cadre défini par l'Agence Régionale de Santé en concertation avec les conseils généraux pour les compétences qui les concernent. Ils participent à la mise en œuvre de la politique de santé publique et des dispositifs de vigilance destinés à garantir la sécurité sanitaire. Ils mènent, en leur sein, une réflexion sur l'éthique liée à l'accueil et la prise en charge médicale* »

214. Le juge administratif est venu apporter quelques précisions à ce sujet. Dans une décision du 29 mars 2000, la Cour administrative d'appel de Nantes[284] a considéré qu'une prestation de blanchisserie, assurée par un établissement public de santé au profit d'une clinique privée, n'entrait pas dans les critères de l'article L. 6145-7 du Code de la santé publique, dès lors que l'activité concernée est sans rapport avec les missions dévolues aux établissements de santé. Pour le juge administratif, une activité exercée à titre subsidiaire doit donc obligatoirement constituer le prolongement d'une activité principale d'un établissement public de santé. Certains auteurs voient, dans cette jurisprudence, l'affirmation selon laquelle un établissement public de santé ne pourrait pas être hébergeur de données de santé, considérant que l'article L. 1111-8 du Code de la santé publique « *n'avait pas pour but d'ouvrir un potentiel d'activité commercial aux établissements publics eux-mêmes* »[285].

215. Pourtant, aujourd'hui, plusieurs établissements de santé sont devenus hébergeurs agréés de données de santé. C'est le cas, par exemple, du Centre Hospitalier Universitaire de Nice, qui a reçu trois agréments différents pour l'hébergement de données de santé. Deux d'entre eux concernent l'utilisation d'une application informatique spécifique (les applications e-nadis et Calliope) et le troisième concerne l'exploitation et la gestion, par le CHU, d'une plateforme technique sur laquelle sont hébergées des applications de ses partenaires. Les Hospices Civils de Lyon sont également agréés pour l'hébergement d'applications gérant des données de santé à caractère personnel, tout comme l'Assistance Publique des Hôpitaux de Paris et l'Assistance Publique des Hôpitaux de Marseille. Enfin, le CHU de Nantes a, quant à lui, reçu un agrément pour une activité d'hébergement assez large, puisqu'il est agréé pour « *une prestation d'hébergement d'applications fournies par les clients et gérant des données de santé à caractère personnel, ainsi que pour une prestation d'hébergement de serveurs contenant des données de santé à caractère personnel* »[286]. Les établissements publics de santé sont donc en train de développer une réelle activité d'hébergement de données de santé.

216. De notre point de vue, il semble raisonnable d'envisager la possibilité pour les établissements publics de santé de développer ce type d'activité. En effet, ce sont bien les établissements de santé qui sont les plus à même de prendre en compte à la fois, les

---

[284] CAA Nantes, 29 mars 2000, Centre Hospitalier de Morlaix, n° 97NT00451.
[285] MARZOUG, Sanaa. « L'hébergement des données de santé à caractère personnel des établissements de santé : quelques repères juridiques », *Actualités JuriSanté*, n° 74, 2011, p. 5.
[286] Description disponible sur le site de l'ASIP santé, [http://esante.gouv.fr], consulté le 2 mars 2017.

contraintes techniques et juridiques qui les entourent, mais également de concilier les besoins des professionnels de santé avec la confidentialité et la sécurité dus aux données de santé des patients. De plus, une interprétation plus souple de l'article L. 6111-1 du Code de la santé publique permet d'envisager l'hébergement des données de santé comme étant le prolongement direct de la mission principale des établissements publics de santé qu'est le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes.

Les établissements de santé ne peuvent pas ou ne souhaitent pas héberger de données de santé disposent d'autres solutions, soumises au respect préalable de certaines conditions.

2) Quelles conditions pour le choix du tiers hébergeur ?

217. Si un établissement de santé fait le choix de confier ses données de santé à un tiers hébergeur, il devra alors respecter les règles du droit des marchés publics (a). L'établissement de santé doit également savoir qu'il lui sera possible de coopérer avec d'autres établissements dans ce cadre (b).

a) L'obligation d'un marché public

218. L'hébergement des données de santé constitue une prestation de service réalisée à titre onéreux soumise à la conclusion d'un contrat entre l'établissement ou le professionnel de santé et l'hébergeur de données. Dès lors, dans le cas d'un contrat conclu entre un prestataire hébergeur de données de santé et un établissement public de santé, la prestation tombe sous le coup des marchés publics[287]. Ainsi, en la matière, ce sont les dispositions de l'ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics[288] et du décret n° 2016-360 du 25 mars 2016 relatif aux marchés publics, qui vont trouver à s'appliquer[289]. Contrairement à certains auteurs[290], nous considérons que la prestation d'hébergement de données de santé doit être vue comme une prestation de service informatique. A ce titre, plusieurs solutions vont alors s'offrir aux établissements de santé. Soit le marché porte sur une somme en-deçà des seuils européens, fixés par le règlement n° 2015/2170 et 2015/2171 du 24 novembre 2015 de

[287] Articles 4 et 5 de l'ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics, *JORF* n°0169 du 24 juillet 2015, p. 12602. (Anciens articles 1 et 2 du Code des marchés publics, abrogé au 1er avril 2016.)
[288] Ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics, *JORF* n°0169 du 24 juillet 2015, p. 12602.
[289] Décret n° 2016-360 du 25 mars 2016 relatif aux marchés publics, *JORF* n°0074 du 27 mars 2016, texte n° 28.
[290] MARZOUG, Sanaa. « L'hébergement des données de santé à caractère personnel des établissements de santé : quelques repères juridiques ». *op. cit.*, p. 5.

la commission modifiant respectivement les directives 2014/24/UE et 2014/25/UE du 26 février 2014[291] ; dans ce cas, il est possible pour l'établissement de recourir à une procédure adaptée, décrite l'article 42, 3° de l'ordonnance de 2015 relative aux marchés publics et à l'article 27 du décret de 2016 relatif aux marchés publics. Au-delà de ce seuil, il sera nécessaire, pour l'établissement, de recourir à une procédure formalisée parmi les procédures suivantes : la procédure d'appel d'offres[292], la procédure concurrentielle avec négociation[293], la procédure négociée avec mise en concurrence préalable[294] et la procédure de dialogue compétitif[295].

219. A titre d'exemple, l'avis public d'appel à la concurrence lancé par l'ASIP santé au sujet de l'hébergement du DMP en 2009 avait respecté la procédure de l'appel d'offre européen, et avait fait l'objet d'une publication au Bulletin Officiel des Annonces des Marchés Publics (BOAMP)[296] et au Journal officiel de l'Union Européenne (JOUE)[297]. Une hypothèse existe toutefois dans laquelle un établissement public n'aura pas à se soumettre aux règles des marchés publics : celle d'une coopération avec d'autres établissements sur le sujet.

b) Les possibilités de coopération

220. L'hébergement de ses données de santé représente, pour un établissement de santé, un coût non négligeable. Une solution qui leur est ouverte est alors de coopérer sur ce sujet avec d'autres établissements afin de mutualiser les coûts et les risques. D'ailleurs, l'informatique est, depuis longtemps, une source de coopérations fructueuses entre les établissements de santé. Il nous faut envisager d'abord les formes que pourrait prendre une telle coopération, avant d'étudier ensuite les conséquences, en termes d'obligations juridiques notamment, pour ces coopérations. Les établissements publics de santé qui souhaiteraient coopérer dans le cadre de l'hébergement de leurs données de santé, auront le choix d'une coopération

[291] Ces seuils, applicables depuis le 1er janvier 2016, sont fixés à 209 000 euros hors taxes pour les marchés de fournitures courantes et services des établissements publics de santé.
[292] Procédure par laquelle l'établissement va choisir l'offre économiquement la plus avantageuse, sans négociation, sur la base de critères objectifs préalablement portés à la connaissance des candidats.
[293] Procédure par laquelle l'établissement va négocier les conditions du marché public avec un ou plusieurs opérateurs économiques.
[294] Procédure par laquelle l'établissement va négocier les conditions du marché public avec un ou plusieurs opérateurs économiques.
[295] Procédure dans laquelle l'établissement va être amené à dialoguer avec les candidats admis à participer à la procédure en vue de définir ou développer les solutions de nature à répondre à ses besoins et sur la base desquelles ces candidats sont invités à remettre une offre.
[296] Référence 09-219810, BOAMP n°198B, Annonce n° 573.
[297] *JOUE* 2009/S 198-28 5000.

conventionnelle ou d'une coopération organique. La solution de la coopération conventionnelle doit être rapidement mise de côté pour des raisons qui ont trait à la fois au principe de spécialité[298] et aux règles applicables en matière de marchés publics[299]. En effet, un contrat de coopération à titre onéreux, passé entre deux ou plusieurs établissements publics de santé, risquerait d'être requalifié en contrat de prestation[300], ce qui serait alors en opposition avec le principe de spécialité, auquel doivent obéir les établissements publics de santé. De même, une coopération conventionnelle à titre onéreux entre un établissement public de santé et un établissement privé de santé, au sein de laquelle l'établissement privé hébergerait les données de santé de l'établissement public, pourrait être requalifiée en contrat de prestation. Il serait alors reproché à l'établissement public de santé de ne pas s'être soumis aux règles du Code des marchés publics pour choisir son prestataire.

221. La coopération organique semble donc être la solution la plus adaptée. S'ouvre alors, pour les établissements publics de santé, une large palette de structures à sa disposition. Pour notre étude, nous choisirons de nous concentrer sur trois structures, qui nous semblent les plus pertinentes au vue de leur objet potentiel.

222. Les établissements vont pouvoir s'orienter d'abord vers le Groupement de Coopération Sanitaire (GCS) de moyens. Cet outil de coopération, particulièrement apprécié des établissements, présente l'avantage de pouvoir faire coopérer des établissements publics, privés et même des professionnels de santé. Selon le Code de la santé publique[301], le GCS de moyens a pour objet de faciliter, de développer ou d'améliorer l'activité de ses membres et peut être constitué pour « *organiser ou gérer des activités administratives, logistiques, techniques, médico-techniques, d'enseignement ou de recherche ; réaliser ou gérer des équipements d'intérêt commun ; il peut, le cas échéant, être titulaire à ce titre de l'autorisation d'installation d'équipements matériels lourds mentionnée à l'article L. 6122-1 ; permettre les interventions communes de professionnels médicaux et non médicaux exerçant dans les établissements ou centres de santé membres du groupement ainsi que des*

[298] *V. Supra.* n° 212 à 216.
[299] *V. Supra.* n° 218 à 219.
[300] DE LARD, Brigitte. « Hébergement de données et coopération », *Actualités JuriSanté*, n° 74, 2011, p. 7.
[301] Article L6133-1 du Code de la santé publique

professionnels libéraux membres du groupement ». La mutualisation de l'hébergement de données de santé semble donc être une activité pouvant être portée par un GCS de moyens.

223. Le Groupement d'Intérêt Public (GIP) est également une solution de coopération organique pour les établissements. Il s'agit d'une personne morale de droit public, régie par le chapitre II de la loi n°011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit[302]. Un GIP peut être constitué entre plusieurs personnes morales publiques ou entre des personnes morales publiques et des personnes morales privées. Il a pour objet d'exercer des activités d'intérêt général à but non lucratif, les membres du GIP mettant en commun les moyens nécessaires à leur exercice. Initialement conçu pour une durée limitée, la loi de 2011 est venue modifier cette particularité. Désormais, le GIP peut être à durée déterminée ou indéterminé. La durée doit être précisée au sein de la convention constitutive. Le GIP semble être un outil adapté à la coopération entre établissements de santé dans le but d'héberger des données de santé.

224. Enfin, le Groupement d'Intérêt Economique (GIE) est également une solution de coopération envisageable, celui-ci pouvant être créé entre des personnes morales de droit privé et public. L'objet principal d'un GIE est de faciliter ou de développer l'activité économique de ses membres. Son but n'est toutefois pas de réaliser des bénéfices pour lui-même. Dans le domaine sanitaire, le GIE a principalement pour objet d'acquérir ou de gérer des équipements d'intérêt commun (bloc opératoire, scanner), de mutualiser des moyens humains, locaux, matériels, ou de fournir aux établissements des prestations ou services auxiliaires à leurs activités respectives. Comme le GIP, le GIE a en théorie une durée de vie limitée, il faudra donc que les établissements qui choisissent cette forme de coopération y soient vigilants.

Une fois la structure de coopération créée, celle-ci devra bien évidemment se plier aux exigences du décret hébergeur et donc obtenir un agrément. A l'heure actuelle, huit agréments

[302] Loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit, *JORF* n° 0115 du 18 mai 2011, p. 8537.

ont été délivrés à six structures différentes de coopérations (un GIE, deux GCS, un GIP et deux SIH[303]).

B. Quelle place laissée au respect du droit des patients ?

225. L'intérêt principal des textes encadrant l'hébergement des données de santé par des tiers est, bien entendu, de protéger la sécurité et la confidentialité de ces données et donc, par la même occasion, les intérêts des patients concernés par ces données. Toutefois, une lecture précise des textes nous permet de constater que le droit des patients, et notamment son droit au consentement (1), n'est pas particulièrement protégé. Le rôle de médecin de l'hébergeur reste cependant un rempart contre les atteintes à la confidentialité des données (2).

1) La disparition progressive du consentement

226. Le consentement du patient était, initialement, un élément obligatoire en amont de tout hébergement auprès d'un tiers (a). Mais les différentes modifications de l'article L 1111-8 du Code de la santé publique ont transformé ce principe en exception (b), avant de le faire totalement disparaitre (c).

a) Le consentement, élément initialement essentiel à l'hébergement

227. En matière de soins, le consentement du patient est un élément fondamental. Le Code de déontologie médicale rappelle d'ailleurs ce principe[304], et la loi du 4 mars 2002 l'a érigé en droit essentiel du patient[305]. En matière de protection des données personnelles faisant l'objet d'un traitement automatisé, et plus particulièrement dans le cas des données de santé, la loi Informatique et Libertés a fait du consentement de la personne concernée par les données, une condition *sine qua non* du traitement. Nous avons toutefois pu constater que ce principe comporte de nombreuses exceptions, sur lesquelles nous ne reviendrons pas.[306]

---

[303] Les Syndicats Inter-Hospitalier sont des structures de coopérations qui ont été supprimées par la loi HPST. Les coopérations qui prenaient cette forme doivent désormais évoluer vers une autre forme juridique.
[304] Article R4127-36 du Code de la santé publique

[305] Article L. 1111-4 du Code de la santé publique.
[306] *V. Supra.* n° 230.

228. Quand il a introduit en 2002 la possibilité, pour un établissement ou un professionnel de santé, d'héberger les données de santé qu'il collecte auprès d'un tiers agréé, le législateur n'a pas oublié la notion de consentement du patient. En effet, l'article L. 1111-8 du Code de la santé publique prévoyait la nécessité d'obtenir, préalablement à l'externalisation de l'hébergement, le consentement exprès du patient. D'ailleurs, dans les premières versions de l'article, ce critère strict ne souffrait d'aucune exception[307]. On devine ici une réelle volonté de la part du législateur de s'assurer que le patient reste bien informé des conditions de conservation des données de santé le concernant. A ce titre, le législateur n'exigeait pas un consentement tacite de la part du patient mais bien un consentement exprès. Cela impliquait donc un véritable travail d'information et de recueil du consentement de la part de l'établissement ou du professionnel de santé. En pratique, le respect de cette obligation pouvait être assuré soit par l'hébergeur lui-même, soit par l'établissement ou le professionnel de santé qui choisissait de déposer ses données, par le biais d'un report contractuel de l'obligation. Cependant, ce principe a vite souffert d'exceptions, avant de totalement disparaître.

b) Le consentement : du principe à l'exception

229. La loi n°2007-127 du 30 janvier 2007[308], en son article 25 III, était venue introduire une exception à cette obligation stricte du consentement exprès, en ajoutant à l'article L. 1111-8 du Code de la santé publique la mention suivante : « *les professionnels et établissements de santé peuvent, par dérogation aux dispositions de la dernière phrase des deux premiers alinéas du présent article, utiliser leurs propres systèmes ou des systèmes appartenant à des hébergeurs agréés sans le consentement exprès de la personnes concernée, dès lors que l'accès détenu est limité au professionnel de santé ou à l'établissement de santé qui les a déposés, ainsi qu'à la personne concernée dans les conditions prévues par l'article L. 1111-7* ».

230. Le législateur avait ainsi, dans un premier temps, restreint l'obligation de consentement aux seuls cas dans lesquels les données collectées, seraient amenées à être partagées entre plusieurs établissements ou professionnels de santé. Cette disposition

---

[307] Ceci n'est plus le cas aujourd'hui, *V. Infra* n° 232.

[308] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le Code de la santé publique, *JORF* n°27 du 1 février 2007, p. 1937.

dérogatoire a constitué une véritable remise en question de l'importance accordée au consentement du patient puisque, dans les faits, elle est devenue la règle applicable. En effet, l'exception prévue par le législateur recouvrait la majorité des cas d'hébergements des données de santé. A titre d'exemple, le dossier médical d'un établissement public de santé, n'a pas pour vocation à être partagé à l'extérieur. Dès lors, on pouvait considérer que l'accès aux données de santé était bien limité à l'établissement de santé qui les avait déposées et le consentement des patients préalable à l'hébergement auprès d'un tiers n'était donc pas nécessaire.

Comme si cette disposition n'était pas suffisante, le législateur est venu, en 2011, amoindrir de nouveau la portée du consentement du patient dans ce contexte. En effet, une disposition de la loi Fourcade, modifiant la loi HPST[309], était venue préciser que les établissements de santé qui souhaitaient confier l'hébergement de leurs données de santé sur support papier à des tiers agréés, pouvaient se dispenser du consentement exprès préalable, si ces données avaient été collectées avant le 10 août 2011, date de la promulgation de la loi. Le législateur avait introduit ici une sorte de dispense générale de consentement, qui touchait en pratique des quantités extrêmement importantes de données personnelles de santé. Au final, « *la valeur du consentement de la personne à l'hébergement de ses données fait défaut, comme émoussée au fur et à mesure des textes* »[310].

231. Il nous semble que le législateur avait souhaité simplifier pour les établissements de santé et les professionnels, une procédure qui s'inscrivait déjà dans un environnement technique et juridique complexe. D'ailleurs, le fait que cette disposition soit apparue cinq ans après la disposition relative à l'hébergement agréé des donnée de santé, montrait bien que le législateur n'avait pas, dans un premier temps, mesuré totalement l'impact d'une telle exigence. Certains auteurs ont critiqué cette quasi-négation du consentement du patient, en contradiction avec les principes fondateurs de la loi Informatique et Libertés. Pourtant, l'évolution récente de l'article L. 1111-8 du Code de la santé publique a fait disparaitre le consentement du patient.

c) La disparition du consentement au profit de la non opposition

[309] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, *JORF* n° 0167 du 22 juillet 2009, p. 12184.
[310] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *PUN*, 2010, p. 299.

232. Le comité d'agrément des hébergeurs, dans son second rapport d'activité[311], publié en septembre 2014, s'était interrogé sur l'intérêt du recueil préalable du consentement du patient avant la mise en place d'un hébergement externalisé. Pour le comité, il était légitime de poser la question de la nécessite de « *solenniser l'accord du patient pour l'hébergement de ses données, alors que le législateur a mis en place au moyen de la procédure d'agrément des garanties fortes de sécurité et de confidentialité* »[312]. Il préconisait ainsi dans son rapport une évolution des textes sur ce point, le recueil du consentement du patient étant en pratique difficile à respecter. La loi de modernisation de notre système de santé a, dans son article 96, fait disparaitre de manière définitive cette exigence au profit d'une non opposition. Désormais, l'hébergement est réalisé « *après que la personne prise en charge en a été dûment informée et sauf opposition de sa part pour un motif légitime* ». Le législateur va donc ici assez loin car le patient, dont le consentement n'est plus recherché, ne pourra de fait s'opposer à l'hébergement externalisé de ses données qu'en avançant un motif légitime, non défini par le texte.

2) Le médecin de l'hébergeur, garant du respect de la confidentialité des données

233. Le décret hébergeur vient introduire une nouvelle fonction, celle du médecin de l'hébergeur. Selon l'article R. 1111-9 du Code de la santé publique, ce médecin est une des personnes « *en charge de l'activité d'hébergement* ». Cette notion reste toutefois assez floue et le législateur n'apporte aucun renseignement sur les missions qui lui seraient dévolues. D'ailleurs, dans son second rapport d'activité, le Comité d'agrément des hébergeurs préconise une intervention du législateur afin de définir clairement le rôle du médecin de l'hébergeur, mais également fournir un cadre réglementaire précis à l'accès aux données de santé hébergées par ce médecin[313].

234. « *Rouage important de la politique de confidentialité de l'hébergeur* »[314], il apparait clairement que le rôle principal du médecin de l'hébergeur consiste à s'assurer, d'une part, du respect de la confidentialité des données et, d'autre part, du droit des personnes concernées

---

[311] Rapport d'activité 2012-2013 du comité d'agrément des hébergeurs, disponible sur [http://esante.gouv.fr]. Consulté le 15 mai 2017.
[312] Rapport d'activité 2012-2013 du comité d'agrément des hébergeurs, disponible sur [http://esante.gouv.fr]. Consulté le 15 mai 2017, p. 20.
[313] *Id.*, p. 23.
[314] Livre blanc de l'association française des hébergeurs agréés de données de santé, 2014, p. 27.

par les données, qu'elle détiennent aux termes de la loi Informatique et Libertés. Selon Philippe BICLET, le Président du Comité d'agrément des hébergeurs, cette fonction a également été mise en place afin que « *le secret professionnel soit protégé lorsqu'une intervention humaine est nécessaire à l'occasion du traitement des données, ce qui est par exemple le cas, en cas d'incident informatique, ou à l'occasion de la restitution des données à un patient ou à ses ayants-droits* »[315]. Le Comité d'agrément des hébergeurs a également précisé les missions de ce médecin de l'hébergeur. Ainsi, dans son rapport d'activité 2006-2011[316], on apprend qu'il peut également être saisi afin de procéder à certaines vérifications de cohérence, dans l'hypothèse d'une suspicion de collision ou de doublon dans les dossiers médicaux. Selon l'association française des hébergeurs agréés des données de santé, ce médecin est également tenu d'insuffler une culture de la sécurité et de la protection des données au sein de l'entreprise.

235. Le médecin devra bien évidemment signer un contrat avec l'hébergeur afin d'encadrer son intervention. L'embauche à temps complet d'un médecin semble difficilement envisageable[317], et l'hébergeur optera plutôt pour un contrat du type prestation de service, de vacation ou encore de mise à disposition. Dans tous les cas, il est nécessaire de veiller à ce que le médecin conserve son indépendance déontologique vis-à-vis de l'hébergeur. Le Conseil National de l'Ordre des Médecins (CNOM) a élaboré un modèle de contrat type qu'il met à disposition sur son site Internet[318]. L'intérêt principal de ce modèle réside dans la précision qui est faite des missions dévolues au médecin de l'hébergeur. De même, son indépendance professionnelle est rappelée. Il est également prévu une clause afin d'éviter d'éventuels conflits d'intérêts. Ainsi, le médecin de l'hébergeur ne pourra être salarié ou exécuter des prestations de service pour le compte de personnes à l'origine des données de santé hébergées ou pour le compte des personnes concernées par ces données. Cette clause permet d'éviter, par exemple, qu'un praticien hospitalier ait accès à l'ensemble des données que son établissement fait héberger, de par son rôle de médecin hébergeur, accès qu'il n'aurait pas eu dans le cadre de son activité normale et en application des règles en matière de secret partagé. Enfin, il est prévu la communication du contrat au Conseil de l'ordre des médecins.

---

[315] BICLET, Philippe. « Hébergement et échange des données de santé », médecine et droit, 2010, pp. 159-160.
[316] Rapport d'activité 2006-2011 du comité d'agrément des hébergeurs, p. 19.
[317] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit.*, p. 297.
[318] Modèle disponible sur [https://www.conseil-national.medecin.fr]. Consulté le 4 mai 2017.

Le Comité d'Agrément des Hébergeurs, dans son premier rapport d'activité, a regretté l'absence dans ce contrat type d'obligation d'alerte auprès d'organismes externes, en cas de découverte d'un manquement à la confidentialité, ceci ayant pu constituer une garantie supplémentaire.

§2. La construction laborieuse du cadre relatif à la communication des données de santé

236. La communication des données de santé par voie électronique répond à des règles strictes, édictées par différents textes successifs. Cependant, ce cadre présente plusieurs lacunes, qui rendent son application difficile (A). Par ailleurs, certaines exigences posées par la réglementation applicable, semblent contestables (B).

A. La communication des données de santé : des prescriptions difficilement applicables en l'état

237. Les dispositions régissant les modalités de communication par voie électronique des données de santé restent muettes sur certains points pourtant essentiels (1). En outre, à l'heure actuelle, des référentiels nécessaires à la bonne application de ce cadre, ne sont toujours pas parus (2).

1) Des questions en suspens

238. L'article L. 1110-4-1 du Code de la santé publique, introduit par la loi de modernisation de notre système de santé, prévoit qu' : « *afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté*

du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés ».

239. Toutefois, le texte ne précise pas si ces dispositions s'appliquent seulement aux échanges entre professionnels de santé, ou également aux éventuels envois de documents médicaux entre professionnels de santé et patients. Or, il est nécessaire de se poser la question. En effet, les patients disposent d'un droit à la communication de leur dossier médical. Actuellement, cette communication se fait par le biais de copies du dossier papier ou d'une copie sur CD du dossier informatisé. Toutefois, la question s'est posée récemment de savoir s'il était possible de communiquer un dossier médical informatisé au patient par courrier électronique. Cette question a fait l'objet d'un avis de la Commission d'Accès aux Documents Administratifs (CADA) qui, selon nous, présente quelques limites.

240. En l'espèce, un patient avait demandé au Centre Hospitalier Universitaire (CHU) que certains éléments de son dossier médical lui soient communiqués et ce, par courrier électronique. Le Directeur Général du CHU lui avait répondu qu'il était disposé à lui communiquer ces éléments sous toute autre forme. Pour justifier sa réponse, le Directeur Général soulignait que la délibération CNIL n° 97-008 du 4 février 1997[319] préconisait que seules les messageries sécurisées et recourant au chiffrement des données puissent être utilisées pour transférer des données médicales nominatives. En conséquence, le Directeur Général de l'établissement, qui n'était pas assuré que la messagerie du patient était suffisamment sécurisée, avait estimé, dans une optique de protection de la sécurité et de la confidentialité des données, que la communication du dossier ne pouvait avoir lieu par ce biais. Le patient a donc saisi la CADA d'une demande d'avis. La Commission, dans un avis rendu le 25 juillet 2013[320], a pour sa part, considéré que cette délibération de la CNIL était rédigée dans des termes non impératifs et concernait les transferts de données médicales entre professionnels de santé. Elle ne pouvait donc pas être invoquée pour faire obstacle à la communication d'un dossier médical à un patient par courrier électronique. Elle a cependant estimé qu'il était nécessaire, pour l'établissement de santé, d'avertir le patient des risques que présente cette modalité de communication. De même, elle a considéré que l'établissement

[319] Délibération portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel n° 97-008 du 04 février 1997.
[320] Avis de la CADA n° 20131540 du 25 juillet 2013.

pouvait tout à fait chiffrer les données qu'il serait amené à communiquer par ce biais, si ses possibilités techniques le lui permettent.

241. Cet avis est, à notre sens, critiquable. En effet, nous ne comprenons pas ce qui justifierait de faire une différence entre données transmises aux professionnels de santé ou données transmises aux patients. Dans l'absolu, les données de santé doivent être protégées le plus strictement possible et en toutes circonstances. Dès lors, il nous parait difficile d'envisager un encadrement de la communication par voie informatique des données de santé qui serait différent selon la personne à qui les données sont transmises. Face aux risques existants en cas d'utilisation d'une messagerie non cryptée, nous estimons qu'un simple rappel aux patients des risques encourus n'est pas suffisant. Avant d'accorder une telle possibilité, il est donc nécessaire qu'une technologie suffisamment sécurisée et notamment les messageries cryptées se développent.

2) Des référentiels non parus

242. Jusqu'à l'adoption de la loi de modernisation de notre système de santé, c'est le décret du 15 mai 2007, dit décret "confidentialité"[321] qui imposait pour tout professionnel, établissement ou réseau de santé, le respect de référentiels définis par arrêté et pris après avis de la CNIL, dans l'hypothèse d'une conservation ou de la transmission par voie électronique de données de santé. De même, depuis les modifications apportées par la loi de modernisation de notre système de santé, l'article L. 1110-4-1 du Code de la santé publique, nouvellement créé, prévoit lui aussi la nécessité pour les professionnels de santé et établissements qui souhaiteraient échanger des données de santé par voie électronique, de respecter certains référentiels de sécurité, publiés par arrêté[322]. Cependant, à l'heure actuelle, aucun référentiel n'a été publié. Certains référentiels, à la portée plus générale, ont bien été adoptés par le législateur. Ainsi, le Référentiel Général de Sécurité (RGS) a été créé par l'article 9 de

---

[321] Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le Code de la santé publique (dispositions réglementaires), *JORF* n°113 du 16 mai 2007, p. 9362.

[322] L'article L. 1110-4-1 du Code de la santé publique prévoit : *« afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés.* »

l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives[323]. La version initiale du RGS (v.1.0) a été rendue officielle par arrêté du Premier Ministre en date du 6 mai 2010. Une version 2.0 a été publiée par arrêté du Premier Ministre du 13 juin 2014, applicable depuis le 1er juillet 2014. Selon l'Agence Nationale de Sécurité de Systèmes d'Information (ANSSI), ce référentiel permet, pour une autorité administrative, « *de garantir aux citoyens et aux autres administrations que le niveau de sécurité de ses systèmes d'information est bien adapté aux enjeux et aux risques et qu'il est harmonisé avec ceux de ses partenaires* ». Toutefois, il nous semble que le législateur, dans sa rédaction du décret confidentialité, entendait faire adopter des référentiels spécifiques aux échanges de données de santé. En effet, le texte précise bien qu'il doit s'agir de référentiels « *élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24* », à savoir l'ASIP santé. Le RGS, bien qu'étant une possibilité d'orientation pour les établissements publics, ne constitue donc pas le référentiel de sécurité tel que défini par le décret confidentialité.

243. L'ASIP santé, pour sa part, s'est attachée à rédiger un référentiel d'interopérabilité[324] des systèmes d'information en santé. Celui-ci est disponible sur son site Internet, au sein d'un espace de publication appelé Répertoire National des Référentiels (RNR). Au sein de ce répertoire, les établissements de santé peuvent consulter le Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS). Ce référentiel a pour ambition affichée de créer « *les conditions d'une interopérabilité reproductible et efficiente entre SI de santé, dans le respect des exigences de sécurité et de confidentialité des données personnelles de santé* ».[325]
Le CI-SIS spécifie les standards qu'il est préférable d'utiliser dans le cadre d'échanges et de partages de données de santé entre systèmes d'informations de santé. L'ASIP Santé propose ainsi tout un éventail de documentation à ce sujet, adapté aux spécificités de certaines activités. Toutefois, ces référentiels n'ont pas été publiés de manière officielle et, s'ils restent des documents de références pour les établissements et professionnels de santé, ils ne leur

[323] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, *JORF* n° 286 du 9 décembre 2005, p. 18986.
[324] L'interopérabilité des systèmes de dossiers informatisés est définie par la commission européenne comme « *la capacité de plusieurs systèmes de dossiers informatisés de santé d'échanger aussi bien des données exploitables par un ordinateur que des informations et des connaissances demandant une intervention humaine* ». Recommandation n° 2008/594/CE de la commission européenne du 2 juillet 2008 sur l'interopérabilité transfrontalière des systèmes de dossiers informatisés de santé, *JOUE* L 190 du 18 juillet 2008.
[325] Disponible sur [http://esante.gouv.fr]. Consulté le 2 mai 2017.

sont pas opposables juridiquement[326]. Même s'il est vrai que ces référentiels doivent être constitués par les acteurs compétents, à savoir l'ASIP Santé, en lien avec les partenaires industriels, il est nécessaire de donner une force juridique à ces documents, afin d'encadrer et de sécuriser les pratiques des établissements et des professionnels de santé.

B. L'utilisation systématique de la carte de professionnel de santé : une utopie abandonnée

244. L'application des règles relatives au partage des données ne pose pas réellement de problème quand il s'agit pour deux professionnels d'échanger oralement. L'exercice se complique dès lors que l'utilisation des TIC entre en jeu. En effet, il va être nécessaire de s'assurer que la personne, qui cherche à accéder à des données en a le droit. Le professionnel de santé va donc devoir s'identifier puis s'authentifier. Il s'agit ici de deux actions différentes : une première au cours de laquelle le professionnel va décliner son identité et une autre qui va permettre au professionnel de « prouver » qu'il est bien celui qu'il prétend être. Afin de réaliser ces deux actions, le législateur a prévu, dans un premier l'utilisation obligatoire et systématique de la Carte de Professionnel de santé (CPS)[327] ou d'un dispositif dit "équivalent"[328]. D'abord mise en place pour l'authentification des professionnels de santé dans le cadre de la transmission dématérialisée des feuilles de soin, son utilisation a donc été élargie[329] à toutes les transmissions de données de santé par voie électronique. Il s'agit, en

---

[326] Ces référentiels sont disponibles en ligne sur le site Internet de l'ASIP santé : [http://esante.gouv.fr].

[327] Article R. 1110-3 du Code de la santé publique : « *en cas d'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du Code de la sécurité sociale est obligatoire* ».

[328] L'article L. 1110-4 du Code de la santé publique, dans sa rédaction applicable jusqu'au 28 janvier 2016 prévoyait qu' « *afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés. Ce décret détermine les cas où l'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du Code de la sécurité sociale ou un dispositif équivalent agréé par l'organisme chargé d'émettre la carte de professionnel de santé est obligatoire. La carte de professionnel de santé et les dispositifs équivalents agréés sont utilisés par les professionnels de santé, les établissements de santé, les réseaux de santé ou tout autre organisme participant à la prévention et aux soins* ».

[329] Article L. 161-33 al.3 du Code de la sécurité sociale : « *dans le cas de transmission électronique par les professionnels, organismes ou établissements dispensant des actes ou prestations remboursables par l'assurance maladie, l'identification de l'émetteur, son authentification et la sécurisation des échanges sont assurées par une carte électronique individuelle, appelée carte de professionnel de santé. Le contenu, les modalités de délivrance et d'utilisation de cette carte sont fixés par décret en Conseil d'Etat après avis de la Commission nationale informatique et libertés* »

pratique, d'une carte contenant les données d'identification de son porteur ainsi que ses conditions d'exercice, et lui permettant ainsi de s'authentifier et de signer électroniquement les différentes opérations qu'il effectue (par exemple la rédaction d'un compte rendu d'hospitalisation). D'abord gérée par le GIP-CPS, cette carte est actuellement distribuée par l'Agence des Systèmes d'Information Partagées en santé (ASIP santé)[330].Ce dispositif permet indéniablement d'assurer la sécurité nécessaire aux données de santé. Cependant, plusieurs bémols peuvent être apportés à son utilisation obligatoire.

245. D'abord d'un point de vue pratique, selon les chiffres de l'ASIP Santé, sur les 1 178 271 cartes actives de la famille des cartes de professionnels (CPS et autres cartes équivalents diffusées par l'ASIP santé), seulement 325 789 ont été distribuées au sein des établissements de santé[331]. Cette différence s'explique notamment grâce à l'historique de cette carte. En effet, au vu de son objet initial, cette carte est peu connue du monde hospitalier et son développement au sein des établissements de santé est aujourd'hui difficile, pour des raisons à la fois techniques, mais également d'habitude. En établissement de santé, cette obligation d'utiliser de manière systématique une carte de professionnel de santé, ou dispositif équivalent, est donc compliqué. Par ailleurs, en instaurant l'utilisation obligatoire de la CPS pour la transmission de données de santé par voie électronique par des professionnels de santé, le décret confidentialité a, en réalité, élargi le champ d'application initial de l'article L. 161-33 du Code de la sécurité sociale qui ne prévoyait l'utilisation de cette carte que dans les cas de la transmission électronique des feuilles de soins dématérialisées à l'assurance maladie.

246. Le décret confidentialité, acte réglementaire, a donc élargi le champ d'utilisation de la CPS, initialement prévu par la loi[332]. Or, un décret ne doit pas venir modifier le champ d'application de la loi, mais simplement en définir les modalités d'application. Nous sommes donc ici face à un décret qui était en réalité contraire à la loi. Ceci relève, comme le souligne à juste titre Caroline ZORN-MACREZ, d'une pratique *contra legem*[333]. En cela, les obligations du décret étaient donc inapplicables.

---

[330]Arrêté du 12 octobre 2009 portant approbation de la modification de la convention constitutive du Groupement d'Intérêt Public « Carte de Professionnel de Santé », *JORF* du 17 octobre 2009. A compter de novembre 2009, le GIP-CPS a intégré l'ASIP santé.
[331] Chiffres disponibles sur [http://esante.gouv.fr], consultés le 1er mars 2017.
[332] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit*., p. 269.
[333] *Id*., p. 269 : « *cette situation illustre parfaitement les débordements d'une pratique réglementaire ultra legem, laquelle dissimule une pratique véritablement contra legem* ».

247. Ces difficultés ont été réglées par l'article 96 de la loi de modernisation de notre système de santé, qui supprime purement et simplement l'exigence de l'utilisation de la CPS ou d'un dispositif équivalent pour la transmission de données de santé par voie électronique. Cette mention a donc disparu de l'article L. 1110-4 du Code de la santé publique, qui prévoit désormais qu'« *afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés* ».

248. Or, à ce jour, et comme nous avons pu le constater précédemment, ces référentiels n'ont toujours pas été publiés et les dispositions du décret confidentialité, applicables précédemment et codifiés aux article R. 1110-1 à R. 1110-4 du Code de la santé publique, ont été remplacés par des dispositions intégrées par le décret du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel[334]. L'encadrement de la transmission par voie informatique des données de santé demeure donc aujourd'hui inabouti.

[334] Décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel, *JORF* n°0169 du 22 juillet 2016, texte n° 21.

Conclusion de la section

249. Bien que présentant certaines lacunes, le décret hébergeur, et l'ensemble de l'encadrement et des procédures relatives à l'hébergement des données de santé auprès d'un tiers, permettent d'assurer la sécurité nécessaire à ces données. Par ailleurs, la récente rénovation du cadre de l'hébergement des données de santé permet de simplifier les démarches préalables qui s'imposent aux hébergeurs, leur apportant plus de souplesse et de réactivité.

250. En ce qui concerne la communication des données de santé en revanche, bien que le législateur ait tenté d'encadrer strictement la communication par voie électronique des données de santé, force est de constater qu'il a malheureusement échoué. Car même si l'idée initiale était très intéressante, l'application n'a pas suivi. De plus, l'obligation d'utiliser de manière systématique la carte de professionnel de santé a été abandonnée récemment par le législateur mais aucune alternative n'a été proposée.

Conclusion du chapitre

251. Les données de santé, dont la collecte, la conservation et la communication sont essentielles à la bonne prise en charge des patients, se doivent d'être suffisamment protégées. Leur vie, de l'archivage à la destruction, en passant par la communication, est en théorie strictement encadrée par un ensemble de règles juridiques épars. Les données de santé produites par les établissements publics de santé ont le statut d'archives publiques. De ce fait, le Code du patrimoine régit leur conservation ainsi que leur destruction. Mais la particularité de ces données, font qu'elles sont également soumises à d'autres règles, plus précises, notamment en matière de secret médical. Et c'est là qu'apparaissent les premières lacunes des textes, qui vont parfois entrer en contradiction. L'introduction des TIC dans la pratique médicale implique une difficulté supplémentaire puisqu'il faut désormais conserver et archiver des données de santé informatisées.

252. Malheureusement, le législateur, en dépit de ses efforts, n'a pas réellement su faire face à l'arrivée massive des TIC et à l'informatisation croissante des données de santé. Bien que leur hébergement auprès d'un tiers soit correctement encadré, le décret "confidentialité", censé réglementer la communication électronique des données, a failli à sa mission, et est resté inapplicable. Aujourd'hui, le législateur, au travers de la loi de modernisation de notre système de santé et de ses textes d'application, a supprimé les dispositions du décret "confidentialité". Cependant, à l'heure actuelle, aucune disposition ne les remplace et la communication des données de santé est soumise au respect de référentiels, qui n'ont toujours pas été, à ce jour, publiés.

Conclusion du titre

253. L'étude des modalités juridiques de l'informatisation des données de santé à l'hôpital nous a conduit à constater que le cadre juridique applicable se révèle complexe à appréhender. Règles de droit commun, règles spécifiques et exceptions aux règles se superposent et ce cadre peut parfois devenir illisible. Il faut dire que le législateur a la lourde tâche de protéger ces données particulièrement sensibles, tout en permettant aux établissements et aux professionnels de santé de mener à bien leurs missions. Un juste équilibre doit donc être trouvé. A l'heure actuelle, l'encadrement juridique de la naissance, la communication, la conservation et la destruction des données de santé informatisées fait l'objet de textes épars. Certains d'entre eux ont montré leurs limites et le législateur s'emploie à moderniser un cadre parfois trop rigide.

L'informatisation des données de santé n'est qu'une partie du rôle joué par les TIC dans la pratique médicale et leur utilisation dans la prise en charge du patient a pris une place importante. Il nous apparait alors nécessaire de s'arrêter sur le cadre juridique qui permet aujourd'hui une telle utilisation.

TITRE 2

TIC ET PRISE EN CHARGE MEDICALE : UN CADRE EN EVOLUTION

« *Favoriser la coordination des professionnels de santé et leur coopération étroite pour améliorer la prise en charge des malades, tel est le but de l'utilisation des TIC […]* »[335]

254. L'utilisation des TIC dans la pratique médicale ne se limite pas à l'informatisation des données de santé. Au contraire, celle-ci n'est qu'une étape permettant le développement de la dématérialisation de la prise en charge du patient et, en la matière, les possibilités techniques sont nombreuses. Ces dernières années ont vu se développer de nombreuses initiatives en ce sens. Cependant, une fois encore, les possibilités techniques doivent être mises au regard de l'intérêt du patient et la protection de ses droits et, un juste équilibre doit être trouvé.

255. Dans le but d'améliorer la coordination et la qualité des soins, et, dans la suite logique de l'informatisation des données de santé, les dossiers médicaux dématérialisés et partagés se sont développés. Si la plupart d'entre eux relèvent du régime de droit commun, le législateur a créé un « *régime spécifique exorbitant de droit commun* »[336] au Dossier Médical Partagé (DMP). Le développement de ce type de dossier représente une première étape dans la dématérialisation de la prise en charge du patient (Chapitre premier) sur laquelle il nous faut nous attarder. Mais les TIC permettent également d'envisager une prise en charge à distance des patients, bousculant ainsi les codes et les règles en place depuis de nombreuses années en la matière. Une étude du cadre juridique naissant de cette pratique nous apparait alors nécessaire (chapitre second).

---

[335] FIESCHI, Marius. « Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins », rapport au ministre de la santé de la famille et des personnes handicapées, janvier 2003, p. 8.
[336] ZORN-MACREZ. Caroline. « Données de santé et secret partagé », *PUN*, p. 305.

Chapitre 1

La dématérialisation des dossiers médicaux : l'exemple du DMP

256. Depuis plusieurs années maintenant, les rapports officiels se multiplient au sujet de l'utilisation des TIC dans le domaine de la santé, et plus spécifiquement dans le cadre de la mise en place de dossiers informatisés. Le but ultime est, bien entendu, la création d'un dossier informatisé partagé, un outil permettant de favoriser une meilleure coordination des professionnels, une amélioration de la qualité de la prise en charge et donc un meilleur état de santé global.

257. Les établissements de santé ont déjà, depuis plusieurs dizaines d'années, commencé l'informatisation de leur dossier médical. Celle-ci se fait de manière progressive et les établissements de santé ne sont pas tous, à l'heure actuelle, au même stade de développement. L'informatisation complète d'un dossier médical demande en effet du temps mais également des moyens à la fois financiers et humains. L'évolution technologique doit par ailleurs être accompagnée par une bonne gestion managériale de la conduite du changement.

258. Il apparait évident que les enjeux de l'informatisation du dossier médical sont importants (amélioration de la prise en charge du patient, meilleure coordination, outil plus facile d'accès, …) et ceux-ci dépassent les portes de l'hôpital. Le recueil, la conservation et le partage de données issues du soin à un niveau régional voire national font partie des préoccupations des pouvoirs publics depuis plus de dix ans. Ainsi, face aux succès de certains de nos voisins européens, et décidé à mettre en place un dossier partagé unique, le législateur est venu créer, en 2004 le Dossier Médical Partagé (DMP) (Section I). Depuis, ce dossier et surtout son encadrement juridique, n'ont cessé d'évoluer pour tenter de faire face aux échecs et aux critiques que le projet subi (Section II).

Section 1. Le DMP, un Dossier médical électronique institutionnel

259. Alors que les projets d'informatisation des dossiers médicaux se développent au sein des établissements de santé et ce de façon plutôt disparate, chaque établissement étant libre de choisir comment il va organiser du point de vue pratique et technique l'informatisation de son dossier médical, le législateur a fait le pari en 2004, de lancer un dossier informatisé, partagé entre tous les professionnels de santé amenés à prendre en charge un même patient. L'originalité du projet réside dans le fait que ce dossier peut également être consulté directement par le patient.

260. Toutefois, perdu dans la "masse" de l'ensemble des dossiers médicaux électroniques qui se développent, il est parfois difficile d'envisager quelle est la place du DMP (Paragraphe 1). D'ailleurs, cela n'est pas étranger au fait que depuis sa création, son cadre juridique évolue de manière hésitante (Paragraphe 2).

§1. La place incertaine du DMP dans le champ des dossiers médicaux

261. DME, DMI, DMP, DP. Les acronymes sont aujourd'hui nombreux et il devient difficile de se retrouver dans le champ des différentes acceptions du dossier médical. Et il est tout autant difficile de réussir à délimiter la place et le rôle dédiés au DMP dans cet ensemble disparate.

Pour réussir cet exercice, il est nécessaire de s'essayer, dans un premier temps, à délimiter les contours et le cadre juridique qui serait applicable aux dossiers médicaux électroniques, terme finalement le plus général et le plus englobant qui réunit l'ensemble des différents dossiers informatisés (A). Cet exercice terminé, il nous sera nécessaire de tenter d'articuler les différents dossiers entre eux afin de chercher à savoir dans quelle mesure ils se complètent et/ou sont redondants (B). Cela aura pour but principal, bien sûr, de chercher à savoir où se situe le DMP dans le paysage des dossiers médicaux.

A. Tentative de délimitation du cadre juridique des DME

262. Terme couramment utilisé, notamment par les professionnels des systèmes d'information hospitaliers, le Dossier Médical Electronique (DME) n'est pourtant pas juridiquement défini de manière claire. Or, il est facile de se perdre dans les méandres des dénominations diverses qui existent actuellement pour désigner le dossier médical. Ainsi, pour nous éclairer à ce sujet, il est nécessaire de tenter de délimiter les contours du DME (2) à la lumière des différentes formes que peut prendre le dossier médical (1)

1) Le dossier médical : un dossier aux formes multiples.

263. Bien que le dossier médical soit un outil désormais solidement ancré dans les pratiques des professionnels de santé, celui-ci ne dispose pas de réelle définition juridique. En effet, il n'est finalement défini que par le biais de son contenu ou de ses modes d'accès et de communication[337]. Or, il existe, à l'heure actuelle un nombre important de dossiers différents qui contiennent des données médicales de patients et qui sont utilisés pour leur suivi. Pour reprendre les propos de Philippe BICLET, *« derrière le terme générique de "dossier médical" se cachent des réalités bien différentes »*[338].

264. Dossier de suivi médical, dossier hospitalier, dossier patient, dossier médical informatisé, dossier médical personnel, dossier pharmaceutique, dossier de réseau,... les dénominations sont aujourd'hui nombreuses et il est parfois difficile de clairement identifier de quel outil il s'agit. Or, pour mieux appréhender le DME et le DMP, il nous semble important de délimiter d'abord les contours de ces différents dossiers. Pour ce faire, nous faisons le choix de concentrer nos travaux sur les seuls dossiers ayant un encadrement juridique précis. En effet, comme nous le verrons, plusieurs dénominations regroupent en réalité la même chose.

265. D'un point de vue strictement juridique, quatre types de dossiers existent réellement. Le plus connu, ou tout du moins, le mieux identifié en pratique est le dossier médical dont le

---

[337] GIOCANTI, Dominique. « Les différentes acceptions des termes "dossier médical" et, dans ce contexte, situation du dossier hospitalier », *RGDM*, n° 37, 2010, p. 164.
[338] BICLET, Philippe. « Le dossier médical dans tous ses états », *Médecine et droit*, 2006, p. 174.

contenu est défini à l'article R. 1112-2 du Code de la santé publique[339] et obligatoirement présent dans les établissements de santé publics ou privés. Ce dossier est couramment appelé dossier hospitalier[340]. En réalité, il n'existe pas de texte qui le définisse juridiquement. Toutefois, par le jeu des différents articles, définissant à la fois son contenu *a minima* (article R. 1112-2 du Code de la santé publique), ou les moyens de sa communication au patient (article L. 1111-7 du Code de la santé publique), il nous est possible d'en dresser les contours. Il apparait ainsi que ce dossier a été conçu par le législateur pour être le plus large possible et contenir l'ensemble des informations médicales d'un patient qui ont pu être collectées à l'occasion de son séjour en établissement de santé. D'ailleurs, les autres dossiers de professionnels se doivent d'être regroupés en son sein (c'est le cas par exemple du dossier d'anesthésie ou encore du dossier de soins infirmiers). A noter que l'article R. 1112-2 prévoit que le contenu énoncé est un contenu *a minima*. Ainsi, les établissements restent libres d'ajouter d'autres éléments, typiques de leur organisation interne par exemple, pour compléter ce dossier. Cela explique la diversité actuelle qui existe en matière d'organisation des dossiers médicaux.

266. L'article 45 du Code de déontologie médicale, codifié à l'article R. 4127-45 du Code de la santé publique vient, pour sa part, imposer à chaque médecin la tenue d'une "fiche d'observation" pour chaque patient. Celle-ci est strictement personnelle au médecin et doit être rédigée, indépendamment du « *dossier de suivi médical prévu par la loi* ». Il s'agit, en réalité, d'un dossier de suivi qui avait été instauré par la Convention Nationale des médecins, suite à la loi du 18 janvier 1994[341]. Toutefois à l'heure actuelle, ceci n'est plus une obligation[342]. Aucun formalisme n'est prévu par la loi concernant ces notes et, il n'est pas rare, encore aujourd'hui, que celles-ci soient tenues par les médecins sur de simples fiches cartonnées, sans réelle organisation. Comme le souligne, à juste titre, le Professeur Marius FIESCHI dans son rapport[343], ce type de dossier médical prend plutôt la forme d'un dossier

---

[339] Article R. 1112-2 du Code de la santé publique : « *un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé* ».

[340] *V.* en ce sens GIOCANTI, Dominique. « Les différentes acceptions des termes « dossier médical » et, dans ce contexte, situation du dossier hospitalier », *op. cit.* ; VEILLEROT Guy. « Le dossier hospitalier », *RGDM*, n°37 2010, pp. 177-183.

[341] Loi n° 94-43 du 18 janvier 1994 relative à la santé publique et à la protection sociale, JORF n°15 du 19 janvier 1994, p. 960.

[342] BICLET, Philippe. « Le dossier médical dans tous ses états », *op. cit*., p. 174.

[343] FIESCHI, Marius. « Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins », Rapport au ministre de la santé de la famille et des personnes handicapées, *op. cit.*

d'archives, et ne correspond pas à un dossier partagé qui serait un outil de coordination pour les professionnels de santé.

Toutefois, ces dernières années, le législateur, dans la suite des préconisations du rapport FIESCHI notamment, qui prônait la mise en place d'un dossier patient partagé, est venu créer deux dossiers informatisés et partagés.

267. Le premier, et celui qui, à l'heure actuelle, a rencontré le plus franc succès, est le dossier pharmaceutique (ou DP), introduit au Code de la sécurité sociale par la loi du 30 janvier 2007[344]. Il s'agit d'un dossier destiné exclusivement aux pharmaciens, et qui permet, par le biais de la carte vitale du patient, de consulter l'ensemble des médicaments délivrés au cours des quatre derniers mois. Initialement conçu comme un outil au service du DMP, afin d'alimenter le volet médicaments de celui-ci, le DP a vécu une première phase d'expérimentation entre 2007 et décembre 2008, phase développée à l'initiative du Conseil National de l'Ordre des Pharmaciens. Le décret n° 2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique[345] a généralisé ce processus, l'ensemble des pharmacies d'officines étant appelées à se doter de l'outil. Puis, la loi HPST[346] a introduit l'article L. 1111-23 au Code de la santé publique, qui prévoit l'ouverture, pour chaque bénéficiaire de l'assurance maladie, et avec son consentement, d'un dossier pharmaceutique, dont le but affiché est de favoriser la coordination, la qualité, la continuité des soins et la sécurité de la dispensation des médicaments[347]. Cet article prévoit également que la mise en œuvre du DP est assurée par le Conseil National de l'Ordre des pharmaciens. En pratique, seul un pharmacien d'office ou

---

[344] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le Code de la santé publique, *JORF* n°27 du 1 février 2007, p. 1937.

[345] Décret n° 2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique *JORF* n°0293 du 17 décembre 2008, p. 19237.

[346] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, *JORF* n°0167 du 22 juillet 2009, p. 12184.

[347] Article L. 1111-23 du Code de la santé publique : « *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, il est créé, pour chaque bénéficiaire de l'assurance maladie, avec son consentement, un dossier pharmaceutique. Sauf opposition du patient quant à l'accès du pharmacien à son dossier pharmaceutique et à l'alimentation de celui-ci, tout pharmacien d'officine est tenu d'alimenter le dossier pharmaceutique à l'occasion de la dispensation. Dans les mêmes conditions, les pharmaciens exerçant dans une pharmacie à usage intérieur peuvent consulter et alimenter ce dossier. Les informations de ce dossier utiles à la coordination des soins sont reportées dans le dossier médical personnel dans les conditions prévues à l'article L. 1111-15. La mise en œuvre du dossier pharmaceutique est assurée par le Conseil national de l'ordre des pharmaciens mentionné à l'article L. 4231-2. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et du Conseil national de l'ordre des pharmaciens, fixe les conditions d'application du présent article* ».

exerçant au sein des pharmacies à usage interne (PUI) peut consulter et alimenter ce dossier. Toutefois, il est prévu, à terme, que le DP soit intégré au DMP, tout du moins en partie, et soit donc, de ce fait, consultable par les autres professionnels de santé.

268. Enfin, le dossier médical partagé (DMP), qui fait l'objet d'une étude poussée tout au long de notre chapitre, est le projet de dossier médical partagé le plus complet, tout du moins en théorie, reflet de la volonté du législateur d'instaurer un dossier partagé par tous les professionnels de santé intervenant dans la prise en charge d'un patient.

Il est utile de signaler que des dispositifs "alternatifs" au dossier médical existent également. Citons plus particulièrement en ce sens le carnet de santé, créé par les articles R 162-1 à R 162-1-6 du Code de sécurité sociale qui, quant à lui, visait plutôt à permettre une continuité et une coordination des soins plus qu'un archivage des informations médicales.

2) Délimitation des contours du DME

Couramment, les termes Dossier Médical Electronique (DME) et de Dossier Médical Informatisé (DMI) sont utilisés de manière indifférente. Nous choisirons ici de suivre ce courant et de ne pas distinguer l'un et l'autre.

269. Le dossier médical électronique (DME) n'est pas réellement un dossier à part entière, clairement défini par les textes. Il s'agit plutôt d'un concept, d'une terminologie générale, employée pour désigner finalement l'ensemble des dossiers patients conservés sur support informatique. Selon Bruno ROUSSEL, le DME « *est le mot utilisé par les professionnels de l'informatique médicale pour désigner les dossiers patients informatisés dans le milieu hospitalier. Par extension, le DME désigne les systèmes informatiques permettant de déployer ces dossiers patients électroniques* »[348]. Face à cette observation, il est nécessaire de se demander si les DME seraient des outils réservés au milieu hospitalier comme l'affirme l'auteur. Nous pensons au contraire qu'il faut plutôt le considérer de manière globale et intégrer dans cette notion l'ensemble des dossiers informatisés, peu importe que leur utilisateur soit un centre hospitalier, un professionnel de santé libéral ou le patient lui-même

[348] ROUSSEL, Bruno. « Informatisation des dossiers médicaux en milieu hospitalier : intégrité et opposabilité des données numériques », *Communication Commerce Electronique*, 2009, étude 15, p. 15.

dans le cadre du DMP. Le DME serait alors le terme général pour désigner tous les dossiers médicaux se présentant sous une forme électronique, et se déploierait alors en différentes sous catégories.

270. Toutefois, comme le souligne à juste titre Bruno ROUSSEL, « *il semble légitime de replacer l'outil technique "DME" dans le contexte juridique du DMP* »[349]. Autrement dit, le DME n'est qu'un outil, un support technique, et le DMP en serait sa déclinaison concrète, ayant une réelle existence juridique. En l'absence d'une définition strictement juridique du DME, il est intéressant de se tourner vers les différents rapports qui ont été produits ces dernières années, au sujet de l'informatisation des données de santé et des dossiers médicaux et ce, afin de tenter d'en définir les contours.

271. Dans le rapport du Professeur Marius FIESCHI[350], le terme de DME n'apparait à aucun moment. L'auteur préfère utiliser le terme de dossier patient partagé, étant entendu que ce dossier, simple projet à l'époque de la rédaction du rapport, est forcément un dossier informatisé.

Dans son rapport d'information de 2008[351] consacré au dossier médical personnel, le député Jean-Pierre DOOR considère le DME comme étant un dossier médical personnel et partagé. Il n'utilise toutefois que très peu de fois ce terme et ne prend donc pas la peine de le définir. D'ailleurs, il utilise indifféremment les termes DME, DMP, dossier patient électronique ou encore de dossier médical informatisé. Pour le député, le DMP est un DME parmi d'autres.

Michel GAGNEUX, dans son rapport portant sur le dossier patient virtuel et partagé, rédigé dans le cadre de la mission de relance du projet de DMP[352], consacre une section à la définition des différents concepts existant en la matière. Ceux-ci restent cependant assez flous, même pour l'auteur. Le terme de DME n'est que peu utilisé dans ce rapport, puisque l'auteur lui préfère l'expression de "Dossier médical électronique partagé" (parfois remplacé

---

[349] *Ibid.*
[350] FIESCHI, Marius. « Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins », *op. cit*.
[351] Rapport d'information déposé par la commission des affaires culturelles, familiales et sociales sur le dossier médical personnel, 29 janvier 2008.
[352] GAGNEUX, Michel. COMBLE, Pierre-Henri. De KERGOMMEAUX, Loïc. « Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé. » Recommandations à la ministre de la santé, de la jeunesse, des sports et de la vie associative. Avril 2008.

par "dossier électronique partagé"). Ainsi, nous comprenons que le dossier électronique tel que l'auteur l'envisage est forcément partagé. D'ailleurs, au sein d'un même paragraphe, il utilise indifféremment les termes de dossier médical électronique, de dossier partagé et de DMP et ce, pour désigner un seul et même outil. Cela révèle selon nous le flou qui entoure toutes ces nouvelles notions qui se développement autour du dossier médical. L'auteur tout de même de donner une définition du DME, précisant que celui-ci se présente « *non comme un produit fini mais comme une dynamique de construction que l'évolution des usages et des technologies façonnera* »[353]. Il est intéressant de relever que Michel GAGNEUX différencie de manière très claire le DMP de l'ensemble des dossiers partagés. Le DMP serait ainsi, pour reprendre son expression, une vue particulière du dossier partagé[354] : tout dossier partagé n'est pas forcément personnel[355] et donc accessible aux patients. Finalement, le rapport introduit un concept parallèle à celui de DME : le dossier virtuel, qui se définirait comme « *le dossier patient unique que les technologies de l'information permettent de présenter aux utilisateurs, professionnels de santé ou patients, sous une forme adaptée à leur contexte d'usage, à partir de multiples dossiers physiquement distincts et répartis* »[356]. Une sorte de dossier "caméléon" qui s'adapterait aux besoins d'information de chacun de ses utilisateurs.

Face à ce flou de définitions, de notions et d'expressions, nous prenons le parti de tenter une définition du DME. Celle-ci se doit, selon nous de rester simple et la plus large possible.

272. Finalement, les dossiers médicaux électroniques regroupent toutes sortes de dossier médical, à partir du moment où il sera informatisé. Il pourra éventuellement être partagé, entre professionnels de santé, il pourra être accessible au patient, comme dans le cas du DMP ou être simplement le dossier hospitalier tel que défini à l'article R. 1112-2 du Code de la santé publique, mais se présentant sous une forme informatisée. Finalement, la définition de Bruno ROUSSEL reste selon nous, la plus proche et la plus adaptée de la réalité actuelle.

---

[353] *Id.*, p. 28.
[354] *Id.*, p. 30.
[355] Rappelons qu'à la date à laquelle ce rapport a été publié, le DMP était l'acronyme de "Dossier Médical Personnel". Ce n'est que depuis la publication de la loi de modernisation de notre système de santé que le DMP est devenue "Dossier Médical Partagé".
[356] GAGNEUX, Michel. COMBLE, Pierre-Henri. De KERGOMMEAUX, Loïc. « Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé. », *op. cit.*, p. 31.

Cet exercice de définition terminé, il nous est nécessaire de réfléchir sur la mise en œuvre, l'intérêt et l'articulation de l'ensemble de ces dossiers entre eux.

B. DMP, DME et autres dossiers médicaux : une articulation indispensable

273. Le DMP était, à l'époque de sa création, un projet fondamentalement novateur dans le cadre des politiques de santé (1). Ce dossier, atypique à plusieurs points de vue, doit aujourd'hui s'articuler avec les autres dossiers médicaux qui peuvent exister (2).

1) Le DMP, un projet novateur

Bien que l'idée d'un DMP ne soit pas nouvelle, le projet dans son ensemble est, dans les faits, original et innovant, il constitue un véritable « *projet de société qui bouleverse les habitudes et les mentalités* »[357].

274. Le projet est original car il s'agit du premier dossier médical dont le patient est titulaire[358]. En effet, jusque-là, bien qu'ils détiennent un droit d'accès à leur dossier médical[359], les patients n'avaient pas un dossier qui leur était directement accessible d'une part, et clairement identifié comme leur appartenant d'autre part. Car c'est bien là l'originalité du DMP : le législateur affiche, dès le départ, son ambition de faire du DMP le dossier du patient. Dès les travaux parlementaires de la loi du 13 août 2004[360], il est rappelé que *« le choix du gouvernement d'utiliser l'expression " dossier médical personnel" plutôt que "dossier médical partagé" vise à souligner qu'il s'agit avant tout du dossier patient »*[361]. Le nom a peut-être aujourd'hui changé, le DMP étant redevenu "partagé" avec la loi de modernisation de notre système de santé[362], le principe affiché reste pour autant le même. Le patient bénéficie d'un véritable contrôle sur l'ensemble de son dossier : il contrôle son ouverture, qui est conditionnée à son consentement exprès et éclairé, il contrôle également sa

---

[357] MONNIER, Anne. « Le dossier médical personnel : histoire, encadrement juridique et perspectives », *RDSS*, 2009, p. 625.
[358] L'article R. 1111-26 du Code de la santé publique dispose : « *Une fois son dossier créé, le bénéficiaire de l'assurance maladie en devient le titulaire* ».
[359] Article L. 1111-7 du Code de la santé publique.
[360] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, *JORF* n°0190 du 17 août 2004, p. 14598.
[361] VASSELLE, Alain. « Projet de loi relatif à l'assurance maladie, rapport fait au nom de la commission des affaires sociales », *Sénat*, n° 424, tome I, 2004.
[362] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte n° 1.

clôture, et il décide, dans une certaine mesure, des professionnels qui pourront y avoir accès ainsi que les informations que ces professionnels pourront consulter. Enfin, et c'est là un des dispositifs les plus originaux, et parfois controversé du DMP, le patient bénéficie d'un droit de masquage sur son dossier.

275. En effet, cette possibilité a été introduite par la loi de financement de la sécurité sociale du 19 décembre 2007 pour 2008[363] qui prévoyait que selon certaines modalités, qui devaient être fixées par un décret pris en Conseil d'Etat, les informations contenues dans le DMP pouvaient être rendues inaccessibles par le titulaire du DMP ou son représentant légal. Quand l'ensemble des dispositions relatives au DMP ont été introduites dans le Code de la santé publique par la loi HPST, cette mesure est restée. Ce décret n'a jamais été adopté et cette possibilité est restée longtemps inactive, les précisions règlementaires et pratiques nécessaires à sa mise en œuvre n'ayant pas été adoptées. Puis, avec l'ultime relance du DMP, amorcée par la loi de modernisation de notre système de santé, cette possibilité a finalement été confirmée. Le décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé[364] est venu insérer, au sein du Code de la santé publique, l'article R. 1111-38 qui prévoit que : « *le titulaire peut décider que des informations le concernant contenues dans son dossier médical partagé ne soient pas accessibles aux professionnels de santé autorisés à accéder à son dossier* ».

276. Le droit de masquage est donc définitivement consacré. Le support du DMP peut, lui également, être considéré comme innovant. En effet, même si au moment de la création du DMP, l'information des systèmes d'information hospitaliers avait commencé depuis plusieurs années, et si des dossiers médicaux électroniques se développent, l'idée d'un dossier totalement dématérialisé et déposé chez un hébergeur agréé est, pour sa part, nouvelle. Dans un premier temps, le législateur avait envisagé la possibilité de faire appel à plusieurs hébergeurs de données différents, chaque détenteur d'un DMP étant libre de choisir l'hébergeur de son choix et d'en changer s'il le souhaite. Toutefois, cette solution lors des premières expérimentations de 2006, présente vite ses limites : tous les hébergeurs ne proposant pas le même niveau de sécurité, malgré les obligations auxquelles ils sont

[363] Loi n° 2007-1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008, *JORF* n°0296 du 21 décembre 2007, p. 20603.
[364] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, *JORF* n°0155 du 5 juillet 2016, texte n° 20.

soumis[365]. Enfin, après avoir songé pendant un temps à la mise en place d'un hébergeur de référence, et avoir classé sans suite l'appel d'offres qui avait été lancé pour le sélectionner, le législateur a adopté[366], ce qui fait aujourd'hui du DMP un dossier unique en son genre : le portail d'accès unique.

277. En parallèle, la politique en matière d'hébergement du DMP a été repensée et, le législateur a fait le choix d'un hébergeur unique : un seul accès, un seul hébergeur pour arriver à un même dossier pour tous les assurés sociaux. Suite à un appel d'offre, la commission des marchés de l'ASIP Santé, a retenu, à l'unanimité de ses membres, le consortium industriel mené par les groupes ATOS Origin et LA POSTE, et constitué des sociétés ATOS wordline S.A.S., SANTEOS S.A., EXTELIA S.A.S., HSC, SOFTWAY Medical Services, EVALAB.

2) Le DMP, complément ou concurrent des autres dossiers ?

« *La multiplicité des informations conduit naturellement à celle des dossiers et cette multiplicité est bien naturelle : chaque professionnel de santé a vocation à avoir son dossier sur ses patients* »[367].

278. En créant le DMP, le législateur a souhaité proposer un outil accessible à tous les professionnels intervenant lors de la prise en charge d'un patient donné. Toutefois, comme le souligne François VIALLA, chaque professionnel, selon sa spécialité, va produire des informations de types et formes différentes (imagerie, compte rendu, résultats de laboratoire, …). De même, chaque professionnel, dans son exercice, va tenir son propre dossier. Or, face à la démultiplication des dossiers se pose la question de savoir comment ceux-ci s'articulent entre eux. Est-ce qu'ils se complètent ? S'alimentent entre eux ? Ou alors sont-ils redondants, auquel cas certains d'entre eux seraient amenés à disparaitre ? Finalement, la question principale qui se pose ici est de savoir si le DMP, de par ses particularités, est un concurrent ou un réel complément aux autres dossiers.

---

[365] *V. Supra*. n° 179 et s.
[366] Loi n° 2007-1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008, *JORF* n°0296 du 21 décembre 2007, p. 20603.
[367] VIALLA, François. « Dossier patient, DMP : quelles frontières », *RGDM*, n° 20, 2006, p. 135.

279. Selon l'avis du Comité Consultatif National d'Ethique (CCNE), relatif au Dossier médical Personnel et à l'informatisation des données[368], « *aux yeux d'un certain nombre d'acteurs de soin, la notion de "dossier médical personnel" recouvre celle de dossier médical partagé entre les professionnels de santé. Les membres du corps médical sont enclins à y voir un outil de travail à usage professionnel. Ils y trouvent un intérêt dans la mesure où toutes les informations utiles sont accessibles aux soignants qui en ont besoin […]. Ils proposent qu'une partie du contenu de ce dossier médical partagé puisse éventuellement constituer le dossier médical personnel* ». Toutefois, la fusion des deux types de dossiers est présentée comme périlleuse et ingérable et il est fait une distinction nette entre le dossier médical, outil professionnel, et le DMP, outil certes utile aux professionnels, mais principalement à destination du patient. Toujours en ce sens, le bilan de la mission menée par Jean-Pierre DOOR tend à montrer qu'une pluralité de DME n'est pas à exclure et que les DME déjà existants et opérationnels poursuivent, de toute manière, des objectifs plus complémentaires que concurrents au DMP. Ainsi, le DMP serait bien un complément des autres dossiers médicaux existants, qu'ils soient partagés ou non.

280. Dans le rapport consacré à la relance du DMP[369], Michel GAGNEUX rappelle que le DMP est avant tout un dossier patient plus qu'un véritable dossier médical. Dès lors, il n'est donc pas envisageable qu'il vienne se substituer aux dossiers médicaux tenus par les professionnels, « *même s'il contribue à les faire évoluer* »[370]. Là encore, le rôle complémentaire du DMP par rapport aux autres dossiers médicaux est mis en valeur.
Toutefois, cette vision n'est pas partagée par tous les auteurs. Ainsi, Olivier SAUTEL considère que « *le DMP viendra d'abord en concurrence avec le dossier papier. Puis il aura vocation à s'y substituer totalement. Le dossier papier est donc voué à la disparition. C'est la logique implacable de la réforme DMP* »[371].

281. Plusieurs critiques peuvent toutefois être émises.. D'une part, l'auteur confond dossier médical électronique et DMP : certes, l'informatisation grandissante conduira certainement à

---

[368] Avis du Comité National Consultatif n° 104, « le Dossier médical personnel et l'informatisation des données de santé », juin 2008, p. 5.
[369] GAGNEUX, Michel. COMBLE, Pierre-Henri. De KERGOMMEAUX, Loïc. « Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé », recommandations à la ministre de la santé, de la jeunesse, des sports et de la vie associative, avril 2008.
[370] *Id.*, p. 27.
[371] SAUTEL, Olivier. « Le dossier médical personnel », *Journal de médecine légale*, 2007, p. 6.

l'avenir la disparition des dossiers médicaux papiers. Mais ce sont bien différents DME, propres à chaque établissement de santé ou professionnel de santé, qui le remplaceront. Nous partageons ici le point de vue de Cécile MANAOUIL[372] et estimons que cette affirmation relève d'une confusion entre informatisation des dossiers médicaux et instauration du DMP. Il n'est pas envisageable, de notre point de vue, qu'un dossier, dont le patient est titulaire, vienne remplacer les dossiers professionnels, que ceux-ci soient partagés ou non. Cette affirmation dénote une mauvaise compréhension des ambitions du DMP, mais également du fonctionnement du système de santé et de l'organisation des professionnels de santé dans leur pratique.

282. Finalement, le DMP est une vision globale de l'état de santé du patient : en cela il permet de compléter les informations que chaque professionnel de santé possède déjà. Toutefois, il nous semble qu'un professionnel de santé ne pourra pas décemment supprimer le propre dossier médical qu'il tient, certainement plus précis dans sa spécialité que ne le sera le DMP. Le DMP ne doit pas être considéré comme concurrent ou redondant avec d'autres dossiers. Ce point a d'ailleurs été éclairci par le législateur en juillet dernier[373], puisque l'article R 1111-28 du Code de la santé publique prévoit désormais que « *le dossier médical partagé ne se substitue pas au dossier que tient chaque établissement de santé […]* ».

[372] MANAOUIL, Cécile. « Le dossier médical personnel (DMP) : autopsie d'un projet ambitieux ? », *Médecine et droit*, 2009, p. 26.
[373] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, *JORF* n°0155 du 5 juillet 2016, texte n° 20.

§2. Le DMP, un encadrement juridique évoluant avec difficultés

283. Projet en route depuis plus de dix ans, le DMP rencontre de nombreuses difficultés à se développer et à trouver sa place. D'ailleurs, la précipitation et les premières orientations balbutiantes du DMP (A) ont conduit le législateur a rapidement repenser son projet et engager plusieurs relances, devenues nécessaires (B).

A. Les premiers pas du DMP : des orientations incertaines

Le DMP est en réalité le fruit d'une longue réflexion relative à l'informatisation des données et les principes fondamentaux qui le régissent sont finalement assez classiques (1). Toutefois, au fur et à mesure des nombreuses critiques du projet, celui-ci a dû s'adapter, au gré notamment des différentes lois de financement de sécurité sociale (2).

1) Origines et principes fondamentaux du DMP

284. L'idée d'un dossier reprenant l'ensemble des éléments relatifs à un patient et partagé dans un objectif de meilleure coordination entre plusieurs professionnels de santé différents n'est pas nouvelle. Avec l'introduction et le développement des TIC dans la pratique médicale, facilitant le partage et la diffusion de l'information médicale, cette idée s'est faite de plus en plus présente.

285. Le rapport de Marius FIESCHI[374], rendu en 2003, faisait d'ailleurs état de cette tentative, depuis de nombreuses années, de mettre en place un dossier partagé. Il soulignait l'échec du projet de Dossier Minimum Commun (DMC). Il rappelait également l'intérêt de mettre en place un dossier visant à rassembler toutes les informations médicales concernant un patient, modèle correspondant alors mieux à la réalité de l'état de santé du patient car non centré sur une seule pathologie. Il avançait alors le nom de "Dossier Patient Partagé" (DPP).

[374] FIESCHI, Marius. « Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins », *op. cit.*

Se basant sur ce rapport, le ministre de la santé de l'époque, M. Philippe DOUSTE-BLAZY, a alors décidé d'en faire un projet national phare. C'est la loi du 13 août 2004 relative à l'assurance maladie[375] qui a créé, en son article 3, le dossier médical personnel[376]. Les dispositions relatives au DMP ne sont alors pas nombreuses, mais elles sont très denses[377] et insérées aux articles L. 162-36-1 à L. 162-36-4 du Code de la sécurité sociale. Comme le soulignait à juste titre Didier TRUCHET[378], cette considération n'est pas anecdotique puisqu'elle détermine le champ d'application de la loi : tous les bénéficiaires de l'assurance maladie pourront ouvrir un DMP, et non pas tous les patients. De plus, le fait que le DMP soit créé par une loi relative à l'assurance maladie, et ses dispositions présentes dans le Code de la sécurité sociale marque bien l'objectif premier confié au DMP : la réalisation d'économies en termes de dépenses de santé. Cet objectif n'a jamais été clairement affiché par le législateur.

L'article L 161-36-1 du Code de la sécurité sociale prévoyait la création du DMP « *afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé* ». Toutefois, en prévoyant ce dispositif au sein d'une loi consacrée à l'assurance maladie, et en insérant son encadrement au sein du Code de la sécurité sociale, le législateur faisait, de fait, du DMP un outil au service de l'assurance maladie. D'ailleurs, dans le rapport relatif au DMP de 2007, la plus grande maîtrise des dépenses d'assurance maladie, via la diminution des actes redondants, inutiles ou iatrogènes fait partie des quatre objectifs initiaux constatés du DMP[379].L'article 3 de la loi du 4 août 2004 a ainsi posé, les bases juridiques du DMP, laissant à un décret pris en Conseil d'Etat le soin d'apporter l'ensemble des précisions pratiques qui seront nécessaires à la bonne mise en œuvre de l'outil. Cependant, ce décret n'a jamais vu le jour.

286. A l'origine, les principes qui régissaient le DMP sont les suivants : en tant que dossier "personnel"[380], le DMP était placé sous le contrôle[381] du patient, celui-ci accordant ou non son

---

[375] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, *JORF* n°0190 du 17 août 2004, p. 14598.
[376] Alors que l'article 3 de la loi du 4 août 2004 est venue créer le Dossier Médical Personnel, la rédaction actuelle de l'article L. 1111-5 du Code de la santé publique, issue de la loi de modernisation de notre système de santé, dispose que : « *dans le respect des règles déontologiques qui lui sont applicables ainsi que des articles L. 1110-4, L. 1110-4-1 et L. 1111-2, chaque professionnel de santé, quels que soient son mode et son lieu d'exercice, reporte dans le dossier médical partagé […]* ».
[377] TRUCHET, Didier. « Que dit la loi ? », *RGDM*, N°20, 2006, p. 67.
[378] *Ibid.*
[379] Rapport sur le Dossier médical personnalisé, *Inspection générale des finances, Inspection générale des Affaires sociales, Conseil générale des Technologies de l'Information*, novembre 2007, p. 1.
[380] Rappelons qu'initialement, le DMP était l'acronyme de « dossier médical personnel ».

consentement à l'ouverture du dossier et désignant les professionnels pouvant y accéder. Les professionnels et les établissements de santé avaient, quant à eux, pour obligation d'alimenter ce dossier. En effet, l'adhésion et le maintien aux conventions nationales signées entre professionnels de santé et l'assurance maladie était soumis à la consultation et à la mise à jour du DMP par les professionnels. En contrepartie, il était également prévu que le niveau de prise en charge des actes et prestations soit subordonnée à l'autorisation donnée par le patient au professionnel de consulter son DMP.

287. Lors de la publication de la loi, cette dernière mesure avait été vivement critiquée et, le Conseil Constitutionnel avait été saisi au motif, notamment, que cette disposition portait atteinte au droit à la protection sociale garanti au titre du préambule de la Constitution de 1946. Le Conseil Constitutionnel a toutefois considéré que, « *eu égard aux finalités des dispositions contestées, qui sont, d'une part, d'améliorer la qualité des soins, d'autre part, de réduire le déséquilibre financier de l'assurance maladie, et compte tenu de l'ensemble des garanties qui viennent d'être rappelées, le législateur a opéré, entre les exigences constitutionnelles en cause, une conciliation qui n'apparaît pas manifestement déséquilibrée ; que, dès lors, les griefs invoqués doivent être rejetés* »[382.] Ainsi, pour les sages du Conseil, le droit à la santé nécessite un système de protection sociale qui se doit d'être en équilibre financier, et par conséquent, des concessions doivent également être opérées de la part des bénéficiaires de ce système[383]. Pour reprendre les mots, de François VIALLA, le patient « *s'est vu reconnaitre des droits, il commence à en découvrir les contreparties* »[384]

288. La loi de 2004, soucieuse de préserver le secret professionnel malgré la mise en place d'un outil destiné à être partagé avec un grand nombre de professionnels, prévoyait des garanties en ce sens, puisque le DMP devait être mis en place dans le respect du secret médical (article L. 161-36-1), et hébergé auprès d'un hébergeur agrée, la consultation se faisant dans le respect des règles déontologiques applicables au professionnel ainsi que dans le respect des articles L. 1110-4 et L. 1111-2 du Code de la santé publique. Enfin, il était également prévu l'interdiction de consulter le DMP dans certaines situations, telle que lors de

---

[381] *V. Supra.* n°112 à 119.
[382] Décision du Conseil Constitutionnel n° 2004-504 du 12 août 2004, *JORF* n°190 du 17 août 2004, p. 14657.
[383] VIALLA, François. « Secret et DMP », *RDS*, 2005, pp. 42-44.
[384] *Id.*, p. 42.

la conclusion d'un contrat d'assurance par exemple, ou de tout autre contrat qui nécessiterait l'évaluation de la santé d'une personne.

Cette première version du DMP a toutefois rapidement fait l'objet de critiques et certaines évolutions ont été instaurées au fil des années.

2) Des évolutions au gré des critiques

289. La loi du 13 août 2004 prévoyait que l'ensemble des précisions utiles à la mise en place du DMP seraient apportées dans un décret pris en Conseil d'Etat. Cependant, bien qu'un projet ait été soumis à concertation publique, ce décret n'a jamais vu le jour. Certaines précisions ou modifications ont toutefois été apportées au projet initial, certaines résultants parfois des critiques émises à l'encontre du projet. Ces compléments sont de deux ordres. D'une part, des éléments pratiques ont été mis en place (a) et d'autre part, des précisions sur le fonctionnement du DMP ont été apportées (b).

a) Les apports pratiques

290. Afin de lancer la mise en œuvre pratique du DMP, un GIP de préfiguration, le GIP DMP, a été créé et sa convention constitutive approuvée par un arrêté en date du 11 avril 2005[385].Il était composé de l'Etat, de la Caisse nationale d'assurance maladie des travailleurs salariés et de la Caisse des dépôts et consignations. Son objet consistait à préparer les dispositions juridiques, organisationnelles, financières et logistiques du futur organisme gestionnaire du dossier médical personnel et d'en assurer les premières réalisations. Ce groupement devait permettre au futur organisme gestionnaire du dossier médical personnel d'être immédiatement opérationnel dans la perspective de la publication du décret d'application de la loi relative à l'assurance maladie. Le GIP-DMP était donc une structure temporaire censée faciliter l'expérimentation puis la mise en place du DMP, amenée à disparaitre dès que l'organisme gestionnaire du DMP aurait été mis en place et apte à effectuer ses missions. Cependant, le législateur s'est révélé quelque peu présomptueux sur le calendrier de réalisation de ce projet : bien que le groupement d'intérêt public "groupement de préfiguration du dossier médical personnel" était initialement créé pour une durée de vie

[385] Arrêté ministériel du 11 avril 2005 portant approbation de la convention constitutive d'un groupement d'intérêt public.

limitée, puisqu'il devait prendre fin le 31 décembre 2005, celui-ci sera maintenu jusqu'en 2009, année de mise en œuvre du programme relance du DMP.

291. De manière pratique, une phase d'expérimentation, autorisé par une délibération CNIL en date du 30 mai 2006[386], a débuté le 1er juin de la même année. Le Cadre de cette expérimentation, ainsi que les perspectives de généralisation du DMP, ont par ailleurs été précisés par la circulaire du 28 juin 2006 relative à la mise en œuvre du DMP par les établissements de santé[387]. Cette circulaire dressait également un calendrier de déploiement particulièrement ambitieux puisque la phase de généralisation était censée débuter au premier semestre 2007.

b) Les apports sur le fond

292. La loi de 2004 instaurant le DMP était loin d'être complète et certaines précisions ont été apportées par la suite. Nous traiterons ici de l'ensemble des modifications qui ont eu lieu sur le projet initial et non pas des modifications apparues après 2009, lors des phases de relance du DMP.

293. La plupart des ajouts ont été apportés par la loi de financement de sécurité sociale pour 2008[388]. Ainsi, ce texte est d'abord venu combler une lacune en matière d'accès au DMP par les ayants droit. En effet, en cas de décès du patient détenteur d'un DMP, rien n'était prévu dans la loi initiale. La LFSS pour 2008 a donc appliqué au DMP les dispositions existantes en matière de communication du dossier médical aux ayants droit d'un patient décédé[389]. Toutefois, aucune précision n'a été apportée au sujet des modalités pratiques d'accès : cet accès doit-il se faire par le biais d'un professionnel de santé ? Du médecin traitant ? Ou encore par le concours du médecin de l'hébergeur ? Rien n'était précisé par cette loi et, aujourd'hui encore, malgré différentes réformes[390], le doute subsiste. Pour notre part, il nous

---

[386] Délibération CNIL n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel.
[387] Circulaire DHOS/E3 n° 2006-281 du 28 juin 2006 relative à la mise en œuvre du dossier médical personnel (DMP) par les établissements de santé, *BO* n° 2006/7.
[388] Loi n° 2007-1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008, *JORF* n°0296 du 21 décembre 2007, p. 20603.
[389] L'article L. 1110-4 du Code de la santé publique prévoit que « *Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès* ».
[390] *V. Infra.* n° 306 à 309.

semble que le médecin traitant serait l'interlocuteur le plus à même de sélectionner les documents à transmettre aux ayants-droits.

294. La LFSS pour 2008 a également apporté une modification très importante dans le fonctionnement du DMP puisqu'elle a introduit le très largement débattu droit au masquage. Pas de manière très précise il est vrai, puisque le texte se bornait à prévoir qu' *« un décret en Conseil d'Etat fixe les conditions dans lesquelles certaines peuvent être rendues inaccessibles par le titulaire du DMP ou son représentant légal, ainsi que les modalités selon lesquelles le professionnel de santé accédant au DMP a connaissance de l'inscription au dossier d'informations rendues inaccessibles par son titulaire ou son représentant légal*».

Par ailleurs, la LFSS pour 2008 a créé le portail d'accès unique au DMP, qui permet au patient de gérer son DMP et notamment les droits d'accès y afférant. Cette disposition a ainsi permis d'assurer une harmonisation en matière d'accès et d'utilisation de son DMP par le patient. La LFSS pour 2008 a également été l'occasion de supprimer une disposition contraire au respect de certains droits fondamentaux et introduite par la loi du 5 mars 2007 instituant le droit au logement opposable[391]. Celle-ci permettait l'accès par un bailleur au DMP d'un candidat à un logement adapté ou spécifique[392].

295. Enfin, la loi du 30 janvier 2007[393] a instauré, non sans mal, le dispositif du "bris de glace", qui permet un accès au DMP dans les cas d'urgences. Désormais, dans ces situations, le consentement préalable du patient pour accéder à son dossier n'est plus nécessaire. Il est intéressant de noter que cette disposition était initialement prévue dans la LFSS pour 2007, mais avait été déclarée non conforme à la Constitution par une décision du Conseil constitutionnel[394].

---

[391] Loi n° 2007-290 du 5 mars 2007 instituant le droit au logement opposable et portant diverses mesures en faveur de la cohésion sociale, *JORF* n°55 du 6 mars 2007, p. 4190.
[392] MANAOUIL, Cécile. « Le dossier médical personnel (DMP) : autopsie d'un projet ambitieux ? », *op. cit.*, p. 29.
[393] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le Code de la santé publique, *JORF* n°27 du 1 février 2007, p. 1937.
[394] Décision du Conseil Constitutionnel n° 2004-504 du 12 août 2004, *JORF* n°190 du 17 août 2004, p.14657.

B. Une rapide remise en question du projet initial

296. Dès 2007, soit à peine trois ans après la promulgation de la loi relative à l'assurance maladie créant le DMP, les premiers bilans relatifs à la mise en œuvre de ce dossier ont été effectués et leur résultat a été négatif (1). Le ministère a alors souhaité reprendre les choses en main et mettre en place une relance du projet (2). Celle-ci, dont les résultats ont été mitigés, a donc été suivie d'une deuxième relance (3) engagée par le biais de la loi de modernisation de notre système de santé.

1) Un premier bilan négatif

297. Face aux ambitions démesurées de la loi du 13 août 2004, aux difficultés à faire avancer correctement le projet et à toutes les critiques relatives au DMP, l'exécutif a ordonné une mission interministérielle de revue de projet sur le DMP afin de *« réaliser un point détaillé sur l'état d'avancement et le pilotage de ce projet ainsi que sur sa capacité de répondre aux objectifs initiaux »*[395]. Cette mission a été confiée à l'Inspection générale des finances, à l'Inspection générale des Affaires Sociales et au Conseil général des Technologies de l'Information. L'ensemble de la mission a été conduite par Michel GAGNEUX, et un rapport a été rendu en novembre 2007 (a). En parallèle, la CNIL a, elle aussi, rendu un rapport, portant pour sa part sur le bilan des premières expérimentations du DMP (b).

a) Le rapport GAGNEUX

Ce rapport visant à effectuer l'audit du projet DMP sur la période 2005/2007 dresse un bilan plus que négatif des premières tentatives de mise en œuvre du DMP.

298. La principale critique porte sur les objectifs initiaux du législateur en matière de mise en œuvre du DMP, hors d'atteintes. A la fois les délais (tout assuré pourrait avoir un DMP ouvert au 1er juillet 2007), le coût et le modèle économique du projet ne permettaient pas le succès pourtant annoncé de celui-ci. En effet, nous pensons que le législateur, au lieu de choisir la précipitation, aurait dû prendre le temps d'étudier l'organisation déployée dans les pays voisins dans le cadre de projets similaires et s'en inspirer directement. L'étude de ces

[395] Lettre de mission relative à la mission interministérielle de revue de projet sur le dossier médical personnel (DMP), rapport sur le dossier médical personnel, *op. cit.*

projets aurait permis, selon nous, de mettre en évidence le caractère utopiste de la méthodologie initiale choisie par notre législateur, notamment en termes de calendrier. Dès lors, il ne peut que ressortir de ce rapport le manque de crédibilité et de lisibilité du projet, du fait des trop nombreuses zones de risques et d'incertitudes dans la stratégie mise en œuvre. Nous ne pouvons qu'être d'accord avec les conclusions de ce rapport, qui montrent que la précipitation a guidé l'ensemble des actions mises en œuvre, ce qui a joué en défaveur du DMP. Alors même que le concept et la finalité du DMP n'étaient pas clairement précisés, seule la mise en œuvre technique faisait l'objet de toutes les attentions.

299. La mission interministérielle de revue du projet a abouti à sept recommandations : déclarer sans suite la consultation à l'époque en cours pour la désignation de l'hébergeur de référence, sauvegarder les acquis, restaurer la confiance dans le projet, relancer la dynamique du projet, résoudre parallèlement les questions majeures, notamment juridiques, en suspens, attribuer au DMP un budget de programme et refonder la gouvernance des systèmes d'information dans le domaine de la santé. Dans la foulée de cet audit, Michel GAGNEUX a ensuite rédigé et présenté un rapport, en 2008, consacré à la relance du DMP[396].Reprenant pour partie les recommandations énoncées dans son précédent rapport, l'auteur dresse les contours de ce qui sera, en 2009, avec la loi HPST, les bases de la relance du DMP.

b) Le bilan de la CNIL

300. Suite aux premières expérimentations qui se sont déroulées d'avril à décembre 2006, la CNIL, qui s'était prononcée sur les dossiers d'agrément des hébergeurs de données de santé sélectionnés pour la phase d'expérimentation, a contrôlé sur site les principaux acteurs. Le but de la CNIL n'était pas tant de réaliser un contrôle exhaustif des différentes pratiques, mais plutôt d'apprécier la réalité des engagements pris par les hébergeurs dans le dossier d'agrément. Le bilan, qui a résulté de ces contrôles, s'est montré sévère.

301. Bien entendu, la courte durée de cette expérimentation, qui a résulté d'un changement de stratégie en cours de route, n'a pas permis à la CNIL de mesurer de manière efficace le fonctionnement des différents acteurs. Il est cependant ressorti un manque de sécurité et une défaillance de certains hébergeurs de santé. Certaines pratiques relatives à la communication

[396] GAGNEUX, Michel. COMBLE, Pierre-Henri. FOLLIET, Alain. DE KERGOMMEAUX, Loïc. LIVARTOWSKI, Alain. LOTH, André. RICHARD, Denis. SAURET, Jacques. « Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé », rapport de la mission de relance du DMP, 23 avril 2008.

au patient de son numéro identifiant santé (INS) et de son Adresse Qualité Santé (AQS) ont été pointées comme de nature à compromettre la confidentialité des informations. Du côté de l'alimentation des dossiers, le constat effectué était le même : les procédures d'identification et d'authentification des personnels ne permettaient pas de maintenir un niveau de sécurité suffisant.

302. L'accès en mode "bris de glace" est une autre des difficultés que le contrôle de la CNIL a mis en valeur. La CNIL a pointé ici, et à juste titre, le caractère contradictoire de certaines situations par rapport à la finalité même du mode d'accès. A titre d'exemple, l'identifiant du patient (AQS) devait être entré pour accéder au DMP en mode bris de glace. Or, la finalité première de ce type d'accès était pourtant d'accèder aux données d'un patient dans des cas d'urgences, notamment si celui-ci est inconscient et donc inapte à renseigner ce type d'informations.

303. La CNIL avait aussi soulevé l'absence de la traçabilité des accès en mode bris de glace au bénéfice du médecin de l'hébergeur, dont la mission principale consistait pourtant à veiller à la confidentialité des données. Le Médecin de l'hébergeur est donc bien le seul légitime et potentiellement capable d'alerter en cas d'utilisation frauduleuse ou trop importante de ce genre d'accès.

304. Enfin, et c'est peut-être là une des problématique ayant conduit à l'échec de cette expérimentation, la CNIL, lors de ces contrôles, a constaté que certains hébergeurs n'avaient pas mis en place l'intégralité de leur architecture technique, préférant attendre la phase de généralisation avant d'engager les investissements nécessaires. Or, il nous semble que ce type de comportement, en plus d'être révélateur d'une certaine méfiance vis-à-vis du projet, a conduit la phase d'expérimentation à ne pas être exécutée correctement ce qui a amené à des conclusions faussées. Bien entendu, d'autres problèmes techniques et juridiques ont été relevés, mais l'implication partielle de certains acteurs n'a pas permis, selon nous, de soutenir correctement le projet.

305. En conclusion de ses contrôles, la CNIL a rappelé aux hébergeurs de santé, mais également au GIP-DMP ainsi qu'au Ministère de la santé, qu'une authentification forte, un chiffrement complet et une information claire et complète des patients étaient les conditions nécessaires à remplir.

En 2009, suite aux différents rapports ayant émis de nombreuses préconisations sur la réforme de l'outil, la Ministre de la santé de l'époque a annoncé la mise en œuvre d'un plan de relance du DMP

2) Une première relance mitigée

306. Lors de son discours[397] à l'occasion d'un colloque consacré à la relance du DMP, la Ministre de la santé, Madame Roselyne Bachelot, avait présenté la nouvelle feuille de route du projet. Reprenant largement les préconisations développées dans les différents rapports consacrés au sujet, la Ministre avait alors annoncé que la nature du DMP serait clarifiée, le dossier repositionné comme étant un outil au service du patient et des professionnels et non pas un outil purement technique, éloigné des réalités pratiques et enfin, que la priorité serait donné aux expérimentations au plus près des pratiques afin d'adapter l'outil aux mieux aux besoins. De même, la volonté de rupture vis-à-vis de l'ancien projet a été marquée par le changement de la gouvernance du projet : l'ASIP santé a ainsi récupéré la gestion du projet.
Le ministère a essayé de se montrer plus prudent et raisonnable dans la mise en œuvre du DMP. Ainsi, une phase d'expérimentation, à l'échelle régionale et non plus nationale a été mise en œuvre en 2009 afin de pouvoir ensuite déployer progressivement une première version nationale. Ces expérimentations ont permis de choisir parmi les solutions les plus efficaces développées en région pour les développer au niveau supérieur.

307. En parallèle de cette annonce, la loi HPST[398] a transposé les dispositions relatives au DMP qui se trouvaient au sein du Code de sécurité sociale, au sein du Code de la santé publique. Ce passage d'un code à l'autre présente une portée hautement symbolique : le but premier du DMP n'est plus la maîtrise des dépenses de santé mais l'amélioration et la coordination des soins. Avec la réforme introduite par Mme BACHELOT, le DMP n'est plus un outil de sécurité sociale mais bien un outil de santé publique.

308. Le DMP n'est plus obligatoire et le patient devient dès lors véritable maître de son dossier, pouvant choisir de l'ouvrir ou non. De même la sanction financière en cas de refus

---

[397] Discours prononcé à l'occasion du colloque consacré à la relance du DMP, 9 avril 2009, disponible sur [http://sante.gouv.fr]. Consulté le 15 mai 2017.
[398] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, *JORF* n°0167 du 22 juillet 2009, p. 12184.

d'accès par certains médecins disparait. Là encore, cette disposition nous apparait comme révélatrice de la volonté du législateur de marquer le changement d'orientation et la priorité donnée à l'amélioration de la coordination de soins, thématique plus attractive que celle de la maîtrise des dépenses de santé.

Révélateur de la prudence nouvelle du législateur, aucune date précise de déploiement n'est actée dans les textes, ceux-ci se contentant désormais de prévoir une mise en œuvre *«dès que l'utilisation du dossier médical personnel est possible sur l'ensemble des territoires auxquels s'applique la présente section* »[399].Toutefois, lors de son discours d'avril 2009, la ministre de la santé avait évoqué le possible déploiement national dès 2010. Or, en pratique, bien que la généralisation sur le territoire soit instaurée en avril 2011, le DMP va pâtir de la suppression, en novembre 2011, de son budget de déploiement par la CNAMTS. Ainsi, en décembre 2011, seuls 56 000 patients disposaient de leur DMP, sans pour autant savoir combien d'entre eux étaient réellement actifs, c'est-à-dire alimentés et consultés. Malgré un projet « techniquement prêt » selon les termes du directeur de l'ASIP de l'époque, Jean-Yves ROBIN, seuls 90 000 dossiers étaient créés en mars 2012, le projet étant figé dans sa phase de test.

309. En dépit d'une relance cohérente et mieux préparée, force est de constater que le DMP, lors de sa première relance a pâti, en plus de problématiques financières, de considérations politiques, qui ont malheureusement pris le dessus sur les considérations de santé publique. Il est en effet utile de rappeler que l'année 2012 a été une année d'élections. Le projet a ainsi subi un retard lié à la mise en œuvre d'un nouveau gouvernement.

3) La loi de modernisation de notre système de santé, un nouveau souffle pour le DMP

310. Dans l'optique d'amorcer une ultime relance du DMP, Marisol TOURAINE, Ministre de la santé, avait annoncé, dès novembre 2012, la mise ne place d'un DMP 2. Toutefois, aucune réelle précision au sujet de ce dossier n'avait été apportée, jusqu'à la présentation du projet de loi de santé, en juin 2014[400]. C'est ainsi que l'article 96 de la loi de modernisation de

[399] Article L. 1111-14 du Code de la santé publique.
[400] Projet de loi relatif à la santé, disponible sur [https://www.legifrance.gouv.fr]. Consulté le 11 mai 2017.

notre système de santé, complété par le décret n° 2016-1545 du 16 novembre 2016[401], sont venus refondre une nouvelle fois le dispositif de DMP.

311. L'exposé des motifs de la loi de modernisation de notre système de santé s'appuie sur le caractère essentiel du DMP dans la coordination des prises en charge et tente de démontrer que le législateur a appris de ses erreurs passées : « *le nouveau dispositif tire les leçons des échecs successifs des différents modèles de développement du DMP, souffrant depuis le début d'une confusion d'objectifs. Assumer les difficultés rencontrées conduit à proposer un DMP pluriel, adapté aux besoins de chacune des parties prenantes, et notamment des professionnels de santé. L'enjeu du "DMP 2" est de définir le socle d'informations qui doit y figurer. La crédibilité de l'outil et sa pleine appropriation par les usagers et les professionnels dépend de la rapidité de son implantation, de sa capacité à devenir un outil efficace de coordination, du rôle que le médecin traitant s'y voit conférer, et enfin des garanties sans faille qu'il apporte dans la défense des intérêts et des droits des usagers*. »[402]
L'ambition du législateur, avec cette ultime relance, est de faire du DMP l'outil de référence comme support de la prise en charge coordonnée des patients, notamment dans le cas des malades atteints de pathologies chroniques.

312. La gestion de ce nouveau DMP et de son déploiement est confiée à la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés (CNAMTS), considérée comme plus à même que l'ASIP santé d'assurer le déploiement effectif de l'outil. Afin de ne pas reproduire certaines erreurs effectuées dans la gestion passée, le législateur a adopté, dans la foulée, le décret d'application des dispositions issues de la loi de modernisation de notre système de santé.

313. Le DMP est désormais défini comme un « *dossier numérique destiné à favoriser la prévention, la qualité, la continuité et la prise en charge coordonnée des soins du patient* »[403]. Le patient reste le "titulaire" du dossier même si celui-ci n'est plus personnel mais désormais partagé. Cette nouvelle dénomination a le mérite de marquer le but premier de ce dossier :

---

[401] Décret n° 2016-1545 du 16 novembre 2016 autorisant la création d'un traitement de données à caractère personnel dénommé « dossier médical partagé », *JORF* n°0268 du 18 novembre 2016, texte n° 14.
[402]Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, exposé des motifs, disponible sur :[https://www.legifrance.gouv.fr]. Consulté le 11 mars 2017.
[403] Article R. 1111-26 du Code de la santé publique.

partager l'information médicale le plus largement possible afin d'améliorer le fonctionnement du système de santé[404].

314. Cette ultime relance s'accompagne d'un plan d'action de la CNAMTS ambitieux afin de faire du DMP un outil incontournable, ouvert pour chaque assuré social. Sa création sera simplifiée puisqu'il la possibilité d'une création directe par le patient, depuis le site de l'assurance maladie, est envisagée.[405]

La CNAMTS a fait le choix d'une stratégie progressive puisque dans un premier temps, le déploiement n'est envisagé que dans neufs départements pilotes.Enfin, afin d'inciter les patients à s'intéresser au DMP et donc à créer le leur, la CNAMTS envisage la création d'une application mobile sur laquelle pourra être consulté le DMP[406].

[404] Etude d'impact du projet de loi relatif à la santé, octobre 2014, p. 99.
[405] « Relance du DMP: une création automatique d'ici fin 2016 et un intéressement à l'alimentation pour les médecins (Cnamts) », *Dépêche TIC santé*, 21 septembre 2015, disponible sur [http://www.ticsante.com]. Consultée le 8 mars 2017.
[406] « DMP: une application mobile attendue "au printemps" 2017 (Nicolas Revel) », *Dépêche TIC santé*, 10 novembre 2016, disponible sur [http://www.ticsante.com]. Consultée le 8 mars 2017.

Conclusion de la section

315. Le DMP, dossier médical informatisé, partagé entre les différents professionnels de santé et accessible directement par le patient, est un projet qui peut être qualifié d'original et ambitieux. Original de par son format et ambitieux de par les objectifs qu'il devait atteindre.
Toutefois, dès le départ, le législateur avait affiché un calendrier de mise en œuvre du DMP beaucoup trop ambitieux. En effet, là où les pays voisins ont mis une dizaine d'année à développer et faire entrer dans les pratiques des dossiers partagés informatisés, le législateur, dans la loi de 2004, annonçait une entrée en vigueur définitive des dispositions au 1er juillet 2007. Or, très rapidement, le projet a fait l'objet de vives critiques, ce qui a amené le législateur, à mettre en œuvre différentes relances du projet.

Section 2. Le DMP : les limites d'un projet ambitieux

« *Le DMP est un projet de société qui bouleverse les habitudes et les mentalités. Il constitue un facteur d'évolution des pratiques médicales et des relations entre patients et professionnels de santé* […] »[407]

316. Projet titanesque à envergure nationale, annoncé comme un outil unique en son genre, le DMP devait remplir des objectifs aux enjeux stratégiques. Toutefois, les différents responsables du projet se sont montrés trop ambitieux et parfois même trop confiants dans la réalisation et la mise en place de ce projet. Les ambitions du DMP étaient certes louables, mais peut-être démesurées face aux moyens et surtout au temps accordé pour sa mise en place (Paragraphe 1). Aujourd'hui, après plus de dix ans de tentatives de mise en place et d'échecs successifs, l'avenir de cet outil prometteur se révèle finalement incertain (Paragraphe 2).

§1. Des ambitions louables mais démesurées

317. Nous ne pouvons que rappeler et souligner, une fois de plus, les ambitions louables du législateur quand il a souhaité mettre en place le DMP. Dès son lancement, l'outil se révélait plein de promesses tant sur le fond que sur la forme (A). Toutefois, de nombreuses lacunes, notamment en termes d'encadrement juridique, sont apparues dès le lancement du projet. Cela s'est alors révélé fâcheux dans la conduite et le développement du projet (B)

A. Un outil plein de promesses

318. L'objectif initial du DMP était d'instaurer une meilleure coordination des soins, afin d'en améliorer la qualité et la continuité. De cela aurait alors résulté une meilleure maîtrise des dépenses de l'Assurance maladie.

En permettant de réduire les interactions médicamenteuses et les actes redondants, mais en facilitant également les échanges entre professionnels de santé, le DMP devait relever le

[407] MONNIER, Anne. « Le Dossier médical personnel : histoire, encadrement juridique et perspectives », *RDSS*, 2009, p. 625.

défi d'améliorer la coordination et la qualité des soins (1). Toutefois, en pratique, l'accent et la priorité ont été axés sur les aspects techniques de l'outil, et notamment la sécurisation des données (2).

1) L'amélioration et la coordination des soins, un enjeu majeur

« Dans quelques mois donc, les premiers DMP seront ouverts. Si le DMP a pu être présenté comme un outil de maîtrise des dépenses, il ne doit y avoir aucune ambiguïté sur la nature réelle du DMP : le DMP est d'abord et avant tout un grand projet de santé publique, au service de la santé de nos concitoyens. »[408]

319. Comme l'avait rappelé la Ministre de la santé de l'époque, Roselyne BACHELOT, lors de son discours consacré à la relance du projet DMP, l'amélioration et la coordination des soins étaient les enjeux prioritaires de la mise en place du DMP.

Ces objectifs, clairement affichés dans les textes fondateurs du DMP, sont finalement classiques pour ce type de dossier partagé. Si nous prenons l'exemple du dossier communiquant en cancérologie, l'objectif est bien d'améliorer la prise en charge globale des patients atteints de cancer. De même, le Dossier Pharmaceutique a bien pour enjeu de mieux coordonner les prescriptions afin d'éviter les interactions médicamenteuses. Toutefois, la particularité du DMP tient à sa volonté de couvrir l'ensemble de la prise en charge du patient, peu importe les spécialités concernées. C'est bien là que réside le caractère à la fois innovant et ambitieux de cet outil. Comme le soulignait à juste titre Caroline ZORN-MACREZ : « *il y a là un nouveau schéma de rationalisation du système de soins par le partage de données de santé grâce à des dossiers utiles aux soins* »[409].

320. Au-delà de cet objectif se dessine la volonté de faire coopérer l'ensemble des acteurs de la prise en charge d'un patient. Car c'est bien par cette coopération que passe la coordination et donc l'amélioration des soins. Le DMP, en étant présenté comme source d'une information diversifiée, complète et partagée, est positionné comme l'outil nécessaire à la

[408] Discours prononcé à l'occasion du colloque consacré à la relance du DMP, 9 avril 2009, disponible sur [http://sante.gouv.fr]. Consulté le 15 janvier 2015.
[409] ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit.*, p. 306.

bonne coopération des professionnels de santé, peu importe leur spécialité ou leur lieu de travail.

321. Néanmoins, il est rapidement apparu que ce sont moins les difficultés techniques ou budgétaires qui ont posé le plus de problèmes au développement du projet, que la barrière de la culture médicale, qui n'est pas forcément celle du partage de l'information. En effet, le positionnement des professionnels de santé face au DMP est original : contrairement aux dossiers médicaux traditionnels, que le professionnel va créer, alimenter et conserver, le DMP est conçu pour le patient et non pour le professionnel qui sera principalement amené à l'alimenter. Il s'agit ici d'un bouleversement des pratiques habituelles des professionnels. Dans le milieu hospitalier, ce choc des cultures est d'autant plus flagrant. De fait, les établissements de santé ont la particularité, du fait des activités variées, de produire un nombre considérable de données de santé diverses et variées. Ainsi, afin de donner vie le plus rapidement possible au DMP lors du programme de relance de 2009, il avait été décidé de mettre l'accent sur l'alimentation des dossiers par les professionnels du secteur hospitalier : ceux-ci ont alors pu être frustrés par cette vision restrictive du rôle qui leur était accordé.

322. Nous pensons que cet état d'esprit illustre bien les attentes peut-être trop élevées du législateur vis-à-vis du DMP. En effet, il nous semble qu'il aurait peut-être été plus opportun de laisser au DMP la vocation première de tout dossier médical, à savoir être un outil professionnel. Bien que les professionnels de santé ne soient pas contre l'idée d'être transparent vis-à-vis de leurs patients, il nous semble qu'il ne faut pas confondre outil de travail et outil d'information. En laissant une part très importante au patient dans le DMP, les professionnels ont pu se sentir dépossédés de ce qui aurait pu être un outil de travail consacré au partage de l'information et à la coordination des soins.

2) La sécurité de l'outil, une priorité

Dès le lancement du projet, la sécurité de l'outil a été une des priorités affichée afin, d'une part, de s'assurer que l'intégrité et la confidentialité des données soient conservées et, d'autre part, que les utilisateurs aient une pleine confiance dans l'outil.

323. En ce qui concerne l'hébergement du DMP, après quelques tâtonnements, c'est la piste de l'hébergeur unique qui a été finalement retenue. Cet hébergeur, en réalité consortium de plusieurs entreprises, a été agréé selon les modalités exigées par l'article L. 1111-8 du Code

de la santé publique et du décret hébergeur. De même, l'accent a été mis sur la traçabilité au sein du DMP. Ainsi, tous les accès sont tracés, qu'il s'agisse de la consultation d'un document, ou de son ajout. Le patient va ainsi pouvoir identifier quel professionnel a eu accès à quel document. La date et l'heure sont également tracées. Par ailleurs, selon les dispositions de l'article R. 1111-31 du Code de la santé publique, le patient, titulaire du dossier, mais également son médecin traitant, les professionnels de santé auxquels le patient aurait confié les mêmes droits que le médecin traitant et les professionnels auteur des informations faisant l'objet des traces peuvent y accéder.

324. Le DMP a surtout permis de donner une impulsion à la mise en place de l'Identifiant National de Santé (INS). En effet, l'article L. 1111-8 du Code de la santé publique prévoyait les dispositions suivantes : « *un identifiant de santé des bénéficiaires de l'assurance maladie pris en charge par un professionnel de santé ou un établissement de santé ou dans le cadre d'un réseau de santé défini à l'article L. 6321-1 est utilisé, dans l'intérêt des personnes concernées et à des fins de coordination et de qualité des soins, pour la conservation, l'hébergement et la transmission des informations de santé. Il est également utilisé pour l'ouverture et la tenue du dossier médical personnel institué par l'article L. 161-36-1 du Code de la sécurité sociale et du dossier pharmaceutique institué par l'article L. 161-36-4-2 du même Code. Un décret, pris après avis de la Commission nationale de l'informatique et des libertés, fixe le choix de cet identifiant ainsi que ses modalités d'utilisation* ».

Cet identifiant, censé regrouper l'ensemble des identifiants qui existent au sein des différents systèmes d'information de santé, a été instauré par la loi du 30 janvier 2007. Considéré par certains auteurs[410] comme étant une donnée de santé à part entière et donc, à ce titre devant bénéficier des protections mises en place par la loi Informatique et Liberté, l'INS a donné lieu à de nombreux débats concernant sa composition. La question s'est d'abord posée de savoir si l'INS pouvait être le Numéro d'Inscription au Répertoire de l'INSEE (NIR – couramment appelé numéro de sécurité sociale). En effet, plutôt que de créer de toute pièce un nouveau numéro, ce qui, en plus de représenter un coût financier et humain non négligeable, pouvait présenter des failles en termes de sécurité, les maîtres d'œuvre du projet

[410] *V.* notamment en ce sens HEBERT, Sophie. « L'identité sanitaire », *RGDM*, 2007, n° 24, pp. 121-138 ; ZORN-MACREZ, Caroline, « Données de santé et secret partagé », *PUN*, 2010, p. 271. En l'espèce l'auteur se base sur les réflexions menées par le groupe de l'article 29 sur la nature des données contenues au sein des DME pour arriver à la conclusion que l'INS est une donnée sensible au sens de la loi Informatique et Libertés.

(à l'époque le GIP-DMP) ont alors avancé l'idée d'utiliser le numéro de sécurité sociale. Toutefois, cette idée a subi de vives critiques de la part notamment des associations de défenses des consommateurs.

La CNIL, quant à elle, avait écarté une telle possibilité dans sa délibération du 20 février 2007[411], estimant que cette utilisation serait de nature à « *altérer les liens de confiance entre les professionnels de santé et les patients, ceux-ci pouvant légitimement s'interroger sur les risques d'accès non contrôlés à leur dossier médical par cet identifiant largement connu* ».

325. Toutefois, la CNIL, consciente des désagréments et de la lourdeur induite par la création d'un nouvel identifiant, avait suggéré dans cette même délibération la possibilité pour créer l'INS de partir du numéro NIR mais transcodé selon des techniques connues d'anonymisation. Cela aboutissant à un numéro non signifiant. L'ASIP santé, chargé de reprendre les activités du GIP-DMP et notamment la mise en place de l'INS, a suivi cette voie dans la conception de l'INS. Le législateur, constatant que « *l'adoption d'un dispositif unique et commun d'identification des patients est une condition nécessaire de l'interopérabilité des systèmes d'information des professionnels et établissements de santé et donc de leur capacité à échanger et partager facilement et de façon sécurisée (absence d'erreur sur le patient) les données médicales nécessaires à la prise en charge des patient* »[412], a définitivement réglé le problème en faisant du NIR le seul identifiant de santé utilisable[413]. En effet, pour le législateur, le NIR présente le double l'intérêt d'être robuste et de permettre une généralisation rapide.

326. Désormais, « *l'identifiant du dossier médical partagé est l'identifiant national de santé, mentionné à l'article L. 1111-8-1* »[414]. Par ailleurs, les conditions d'utilisation du NIR en tant qu'identifiant national de santé ont été précisées par le décret n° 2017-412 du 27 mars

[411] Délibération CNIL n° 2007-036 du 20 février 2007 portant avis sur deux projets d'arrêtés relatifs, d'une part, aux spécifications physiques et logiques de la carte d'assurance maladie et aux données y étant contenues et, d'autre part, aux conditions d'émission et de gestion des cartes d'assurance maladie.
[412] Etude d'impact du projet de loi relatif à la santé, p. 187.
[413] L'article 193 de la loi de modernisation de notre système de santé vient créer un article L. 1111-8-1 au Code de la santé publique, qui prévoit : « *le numéro d'inscription au répertoire national d'identification des personnes physiques est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, dans les conditions prévues à l'article L. 1110-4* ».
[414] Article R. 1111-33 du Code de la santé publique.

2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé[415].

B. Des lacunes certaines

327. Malgré les réformes et relances entourant le projet, de nombreuses inconnues subsistent aujourd'hui encore, faisant du DMP un outil mouvant et parfois flou (1). Quant aux droits des patients, ceux-ci sont incertains, malgré l'affichage positif que le législateur a souhaité donner (2).

1) Le DMP, un outil à géométrie variable

328. La question du contenu du DMP a longtemps posé problème. Lors de la création de l'outil en 2004, le Code de la sécurité sociale prévoyait les dispositions suivantes : « *chaque bénéficiaire de l'assurance maladie […] dispose d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L. 1111-8 du même Code* ». Ainsi, le législateur renvoyait aux données visées à l'article L. 1111-8 du Code de la santé publique, à savoir les « *données de santé recueillies à l'occasion d'actes de soins, de prévention ou de diagnostic* ». Or, cette référence était maladroite. En effet, comme nous avons pu le voir longuement lors d'un précédent paragraphe, la notion de données de santé n'a fait, pendant longtemps, l'objet d'aucune définition juridique. Celle finalement adopté par le Règlement Européen se montre quant à elle très large. Pourtant, il semble difficilement envisageable que le DMP puisse être un dossier "fourre-tout", véritable recueil exhaustif des données et informations relatives directement ou indirectement à la santé du patient. En effet, rappelons que le but initial du DMP était bien d'améliorer la coordination des soins. Dès lors, seuls les éléments permettant d'atteindre ce but devraient figurer en son sein, ni plus, ni moins. Face à un dossier surchargé, les professionnels ne seraient plus en capacité de retrouver les éléments utiles au suivi de leur patient.

[415] Décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé, *JORF* n°0075 du 29 mars 2017, texte n° 23.

329. Le rapport sur le Dossier médical personnel de 2007[416], relatif au bilan du DMP, soulignait que l'absence d'étude approfondie du contenu du DMP en amont de la création de l'outil a été une des erreurs majeures lors de la création du DMP. Même la note relative aux propositions de contenu, remise au ministre de la santé par le Docteur Jean-Marie PICARD[417], n'envisageait finalement que succinctement ce contenu. L'erreur serait d'envisager le DMP comme un dossier se voulant exhaustif, véritable « *réplique électronique d'une armoire de rangement* »[418]. Or, il est pourtant évident que ce dossier ne doit pas et ne pourra pas être exhaustif : ne doit pas pour les raisons exposées précédemment et ne pourra pas pour une raison très pratique : le contenu du DMP dépend de la capacité mais aussi de la volonté des professionnels à l'alimenter.

330. Alors que la loi HPST, initiatrice de la première relance du DMP, n'a apporté que peu d'éléments nouveaux quant au contenu du DMP, le décret du 4 juillet 2016[419] tente de régler cette difficulté, en créant au sein du Code de la santé publique, une sous-section consacrée au contenu du DMP. Un contenu *a minima* du dossier est désormais prévu par l'article R. 1111-30 du Code de la santé publique, permettant d'assurer un socle de documents commun à tous les DMP, ceux-ci ne risquant plus désormais d'être alimentés de manière disparate, selon le bon vouloir des professionnels de santé.

2) Les droits et devoirs des patients, un manque de clarté

331. Une des questions qui a été et, qui reste encore aujourd'hui régulièrement soulevée, est celle de la protection du secret médical dans le cadre de la mise en place d'un outil partagé avec un grand nombre de personnes et accessible via Internet. Dès l'origine du projet, le législateur avait bien prévu que le DMP soit instauré dans le respect du secret médical[420]. Dans l'absolu, le fonctionnement du DMP ne change rien aux règles relatives au secret médical. D'ailleurs, nous n'adhérons pas à l'affirmation de Marie-Catherine CHEMTOB-CONCE qui considère que « *la mise en œuvre du DMP […] permet de mieux protéger le*

[416] Rapport sur le dossier médical personnalisé, Inspection générale des finances, Inspection générale des Affaires sociales, Conseil générale des Technologies de l'Information, novembre 2007.
[417] PICARD, Jean-Marie. « Dossier Médical Personnel : proposition de contenu », enquête qualitative menée auprès de professionnels sous l'égide de la CNAMTS.
[418] Rapport sur le Dossier médical personnalisé, Inspection générale des finances, Inspection générale des Affaires sociales, Conseil générale des Technologies de l'Information, novembre 2007, p. 25.
[419] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, *op. cit.*
[420] Article L. 161-36-1 alinéa 1 du Code de la sécurité sociale.

secret médical, le secret professionnel »[421]. Au mieux le DMP ne met pas plus en danger le secret professionnel qu'un autre dossier informatisé, mais en aucun cas il n'est possible d'envisager qu'un dossier médical informatisé, pouvant être accessible par un nombre important de professionnels de santé différents, sera plus protecteur du secret médical. De plus, l'outil en lui-même, comme tout dossier informatisé, est forcément vecteur de risques accrus en termes de sécurité et de violation de la confidentialité des données.

332. Néanmoins, en ce qui concerne la sécurisation technique du DMP, l'hébergeur du DMP offre d'importantes garanties, exigées dès le lancement de l'appel d'offre et confirmée suite à l'obtention de l'agrément hébergeur. A l'heure actuelle, aucune autre garantie technique supplémentaire ne pourrait être apportée et en cela, nous pouvons affirmer que le DMP apporte une forte protection du secret professionnel. Cependant, il ne faut pas oublier que le DMP créé une nouvelle forme de partage des données de santé. Dans les faits, force est de constater que de nombreux professionnels auront, avec cet outil, potentiellement accès à de nombreux documents issus de la prise en charge du patient. Il est donc nécessaire de se préoccuper de la protection réservée à la confidentialité des données.

333. Un autre problème, intimement lié à la problématique relative au secret professionnel, avait été soulevé lors de la saisine du Conseil constitutionnel d'un recours contre la loi relative à l'assurance maladie : pour les auteurs de la saisine, les dispositions relatives au DMP méconnaissaient le droit au respect de la vie privée. Le Conseil Constitutionnel, dans sa décision n° 2004-504 du 12 août 2004[422], avait toutefois déclaré les dispositions conformes à la constitution, estimant que les garanties présentées par le législateur afin d'assurer le respect du secret professionnel et de la confidentialité des données étaient des garanties suffisantes pour préserver le droit au respect à la vie privée.

---

[421] CHEMTOB-CONCE, Marie-Catherine. « Dossier Médical Personnel et Dossier Pharmaceutique », Gazette du palais, 2007, pp. 2-5.

[422] « *Considérant, en second lieu, que le dossier médical personnel sera élaboré « dans le respect du secret médical » ; qu'il résulte du renvoi à l'article L. 1111-8 du Code de la santé publique que l'hébergement des données et la possibilité d'y accéder seront subordonnés au consentement de la personne concernée ; que le traitement des données sera soumis au respect des dispositions de la loi du 6 janvier 1978 susvisée ; que l'hébergeur devra faire l'objet d'un agrément ; que l'accès au dossier par un professionnel de santé sera soumis à l'observation des règles déontologiques ainsi que des dispositions des articles L. 1110-4 et L. 1111-2 du Code de la santé publique, qui imposent notamment le respect de la vie privée et du secret des informations concernant le patient ; que l'accès au dossier médical en dehors des cas prévus par la loi sera puni des peines prévues à l'article 226-13 du Code pénal ; que ces sanctions s'appliqueront sans préjudice des dispositions du Code pénal relatives aux « atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques* ».

334. D'une manière générale, un tel dossier ouvre le débat sur la place accordée aux droits fondamentaux face aux enjeux politiques sanitaires et économiques que sont la coordination des soins et la maîtrise des dépenses de santé. Bien qu'abandonnée, l'idée d'une sanction financière sous la forme d'un non remboursement en cas de refus d'accès à sa DMP avait été pourtant validée par le Conseil constitutionnel, celui-ci reconnaissant la supériorité de la maîtrise des dépenses de santé sur finalement, le respect à la vie privée.

335. L'autre question relative aux droits des patients dans le cadre du DMP concerne la place accordée à son consentement. En effet, dans le cadre du DMP, le consentement du patient peut être multiple : le patient va devoir consentir à l'ouverture de son DMP, puis il va devoir "habiliter" les professionnels qui auront accès à ce dossier : il doit donc consentir à partager ses données de santé avec ces professionnels. En ce qui concerne le consentement à la mise en place de son DMP, cela ne pose pas de problème particulier. L'article L. 1111-14 du Code de la santé publique prévoit en effet les dispositions suivantes : « *le dossier médical partagé est créé sous réserve du consentement exprès de la personne ou de son représentant légal* ». Cette formulation, issue de la refonte du DMP introduite par la loi de modernisation de notre système de santé, a le mérite d'être beaucoup plus claire qu'auparavant. En effet, dans sa rédaction antérieure, l'article L. 1111-14 du Code de la santé publique ne prévoyait pas le consentement préalable du patient à la création de son DMP. Toutefois, les dispositifs techniques mis en place pour permettre la création du DMP permettent de s'assurer du consentement préalable du patient, celui-ci devant remettre sa carte vitale au professionnel qui se chargera de créer son DMP.

336. Concernant l'habilitation des patients et donc l'autorisation d'accès au DMP, plusieurs exceptions vont venir affaiblir le principe du consentement préalable du patient. Par principe, « *l'accès au dossier médical personnel des professionnels mentionnés au premier alinéa est subordonné à l'autorisation que donne le patient d'accéder à son dossier* »[423]. Il existe cependant des hypothèses dans lesquelles le consentement du patient ne sera pas nécessaire pour accéder à son DMP : en cas de risque immédiat pour une personne hors d'état d'exprimer sa volonté et en cas d'appel d'urgence (appels au centre 15). Toutefois ces deux

[423] Article L. 1111-15 du Code de la santé publique.

hypothèses, qui reprennent finalement la classique exception de l'urgence vitale, sont dans le cas du DMP assez bien verrouillées. Introduites par la loi de 2007[424], ces dispositions prévoient une exception à l'exception. En effet, un médecin peut accéder au DMP sans que le patient ne l'ai autorisé, et ce en cas de risque immédiat ou en cas d'appel aux services d'urgences, sauf si cette personne avait auparavant manifesté son opposition expresse à ce que son dossier soit consulté ou alimenté dans une telle situation. Ainsi, une opposition expresse rendra le DMP inaccessible, peu importe les circonstances.

337. Nous estimons que ces dispositions, certes soucieuses de garantir la sécurité des données et le respect du droit des patients, ne sont toutefois pas forcément dans l'intérêt de ce dernier. Il nous semble en effet que le principe de sauvegarde de la vie humaine doit rester une priorité par rapport à d'autres droits fondamentaux et nous déplorons qu'une opposition expresse puisse verrouiller totalement l'accès au DMP, accès qui, dans certaines situations, pourrait être la seule source d'informations.

338. Enfin, le DMP introduit la possibilité, pour un professionnel qui aurait été habilité par un patient, de recueillir son consentement afin qu'un autre professionnel à qui il pourrait être opportun de confier une partie de la prise en charge, puisse accéder également au DMP. Finalement rien de très original dans cette mesure qui est directement inspirée des modalités de partage d'informations entre professionnels de santé prévues au sein de l'article L. 1110-4 du Code de la santé publique[425].

§2. Un outil à l'avenir incertain

339. A l'heure actuelle, le bilan des dix premières années du DMP est plus que mitigé. Dès lors, l'avenir de cet outil ambitieux se présente assez mal. En effet, le DMP est victime de ses premiers échecs et, de ce fait, est mal perçu par ses utilisateurs, quels qu'ils soient (A).

---

[424] Loi n° 2007-127 du 30 janvier 2007 ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le Code de la santé publique, *JORF* n°27 du 1 février 2007, p. 1937.

[425] L'article L. 1110-4 prévoit les dispositions suivantes : « *le partage, entre des professionnels ne faisant pas partie de la même équipe de soins, d'informations nécessaires à la prise en charge d'une personne requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée, dans des conditions définies par décret pris après avis de la Commission nationale de l'informatique et des libertés* ».

Finalement, malgré les relances diverses depuis sa création, le DMP peine à trouver sa place et il est légitime de se demander si cet outil n'est finalement pas voué à l'échec (B).

A. Un outil mal perçu

340. L'ensemble des rapports qui ont pu être rédigés au sujet du DMP pointent la même faille : le manque de confiance et d'adhésion à l'outil, que cela soit de la part des professionnels ou des patients. Les professionnels de santé, et plus particulièrement les professionnels du milieu hospitalier ne cachent pas leurs doutes et leur hostilité face à ce projet : leurs craintes sont nombreuses et portent tant sur la charge de travail induite par ce nouvel outil que sur les conséquences qu'il aura sur leur pratique quotidienne et leur responsabilité. Nous pouvons en effet constater que l'introduction du DMP dans la pratique médicale ne se fera pas sans conséquence sur la responsabilité des professionnels de santé (1). Mais la fonctionnalité qui reste la plus appréhendée, et donc source de doute, est le droit de masquage des données (2) accordé au patient.

1) DMP et responsabilité

Plusieurs questions se sont posées avec l'introduction du DMP quant à la responsabilité des praticiens.

341. La première concerne les nouvelles responsabilités pesant désormais sur les professionnels du fait de leurs obligations en lien avec l'ouverture d'un DMP. En effet, les dispositions du Code de la santé publique prévoient que l'usager doit donner un consentement exprès à l'ouverture de son DMP. Ainsi, cela induit en toute logique, pour le professionnel de santé qui sera amené à accompagner le patient dans l'ouverture de son dossier, de lui diffuser une information claire à ce sujet dans un premier temps, puis recueillir son consentement dans un second temps. Face à ces nouvelles obligations, l'ASIP santé a toutefois créé des brochures d'information délivrables aux patients, afin de faciliter la tâche des professionnels. De même, l'outil informatique, support du DMP, prévoit une case qui doit être cochée par le professionnel afin de valider virtuellement le consentement du patient. Enfin, l'outil informatique stocke et conserve la trace et la date d'obtention du consentement. Ainsi, dans l'hypothèse d'un contentieux au cours duquel un patient prétendrait ne pas avoir consenti à l'ouverture de son DMP, le professionnel pourrait se défendre en utilisant un faisceau

d'indices, composé de l'ensemble de ces outils. Bien qu'en théorie possible, ce genre de contentieux n'est donc pas, d'après nous, à craindre de la part du professionnel.

342. La deuxième réflexion à avoir en termes de responsabilité concerne l'obligation d'information classique dont tout professionnel est redevable vis-à-vis de son patient En effet, le DMP permettrait-il d'alléger l'obligation d'information qui pèse sur les professionnels de santé ? Cette théorie est celle soutenue par certains auteurs, pour qui le DMP en diffusant une meilleure information au patient, permettra d'éviter les incompréhensions autour desquelles se cristallisent parfois les contentieux. C'est la théorie avancée notamment par Jérôme CAYOL[426]. Mais peut-on réellement considérer que l'obligation d'information du patient sera correctement remplie une fois le DMP complété. Nous pensons que ce n'est pas le cas et qu'il serait même dangereux d'accepter une telle possibilité. En effet, comme l'exige le Code de la santé publique, et comme le rappelle régulièrement la jurisprudence, l'information dispensée se doit d'être claire, loyale et surtout compréhensible. Or, même si l'information contenue au DMP peut remplir les deux premiers critères, seule une discussion entre le professionnel et son patient permettra de s'assurer que l'information dispensée a été adaptée au degré de compréhension du patient et a bien été acquise.

343. Par ailleurs, comme cela est régulièrement souligné par les professionnels, le patient ne sera pas toujours capable de gérer l'abondance de ces informations et surtout la réalité, parfois très dure, de certaines d'entre elles. Il nous semble donc que l'obligation restera la même. Peut-être sera t-elle-même renforcée, car le professionnel devra également s'assurer que le patient a compris et intégré d'une part les informations reçues, mais également les informations présentes sur son dossier.

344. Enfin, des questions quant aux responsabilités pesant sur les professionnels au sujet de la tenue et de la consultation du DMP se posent. Concernant la tenue du DMP d'abord, nous le savons, les professionnels de santé ont pour rôle de l'alimenter. Mais quelles seraient les conséquences s'ils ne le font pas ou le font mal ? Se pose également la question de la qualité de l'information déposée au sein du DMP et des répercussions en termes de responsabilité. Nous retrouvons finalement ici le raisonnement relatif au contenu du dossier : enregistrer

[426] CAYOL, Jérôme. « Réflexions sur la responsabilité médicale à la suite de l'introduction du dossier médical personnel », *Médecine et droit*, 2006, pp. 85-87.

l'intégralité des informations de santé d'un patient au sein du DMP risquerait de faire se perdre l'information utile et nécessaire dans une masse de données insignifiantes. Cela pourrait alors entrainer un défaut ou un retard dans la prise en charge du patient qui lui serait préjudiciable. Qui serait alors responsable ? La même question peut être posée au sujet de la qualité de l'information. Comme le soulignait à juste titre Gilles LUCAZEAUX, procureur général près la Cour d'Appel de Nancy, «*qu'en est-il du jour où l'on s'interrogera sur la qualité du dossier tenu ? S'il n'est pas de bonne qualité, ne va-t-on pas ouvrir la boite de Pandore, c'est-à-dire d'éventuelles responsabilités ?* »[427].

Dans l'hypothèse d'un dossier mal géré, finalement le droit commun trouverait à s'appliquer : pour que la responsabilité pénale du praticien soit retenue, il serait nécessaire d'apporter la preuve d'une faute caractérisée, c'est-à-dire une faute dont le médecin ne pouvait pas ignorer les conséquences et leurs risques, et d'un préjudice du fait de la mauvaise tenue.

345. Une meilleure connaissance du patient par le médecin, de fait de l'accessibilité à certaines données qui lui auraient été cachées auparavant, entrainerait-il une responsabilité accrue des praticiens ? Certes, cela est parfaitement envisageable. Toutefois, cela induit-il une obligation de consultation du DMP ? Un professionnel pourrait-il être fautif du fait de la non consultation du DMP alors qu'il y avait accès ? Nous pensons en effet que, comme dans l'hypothèse de la non consultation d'un dossier médical par un praticien, ou en cas d'interrogatoire incomplet, le praticien qui ne consulterait pas le DMP auquel il aurait accès, faillirait à son obligation de moyens. Ainsi la responsabilité civile de l'établissement de santé ou celle du médecin pourrait être engagée. Toutefois, il est certain qu'en ce qui concerne la mise en œuvre de la responsabilité médicale, responsabilité pour faute, les règles restent inchangées. Tout au plus, le DMP permettra au patient d'établir plus facilement le lien de causalité entre le préjudice subi et la faute du professionnel.

346. Plusieurs obligations nouvelles vont peser sur le professionnel : obligation légale d'informer le patient au sujet du DMP et d'obtenir son consentement pour la création du dossier. Comme le rappelle l'ASIP santé à juste titre, c'est au patient qui invoquerait un

[427] LUCAZEAUX, Gilles. « La justice pénale et les informations médicales», *RGDM*, n° 20, 2006, pp. 189-194.

manquement, d'apporter la preuve. Le législateur a par ailleurs prévu une traçabilité de l'ensemble des actions effectuées sur le DMP, accessibles par le patient. L'articulation des règles concernant le consentement d'accéder à son dossier, donné par un patient à un professionnel, avec les règles relatives au secret partagé doivent être mises à plat. Cette articulation n'est pas si simple qu'il y parait et, contrairement à une partie de la doctrine, comme Marie-Catherine CHEMTOB-CONCE par exemple, qui considère que « *le DMP ne crée aucun changement quant au secret médical* » et que « *la mise en œuvre du DMP ne change pas en soi la responsabilité médicale des professionnels de santé et des établissements de soin mais permet de mieux protéger le secret médical le secret professionnel et la vie privée du patient* » nous considérons, au contraire, que le DMP ouvre de nouvelles possibilités d'accès aux données de santé et fragilise ainsi la protection de celles-ci.

347. Finalement, la doctrine s'accorde en grande majorité pour souligner que le DMP ne changera strictement rien aux règles de responsabilités applicables.[428] Les règles ordinaires s'appliquent et le DMP ne sera finalement qu'un outil de plus dans la preuve de la responsabilité. Mais il faut toutefois souligner qu'il est aussi un outil en plus donc une source supplémentaire de mise en œuvre de la responsabilité des professionnels et ce, pour toutes les raisons évoquées précédemment.

2) La théorie du masquage

348. Depuis l'introduction de la possibilité, pour le patient, de masquer certaines informations vis-à-vis de certains professionnels, ceux-ci ont pu faire part de leurs craintes vis-à-vis du dispositif. Cette possibilité est prévue à l'article R. 1111-38 du Code de la santé publique qui prévoit que « *le titulaire peut décider que des informations le concernant contenues dans son dossier médical partagé ne soient pas accessibles aux professionnels de santé autorisés à accéder à son dossier. Ces informations restent cependant accessibles au professionnel de santé qui les a déposées dans le dossier médical partagé et aux professionnels de santé visés à l'article R. 1111-43. Cette décision est modifiable à tout moment par le titulaire* ».

[428] *V*. en ce sens PY, Bruno. « Conclusions sur les aspects juridiques », *RGDM*, n° 20, 2006, p. 239.

349. Le décret du 4 juillet 2016[429] a acté de manière définitive cette possibilité, sans apporter pour autant beaucoup de précisions à ce sujet. D'une manière générale, cette notion de masquage de certaines données a été longuement débattue avec l'ensemble des acteurs du DMP. En pratique, le "masquage", terme fortement connoté il nous semble, n'est que la traduction informatique du colloque singulier qui existe entre le patient et un professionnel de santé. En effet, lors d'une consultation, le patient est libre de choisir de cacher des informations à son praticien. Or, ce dernier en a parfaitement conscience et ne se contente pas des informations que le patient sera enclin à lui donner. Il était donc normal d'accorder cette même faculté au patient au sein de son DMP. A ce sujet, le rapport FAGNIEZ[430] soulignait le risque d'affaiblissement du colloque singulier du fait de la consultation du DMP, le professionnel se basant uniquement sur les informations contenues et ne cherchant plus à interroger le patient : en cela, le masquage de certaines données va préserver ce dialogue précieux. De plus, au titre de l'article L. 1110-4 du Code de la santé publique, le patient a le droit de s'opposer à ce que deux professionnels échangent des données le concernant : cette possibilité lui est donnée au sein du DMP à travers le masquage.

350. Pour notre part, nous pensons que le masquage est simplement la traduction informatique de la liberté accordée au patient de cacher des choses au professionnel qui le prend en charge. Toutefois, bien que cette fonctionnalité soit très respectueuse des droits des patients, il nous semble qu'elle aille finalement à l'encontre de l'enjeu premier du DMP qui est le partage d'informations pour une meilleure coordination des soins. En effet, dans l'absolu, un patient pourrait choisir de ne donner accès qu'aux documents que le professionnel a déposé au sein du DMP, lui masquant l'intégralité des autres données. Or, ceci diminuerait clairement l'intérêt du DMP.

351. Nous pensons qu'il aurait peut-être été plus efficace d'abandonner cette fonctionnalité de masquage au profit d'une validation de la part du patient des documents que le professionnel peut partager au sein du DMP. Une autre solution, et c'est une des propositions formulées au sein du rapport FAGNIEZ, aurait été de tenter d'éviter le masquage « solitaire » et d'inciter les patients à se faire accompagner par un professionnel de confiance, par exemple

---

[429] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, *JORF* n°0155 du 5 juillet 2016, texte n° 20.

[430] FAGNIEZ, Pierre-Louis, « Le masquage d'informations par le patient dans son DMP », rapport au ministre de la santé et des solidarités, 30 janvier 2007.

leur médecin traitant dans le choix des documents qu'ils souhaitent masquer, une sorte « *d'omission partagée* »[431].

B. Un projet voué à l'échec ?

352. A l'heure actuelle, le projet DMP n'affiche pas un bilan positif. Le dernier rapport sur le sujet a été rédigé par la Cour des comptes en juillet 2012 et le bilan financier qu'elle y dresse révèle la situation critique du projet (1). Toutefois, le législateur a tenu, à l'occasion d'une ultime refonte, à relancer le projet, sous l'égide, cette fois-ci, de la CNAMTS (2)

1) Le coût important du DMP

353. Présenté lors de son lancement comme un outil censé diminuer les coûts de santé et donc favoriser des économies pour l'assurance maladie, le DMP est bien loin d'avoir les effets escomptés à ce niveau. Pire encore, il est accusé de coûter beaucoup plus d'argent que ce qu'il n'a pour l'instant ou même ne pourra à terme amener comme économies, présentant pour certains « *un coût excessif pour un succès mitigé* »[432].

354. En juillet 2012 la Cour des comptes, saisie par le président de la commission des finances de l'Assemblée Nationale d'une demande d'enquête sur « *le coût du dossier médical personnel depuis sa mise en place* », a rendu un rapport dressant un bilan négatif à ce sujet[433]. Le chiffre avancé par la Cour des comptes dans son rapport s'élève à 210 millions d'euros dépensés entre 2004 et fin 2011, dont un quart en expérimentation. Toutefois, la Cour des comptes apporte rapidement un bémol important à ce chiffre qui ne tient pas compte de l'ensemble des coûts induits par le projet. Plusieurs défaillances, liées de manière plus ou moins directe aux aspects financiers du projet, sont pointées par le rapport. L'absence d'évaluation médico-économique, ainsi que l'absence de définition d'une stratégie nationale en termes de systèmes d'information de santé sont présentées comme des lacunes et donc de grosses erreurs stratégiques de la part des pouvoirs publics. De même, l'absence flagrante de suivi des coûts du projet ainsi que l'ignorance des coûts induits sont autant de risques lourds

---

[431] FAGNIEZ, Pierre-Louis, « Le masquage d'informations par le patient dans son DMP », *op. cit.*, p. 12.
[432] Article paru sur « Le Monde santé », disponible sur [http://www.lemonde.fr]. Consulté le 10 février 2015.
[433] Cour des comptes, « Le coût du dossier médical personnel depuis sa mise en place », communication à la commission des finances de l'Assemblée Nationale, Juillet 2012.

selon la Cour pour le bon aboutissement du projet. Finalement, nous partageons pleinement l'avis de la Cour des comptes qui considère que « *ces défaillances attestent […] d'une absence particulièrement anormale et préjudiciable de stratégie et d'un grave défaut de continuité de méthode dans la mise en œuvre d'un outil annoncé comme essentiel à la réussite de profondes réformes structurelles* »[434].

355. Depuis ce rapport, les détracteurs du projet n'en finissent pas d'invoquer des chiffres beaucoup plus importants. Ainsi, en janvier 2014, la somme de 500 millions d'euros a été avancée dans un article publié au sein du journal le Parisien[435]. Cette somme serait issue d'un document interne du Conseil national de la qualité et de la coordination des soins. L'ASIP santé, alors encore en charge de la gestion du DMP à l'époque, avait souhaité rectifier ces différentes informations qu'elle qualifie d'erronées. Ainsi, dans un document disponible sur leur site Internet[436], le groupement, se basant sur des données qu'elle qualifie d'exactes, documentées et vérifiées, avance des sommes très différentes. Tout d'abord, en ce qui concerne la phase initiale de recherche et de développement (phase d'expérimentation allant de 2005 à 2008), l'assurance maladie aurait versé au groupement en charge du projet (à l'époque le GIP DMP) la somme totale de 92 millions d'euros, via le fonds d'aide à la qualité des soins de ville (FAQSV) jusqu'en 2007, le fonds d'intervention de la qualité et de la coordination des soins (FIQCS) à partir de 2008, et le fonds national de gestion administrative (FNG) de la Caisse nationale d'assurance maladie des travailleurs salariés (CNAMTS), étant entendu que 90 millions d'euros ont été affecté à la préparation de la conception. Toutefois, ces chiffres ne concordent pas avec ceux avancés par la Cour des comptes dans son rapport de 2012, qui pour sa part avançait la somme d'environ 70 millions d'euros.

En ce qui concerne la phase qualifiée de phase de construction et d'amorçage par l'ASIP, celle-ci se rapporte aux chiffres de la Cour des comptes : entre 2010 et 2013, 97 millions d'euros auraient servis à financer le DMP (sur les 152 millions d'euros versés à l'ASIP). Cette information nous amène à formuler deux remarques. La première concerne l'année 2009, passée sous silence par l'ASIP santé. Bien qu'entre 2008 et 2009, le projet a

---

[434] *Id*. p. 11.
[435] « Dossier médical personnel : un demi-milliard pour rien », *le Parisien*, 4 janvier 2014, disponible sur [http://www.leparisien.fr]. Consulté le 6 février 2017.
[436] Chiffres disponibles sur [http://esante.gouv.fr]. Consultés le 10 février 2015.

pris un nouveau tournant[437], les financements n'ont pas été stoppés pour autant. La Cour des comptes annonce pour cette année-là la somme de 24 millions d'euros versés dont 20 millions alloués au DMP.

356. Notre seconde réflexion concerne la justification de ces chiffres. L'ASIP les présente comme étant ceux de la Cour des comptes. Or, dans son rapport, la Cour précise que les sommes annoncées comme étant affectées au DMP sur le total versé par l'assurance maladie sont les sommes présentées comme tel par l'ASIP. L'ASIP tente habilement de justifier les chiffres qu'elle avance et de leur fournir un caractère officiel qui n'existe pas réellement. Alors que la Cour des comptes annonçait la somme de 210 millions d'euros à fin 2011 ; l'ASIP estime que seuls 187 millions ont été réellement alloués au projet au 31 décembre 2013. Cette différence s'explique par la méthode retenue par l'ASIP santé. En effet, celle-ci a fait le choix ne pas associer au coût du DMP des coûts d'actions conduites au niveau régional, alors que la Cour les considère justement comme étant à comptabiliser.

357. Finalement, comme la Cour des comptes le soulignait à juste titre, un véritable chiffrage du coût du DMP se révèle quasiment impossible. Il semble en effet difficile de savoir ce que l'on considère comme entrant dans le champ du coût imputable au DMP : à ce sujet les différents acteurs ne sont clairement pas d'accord. Par ailleurs, le manque total de suivi et de management du projet en termes de finances ne permet pas une transparence suffisante et pourtant nécessaire pour dresser ce type de bilan. Ainsi, là où les détracteurs du projet annoncent des coûts colossaux qu'il est nécessaire de stopper, les fervents défenseurs du projet tentent de minimiser le coût réel. Dans tous les cas, nous estimons déplorable que le montant total des fonds publics consacrés à un projet national aussi conséquent ne puisse être établi. Cela révèle une défaillance importante et préjudiciable dans la gestion des fonds publics.

2) Les bémols face à la relance de la loi de modernisation de notre système de santé

358. Face à l'impossibilité de généraliser le développement du DMP, le législateur s'est penché, dès 2011, sur les possibilités d'évolution envisageables pour ce dossier. Ainsi, un

[437] *V. Supra*. n° 306 à 309.

projet alternatif a d'abord été envisagé par la loi Fourcade[438] : le dossier médical implanté sur support portable numérique sécurisé. Une expérimentation, qui visait spécifiquement un échantillon d'assurés souffrant d'une affection de longue durée, devait être menée selon les termes de la loi avant le 31 décembre 2013. Toutefois, ce projet s'est conclu par un échec. En effet, dès 2012, la CNIL avait émis des doutes importants quant à la sécurité qui pouvait assurer un tel dispositif. Les limites techniques que pouvait présenter un tel support notamment en termes d'intégrité et de disponibilité des données mais aussi en termes de sécurité (possibilité de virus, notamment) avaient été pointées.

359. L'Association pour la promotion de l'informatique et de la communication en médecine (Apicem) avait toutefois tenté fin 2012 de lancer une expérimentation du dossier sur clef USB sans réussir pour autant à tenir l'échéance légale fixée au 31 décembre 2013, et la Ministre de la santé, Marisol TOURAINE, a refusé de prolonger ce délai. Elle avait d'ailleurs rappelé être défavorable à la prolongation de ce type d'expérimentation[439], précisant néanmoins s'engager à ce qu'un programme permettant d'aboutir au DMP 2 soit rapidement mis en place.

360. La refonte du DMP n'a finalement eu lieu qu'en 2016 avec la loi de modernisation de notre système de santé. Le législateur a opéré un virage majeur, qui, sur certains points, peut être considéré comme un retour en arrière : le Dossier Médical Personnel devient, dans sa version 2.0, Partagé. Changement de formulation lourde de sens puisque l'outil au service du patient devient désormais un service pour les professionnels de santé, le patient, qui en reste "titulaire" conservant le consentement à son ouverture et l'accès direct.

361. Autre retour en arrière : l'enjeu de ce dossier serait une nouvelle fois recentré sur la maîtrise des dépenses de santé. En effet, bien que la loi de modernisation de notre système de santé ne le présente pas de manière claire, en prévoyant un contrôle du projet par la CNAMTS et non plus par l'ASIP santé, le législateur affiche clairement la priorité donnée à l'outil. D'ailleurs, le contenu du DMP, prévu par l'article R. 1111-30 du Code de la santé publique,

---

[438]Loi n° 2011-940 du 10 août 2011 modifiant certaines dispositions de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, *JORF* n°0185 du 11 août 2011, p. 13754.

[439] Question écrite n° 48488, publiée au JO le 4 février 2014, p. 934, réponse apportée et publiée au *JO* le 17 juin 2014, p. 49223.

intègre les données de remboursement de l'assurance maladie, considérées comme étant nécessaires à la coordination des soins. Ce contrôle est critiquable à plusieurs niveaux. D'une part, nous pouvons légitimement nous poser la question de la possibilité, pour l'assurance maladie, de concilier ses missions propres, avec la gestion et la mise en place d'un dossier partagé, dont le contenu sera plus que sensible. D'autre part, et comme nous l'avons déjà souligné, il s'agit ici d'un revirement à la symbolique forte : le DMP n'est plus un outil de santé publique et les priorités ne sont plus les mêmes. Toutefois, face aux nombreuses critiques qu'a pu essuyer le projet, que ce soit en termes de gestion ou de financement, nous estimons que la décision de confier la conduite du projet à l'organisme qui en sera le principal financeur, relève du bon sens et permettra certainement de mener à bien le projet plus facilement, même si celui-ci s'éloignera de son essence initiale.

Conclusion de la section

362. Outil plein de promesses, le DMP n'a toutefois pas réussi, à ce jour, à atteindre les objectifs qui lui avaient été fixés. A sa décharge, nous ne pouvons que constater l'ambition démesurée du législateur dès le début du projet. Bien que les enjeux soient louables, les moyens qui lui ont été accordés (juridiques, financiers ou humains) n'étaient pas adaptés à l'ampleur de la tâche. A sa décharge, le DMP n'a pas rencontré le succès escompté auprès des professionnels de santé, et, à défaut d'alimentation, il a peu à peu perdu de son intérêt. Face aux critiques qui ne cessent de se développer, notamment sur le coût aujourd'hui encore obscur du DMP depuis 2004, le législateur a souhaité lui donner une dernière chance. Avec la loi de modernisation de notre système de santé, il tente donc le tout pour le tout, en confiant à la CNAMTS le soin de relancer de manière efficace ce dossier qui se fait attendre.

Conclusion du chapitre

363. Depuis plusieurs années, le développement des TIC en santé a amené les professionnels de santé et les établissements de santé à se doter de dossiers médicaux électroniques.

364. Face au développement de l'informatisation mais également aux nécessités accrues de partage de l'information entre les professionnels de santé et inspiré des expériences réussies de nos pays voisins, le législateur a souhaité, en 2004, mettre en place un dossier informatisé partagé national : le Dossier Médical Personnel était né. Présenté comme un complément des autres dossiers et se démarquant par plusieurs originalités et innovations (portail d'accès unique, accessibilité et contrôle de son dossier par le patient,…), le DMP avait des ambitions louables. Toutefois, très rapidement, cette ambition du législateur s'est retournée contre le projet, qui pâti, depuis dix ans, d'un manque d'encadrement juridique et managérial. Au fil des années, les acteurs ont alors perdu confiance dans l'outil jusqu'à récemment dénoncer son coût exorbitant. Le DMP est aujourd'hui considéré par certains comme un échec.

365. La loi de modernisation de notre système de santé, prévoyant une ultime relance du projet, sera peut-être la bouée de sauvetage du Dossier Médical, devenu Partagé. En modérant ses ambitions et en confiant la gouvernance du projet à un acteur qui a déjà participé à un projet d'informatisation des données de santé mené à bien[440], le législateur accorde au DMP toutes les chances dont il a besoin pour fonctionner.

[440]La CNAMTS fait partie du GIE SESAM-VITALE, en charge notamment, de la mise en place et du déploiement de la carte vitale.

Chapitre 2

L'utilisation des TIC dans la prise en charge du patient

366. Les Technologies d'Information et de la Communication ont apporté de nouvelles possibilités de prise en charge du patient. Avec elles, se sont donc développées de nouvelles pratiques médicales à distance, permettant notamment de réduire les inégalités d'accès aux soins pour certaines populations en difficulté, soit de par leur situation personnelle (par exemple les détenus ou les personnes âgées), soit de par leur situation géographique.

Ces pratiques, maintenant ancrées pour certaines d'entre elles depuis une vingtaine d'années, se sont récemment vues encadrées par le législateur (Section I), soucieux à la fois de préserver les droits des patients mais également d'éviter certaines déviances. Le développement de l'utilisation des TIC dans le cadre de la prise en charge du patient a cependant rendu plus complexes les règles applicables en matière de responsabilité médicale. En effet, ces pratiques induisent de nouveaux risques et font intervenir de nouveaux acteurs, rendant ainsi nécessaire la clarification des règles applicables en matière de responsabilité (Section II).

Section 1. La prise en charge à distance, un cadre naissant

367. La pratique de la médecine à distance n'est pas nouvelle. En effet, certains réseaux de télémédecine existent et fonctionnent depuis près de vingt ans. Ces pratiques ont d'abord consisté en du conseil téléphonique, ou des visioconférences, avant de se structurer, conduisant à la naissance de véritables réseaux de référence[441]. Pourtant, la notion de télémédecine a longtemps été dépourvue de définition juridique, la pratique n'étant absolument pas appréhendée par le droit. Ce n'est que récemment que le législateur s'est penché sur cette pratique pour l'encadrer (Paragraphe 1).

En revanche, il s'est intéressé bien plus tôt à la question de prescriptions médicales informatisées (Paragraphe2), souhaitant sécuriser la prise en charge médicamenteuse des patients.

§1. La télémédecine, une pratique ancienne récemment consacrée par le législateur

368. Le législateur est récemment venu s'intéresser à une pratique qui, pourtant, se développait depuis plus de vingt ans[442]. Ainsi, l'article 78 de la loi HPST, complété par le décret du 9 octobre 2010[443], ont posé les règles applicables aux activités de télémédecine. Toutefois, ce cadre, défini de manière stricte et circonscrite (A), s'ajoute au cadre général relatif aux droits des patients et à la protection de leurs données de santé, rendant la pratique de la télémédecine lourde à mettre en place (B).

---

[441] *V.* notamment en ce sens, TIERS, Gonzague. CAPON, Catherine. CLEMENTE, Hélène. « Télémédecine en région Nord-Pas de Calais », *ITBM-RBM*, 2000, 271-4, au sujet du réseau de télémédecine TELURGE, opérationnel depuis mai 1996.
[442] *Ibid.*
[443] Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine, *JORF* n° 0245 du 21 octobre 2010, texte n° 13.

A. Un cadre spécifique strictement défini par la loi HPST

369. L'article 78 de la loi HPST fixe le cadre actuel de la télémédecine. Cet article et son décret d'application viennent sécuriser la pratique de la télémédecine. Ce cadre, instituant une procédure préalable au développement de toute activité de télémédecine (2) présente également l'intérêt de venir définir légalement la télémédecine (1).

1) La télémédecine, seule pratique à distance légalement définie

a) Définition des différentes pratiques

370. Avec le développement de l'utilisation de TIC dans la pratique médicale s'est également développé un champ lexical relatif à l'exercice à distance de la médecine. Ainsi, il nous parait indispensable de définir certains termes, afin de les exclure de notre réflexion. En effet, il est régulièrement fait usage, et parfois de manière indifférenciée, des termes télésanté, e-santé, m-health ou encore e-health.

371. Dès 1998, l'Organisation Mondiale de la Santé affirmait la nécessité de distinguer la télésanté de la télémédecine, ce dernier terme devant être réservé aux seules actions cliniques et curatives de la médecine utilisant les TIC[444]. Comme le soulignait à juste titre Pierre LABORDES dans son rapport relatif à la télésanté[445], ce terme reste une notion imprécise. Pour lui, « *son champ d'application est plus vaste que celui de la télémédecine par sa vocation à couvrir, outre le domaine médical au sens strict, le domaine très large et divers du médico-social* »[446]. D'une manière plus précise, Pierre LABORDES tente de définir différentes pratiques qu'il considère comme appartenant au domaine de la télésanté. Pour le député, peuvent donc relever de la télésanté des activités telles que la téléinformation, la télévigilance, le télémonitoring, la télécollaboration, la téléprescription,...[447]. Ainsi, la télésanté se distinguerait assez clairement de la télémédecine.

---

[444] HAS. « Efficience de la télémédecine : état des lieux de la littérature internationale et cadre d'évolution », juillet 2013, p. 11, disponible sur [http://www.has-sante.fr]. Consulté le 15 mai 2017.
[445] LABORDES, Pierre. « La télésanté : un nouvel atout au service de notre bien-être », *La Documentation française*, octobre 2009.
[446] *Id*. p. 36.
[447] LABORDES, Pierre. « La télésanté : un nouvel atout au service de notre bien-être », *op. cit.*, p. 37.

L'exercice de définition se complique toutefois quand on en vient à définir les notions d'e-santé et de m-health. Cette difficulté provient essentiellement de confusions dans la traduction faite de ces notions. Ainsi, il n'est pas rare que le terme e-santé soit utilisé pour faire référence à l'activité de télésanté. C'est le cas par exemple de Pierre SIMON et Dominique ACKER qui, dans leur rapport relatif à la télémédecine, emploient ces deux termes de manière indistincte : « *les technologies du numérique appliquées à la santé couvrent le champ de la e-santé ou télésanté […]* »[448]. Or, initialement, le terme de "e-health", qui pourrait être traduit littéralement par "e-santé" a été utilisé par l'OMS pour faire référence aux « *activités, services et systèmes liés à la santé, pratiqués à distance au moyen des TIC, pour les besoins planétaires de promotion de la santé, des soins et du contrôle des épidémies, de l'épidémiologie, de la gestion et de la recherche appliquées à la santé* ». Cette définition est donc bien plus large que celle donnée pour la télésanté.

Dans ses travaux consacrés à l'encadrement juridique de la gestion électronique des données médicales, N'Da Brigitte ETIEN-GNOAN[449] s'appuie sur la définition proposée par Gunther EYSENBACH pour délimiter les contours de l'e-santé. Ainsi elle en déduit que :« *la e-santé ne s'inscrit pas dans une logique personnalisée de diagnostic ou de thérapie alors que la télésanté, même si elle consiste quelque fois en des transmissions d'informations ou de formation, elle est plus marquée par des actes ou services adressés à des personnes de manière personnelle* »[450]. La notion de "e-santé" serait donc un terme permettant de désigner des pratiques plus génériques et moins personnalisées que sont la télésanté ou la télémédecine.

Enfin, le terme "m-health" désigne la mobile-health ou santé-mobile. Il s'agit des services d'informations mais également de recueil d'informations de santé via des objets connectés afin de dispenser des conseils santé personnalisés. Cette pratique en plein essor ne fera pourtant pas l'objet de notre étude ici et nous ne pousserons donc pas plus loin l'exercice de définition. En effet, il s'agit d'une pratique qui ne touche aujourd'hui que de très loin les

---

[448] SIMON, Pierre. ACKER, Dominique. «La place de la télémédecine dans l'organisation des soins », novembre 2008, p. 8.
[449] ETIEN-GNOAN, N'Da Brigitte. « L'encadrement juridique de la gestion électronique des données médicales », décembre 2014, thèse pour obtenir le grade de docteur en droit, disponible sur [http://pepite-depot.univ-lille2.fr]. Consulté le 15 mai 2017.
[450] *Id*. p. 224.

établissements publics de santé et c'est pourquoi nous préférons l'exclure de notre champ d'étude.

372. Cet exercice terminé, nous pouvons nous concentrer sur la notion de télémédecine, seule notion dans le domaine ayant une réelle existence et définition légale.

L'article 78 de la loi HPST vient créer au sein du titre premier, du livre troisième de la sixième partie du Code de la santé publique[451], un chapitre six, intitulé « Télémédecine ». Celle-ci est définie comme *« 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* ». Toujours selon l'article L. 6316-1 du Code de la santé publique, la télémédecine : « *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.* ». Avec cette définition, le législateur fait donc de la télémédecine un acte médical à part entière, clairement défini d'une part, et juridiquement consacré d'autre part.

b) Les cinq actes de télémédecine

373. Le décret du 9 octobre 2010 définit cinq actes relevant de la télémédecine. Dès lors, seules les pratiques correspondant à une de ces cinq définitions seront considérées comme des actes de télémédecine entrant dans le cadre légal (sous réserve, bien entendu, de répondre également aux autres contraintes du décret[452]). La liste de ces actes a été codifiée au sein de l'article R. 6316-1 du Code de la santé publique.

374. Le premier acte de télémédecine est la téléconsultation, acte ayant pour objet de permettre à un professionnel médical de donner une consultation à distance à un patient. Un professionnel de santé peut être présent près du patient et, le cas échéant, assister le professionnel médical au cours de la consultation. Le texte précise également que les psychologues peuvent également être présents auprès du patient.

---

[451] « Etablissements et services de santé »
[452] *V. Infra* : n° 377 à 381.

375. Le deuxième acte de télémédecine est la téléexpertise. Celle-ci a pour but de permettre à un professionnel médical de solliciter à distance l'avis d'un ou plusieurs professionnels médicaux en raison de leurs formations ou de leurs compétences particulières, sur la base des informations médicales liées à la prise en charge d'un patient. Cette pratique est finalement l'application aux TIC de la possibilité dont dispose le professionnel de pouvoir solliciter un confrère dans certains cas.

376. Le troisième acte visé par le décret du 9 octobre 2010 est la télésurveillance médicale. Cette pratique 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. L'enregistrement et la transmission des données peuvent être automatisés ou réalisés par le patient lui-même ou par un professionnel de santé. La quatrième pratique est la téléassistance médicale, permettant à un professionnel médical d'assister à distance un autre professionnel de santé au cours de la réalisation d'un acte.

Enfin, le législateur a également inscrit parmi les actes de télémédecine la réponse médicale apportée dans le cadre de la régulation médicale.

Seules ces cinq pratiques sont constitutives d'un acte de télémédecine.

2) Une procédure préalable stricte

377. Le décret du 9 octobre 2010 ne s'est pas contenté d'apporter des définitions, il a également instauré le cadre légal, conventionnel et financier dans lequel doit s'inscrire l'acte de télémédecine. Plusieurs exigences préalables au développement d'un projet de télémédecine doivent donc d'être respectées. Nous ne nous attarderons pas ici sur les règles de droit commun, applicables à l'exercice de la médecine d'une manière générale, qui vont s'opposer également à l'activité de télémédecine, ces éléments étant développés ultérieurement[453]. Nous préférons nous concentrer sur les règles propres à l'activité de télémédecine, édictées par le décret de 2010.

[453] *V. Infra.* n° 425 et s.

378. Celles-ci sont de trois ordres. D'abord, l'activité de télémédecine ne peut pas être mise en place si elle ne s'inscrit pas, au choix, dans un programme national, dans un contrat pluriannuel d'objectifs et de moyens[454] (CPOM) ou dans un contrat particulier signé avec le Directeur Général (DG) de l'ARS. Le décret précise également que le CPOM ou le contrat particulier signé avec le DG ARS devra respecter par ailleurs les prescriptions du programme relatif au développement de la télémédecine, lui-même inclus dans le projet régional de santé[455]. On peut noter ici une volonté de la part du législateur de s'assurer que les projets de télémédecine se développent en lien avec les ARS et dans le respect des besoins de santé des populations. De ce fait, elles jouent un rôle important puisqu'elles garantissent la cohérence des activités développées avec les besoins du territoire. Il s'agit également d'un moyen utile pour orienter le développement de projets sur des thématiques ou des spécialités considérées comme prioritaires. Il est important de préciser que, suite au décret dit "Télémédecine", la Direction Générale de l'Offre de Soins (DGOS) a souhaité mettre en place une stratégie nationale de déploiement de la télémédecine. Celle-ci a consisté en la mise en place d'un comité de pilotage national[456], en charge de coordonner les initiatives des différents acteurs de la télémédecine. En 2011, ce comité de pilotage national a identifié cinq thématiques considérées comme étant des priorités nationales de déploiement de la télémédecine. Il s'agit de la permanence des soins en imagerie, de la prise en charge de l'AVC, de la santé des personnes détenues, de la prise en charge des maladies chroniques et des soins en structures médico-sociale ou HAD. Ces thématiques sont, à l'heure actuelle, priorisées dans les programmes régionaux de développement de la télémédecine.

---

[454] Article L. 6114-1 du Code de la santé publique : « *l'agence régionale de santé conclut avec chaque établissement de santé ou titulaire de l'autorisation prévue à l'article L. 6122-1 un contrat pluriannuel d'objectifs et de moyens d'une durée maximale de cinq ans. Lorsqu'il comporte des clauses relatives à l'exécution d'une mission de service public, le contrat est signé pour une durée de cinq ans*. »

[455] Article L .1434-2 du Code de la santé publique : « *le projet régional de santé est constitué :*
1° D'un plan stratégique régional de santé, qui fixe les orientations et objectifs de santé pour la région ;
2° De schémas régionaux de mise en œuvre en matière de prévention, d'organisation de soins et d'organisation médico-sociale ;
3° De programmes déclinant les modalités spécifiques d'application de ces schémas, dont un programme relatif à l'accès à la prévention et aux soins des personnes les plus démunies et un programme relatif au développement de la télémédecine. La programmation peut prendre la forme de programmes territoriaux de santé pouvant donner lieu à des contrats locaux de santé tels que définis à l'article L. 1434-17.
Le plan stratégique régional de santé prévoit des articulations avec la santé au travail, la santé en milieu scolaire et la santé des personnes en situation de précarité et d'exclusion »

[456] Ce comité de pilotage est animé et coordonné par la DGOS en lien avec d'autres partenaires institutionnels tels que la DSSIS, l'ASIP Santé, la DSS, la CNAM-TS, l'ANAP, la HAS, la DATAR, la DGCIS et les représentants des usagers.

379. Les établissements, organismes et/ou professionnels de santé qui participent à une activité de télémédecine vont également devoir conclure entre eux une convention, afin de régir leurs relations et les conditions d'organisation de cette activité. A ce sujet, la CNIL recommande que les engagements et les responsabilités des acteurs soient rappelés dans ces conventions. Celles-ci devront également, en pratique, comprendre les mentions relatives à l'organisation de l'activité, à l'hébergement, à la sécurité et la confidentialité des données, mais également celles relatives à la procédure dégradée à organiser dans l'hypothèse d'une défaillance de la solution technique initiale.

380. Enfin, les organismes, établissements ou professionnels de santé qui mettent en place une activité de télémédecine doivent s'assurer à la fois de la formation, mais aussi des compétences techniques des professionnels qui prennent part à l'activité. Toutefois, notons que le décret reste muet en ce qui concerne les moyens de contrôle de la bonne formation des professionnels. En cas de contentieux, il reviendrait alors à l'établissement de santé d'apporter la preuve qu'il a bien formé ses professionnels à l'utilisation de la solution technique qu'il aurait mis à disposition de ceux-ci.

381. Le cadre de la mise en place d'une activité de télémédecine ne s'arrête pas à ces procédures préalables. D'autres procédures administratives vont devoir être respectées, impliquant plusieurs acteurs. Cet ensemble forme alors un cadre assez pesant pour les responsables de projets de télémédecine, susceptibles de les freiner.

B. Un cadre lourd, frein au développement de l'activité ?

382. Certains acteurs de la télémédecine considèrent aujourd'hui que le cadre légal, bien que sécurisant, peut constituer un frein au développement rapide de la télémédecine. Effectivement, force est de constater que les projets aboutis ne sont pas aujourd'hui aussi nombreux que les professionnels du secteur auraient pu l'espérer (1). Ce constat résulte principalement des lourdeurs administratives qui entourent la mise en place d'une activité de télémédecine, qu'elles soient prévues par les textes, ou induites par la nature même de l'exercice (2). Des pistes d'amélioration sont actuellement étudiées afin d'encourager le développement de la télémédecine (3).

1) Etat des lieux de l'activité en France

383. La DGOS, suite à un premier état des lieux des projets de télémédecine existant en France, réalisé à la fin de l'année 2011, a procédé à un nouveau recensement au 31 décembre 2012[457]. Cette seconde étude a permis d'établir un bilan plus complet et mettre en valeur l'évolution des projets. Alors que 256 dispositifs de télémédecine étaient recensés pour 2011, l'enquête menée en 2012 a révélé l'existence de 331 dispositifs, soit une augmentation de près de 50% en un an. Les actes de téléconsultation et de téléexpertise sont largement majoritaires, puisqu'ils représentent 78 % des projets. Sur l'ensemble de ces projets, 169 sont opérationnels et prennent en charge des patients (contre 161 encore à l'état de conception au moment du recensement). 53% de ces projets concernent de manière exclusive le secteur hospitalier et 30 % impliquent le secteur ambulatoire. A ce sujet, il est utile de préciser qu'il s'agit ici d'une augmentation de 179% par rapport à 2011. Cependant, ces chiffres soulignent une prédominance du secteur hospitalier dans le cadre de l'activité de télémédecine.

384. En adéquation avec les priorités définies au niveau national, 25 régions comptent au moins un dispositif de télémédecine ayant pour objectif la prise en charge d'une maladie chronique. De même, d'une manière globale, 30 dispositifs de télémédecine concernent la prise en charge de l'accident vasculaire cérébral (AVC), 30 projets l'insuffisance rénale et 24 projets l'insuffisance cardiaque.

385. Ces chiffres d'ordre général sur l'évolution de la télémédecine étant exposés, il est intéressant de s'attarder sur un point mis en valeur dans ce rapport de la DGOS : l'état des lieux de la contractualisation et du conventionnement.

En ce qui concerne le conventionnement avec l'ARS, la DGOS affirme que sur les 169 projets opérationnels, seuls 24 % ont fait l'objet d'une contractualisation avec l'ARS (soit environ 41 projets). Aucun chiffre n'est mentionné quant aux projets en cours d'élaboration. Pour autant, 81 % des 331 dispositifs de télémédecine s'inscrivent dans les priorités du programme régional de télémédecine de leur région.

---

[457] « La preuve par 10. Principaux enseignements du bilan PRT et du recensement des projets télémédecine 2013 », Direction Générale de l'Offre de Soins. A noter qu'à l'heure actuelle, ce bilan est le seul bilan officiel qui existe concernant l'état des lieux de l'offre de télémédecine en France.

Le conventionnement entre les acteurs d'un dispositif de télémédecine n'a pas plus de succès puisque seulement 51% des projets opérationnels (donc 86 projets) ont donné lieu à un conventionnement entre les acteurs. La DGOS précise que ce conventionnement recensé peut être total ou partiel, sans pour autant préciser ce qu'elle entend par conventionnement partiel. Or, cette situation va non seulement à l'encontre des dispositions du décret de 2010, qui impose la signature d'une convention, mais également à l'encontre de la plupart des recommandations émises à ce sujet.

386. Alors que la DGOS semble se féliciter de ce développement qu'elle considère comme remarquable, nous ne pouvons que constater que le nombre limité de projets officiels de télémédecine, pour une activité qui dispose d'une existence légale depuis peu de temps, mais se développe toutefois depuis presque 20 ans. Pour nous, cet état de fait tend à montrer qu'il existe encore aujourd'hui des freins au développement des activités de télémédecine, freins qui ne sont pas d'ordre technique.

2) Le poids des procédures préalables

387. La mise en œuvre d'un projet de télémédecine sous-entend, pour son initiateur, de traiter avec une diversité d'interlocuteurs, administratifs ou médicaux, afin soit d'obtenir les autorisations nécessaires à l'activité, soit de contractualiser. Cette procédure préalable est en partie prévue par le décret de 2010 : c'est le cas de la contractualisation préalable obligatoire avec l'ARS ou entre les acteurs d'un même projet (a) mais elle peut également être en partie induite par la nature même de la télémédecine, activité nécessitant une collecte, un traitement et un archivage de données informatisées (b).

a) La contractualisation avec les acteurs

388. Comme nous avons pu le voir précédemment, si l'activité de télémédecine ne s'inscrit pas dans le cadre d'un programme national défini par arrêté pris par le ministre en charge de la santé, ou si elle n'est pas inscrite au sein d'un CPOM quand il s'agit d'une activité menée par un établissement de santé, elle doit faire l'objet d'un contrat signé avec l'ARS. Or, à l'heure actuelle, l'orientation prise par le Ministère de la santé est bien de confier l'organisation des activités de télémédecine aux ARS. Il n'existe donc pas, à ce jour, de programme national de télémédecine.

389. Pour permettre d'accompagner les différents acteurs dans cette démarche de contractualisation, la DGOS a publié en 2012 un guide méthodologique[458]. Ce guide considère la contractualisation avec l'ARS comme un levier, permettant d'assurer une meilleure visibilité aux porteurs des projets de télémédecine, tout en assurant la qualité des activités mises en place. En l'absence de précisions dans le décret, le guide méthodologique présente l'intérêt de préconiser une durée et un périmètre pour les contrats : ceux-ci doivent donc, selon le Ministère, avoir une durée calée sur celle du programme régional de télémédecine, et être signés une fois la phase de conception terminée, mais avant la prise en charge effective des patients. Enfin, le guide propose un contrat-type.

390. Les porteurs d'un projet de télémédecine doivent également prévoir une convention entre eux. Celle-ci a notamment pour but de prévoir les modalités pratiques de l'organisation de l'activité (en termes de solution technique choisie par exemple) mais rappelle également les obligations de chacun en matière de droit des patients ainsi qu'en termes de répartition des responsabilités. Ainsi, dans le cadre de la mise en place d'un projet de télémédecine, le décret de 2010 exige, *a minima*, la mise en place de deux conventions différentes. Cette procédure, bien qu'utile en plusieurs points, reste lourde pour les différents acteurs. Elle implique une charge administrative supplémentaire qui pourra s'avérer chronophage, surtout lorsque le nombre d'acteurs concernés par l'activité sera important. Or, il ne faut pas oublier que le but premier d'un projet de télémédecine est l'amélioration de la prise en charge des patients. Pourtant, cette charge administrative est souvent une cause de retard dans le lancement des activités de télémédecine.

b) Les procédures induites par l'activité.

- La procédure préalable auprès de la CNIL

391. Initialement, la CNIL exigeait que l'activité de télémédecine soit préalablement soumise à une demande d'autorisation[459]. Cependant, la CNIL, dans une démarche de simplification des formalités préalables, a décidé de soumettre au régime de la déclaration les traitements de données de santé qui relèvent des exceptions prévues à l'article 8 II de la loi Informatique et Libertés. Cette démarche de la CNIL s'inscrit dans la continuité de la

[458] Circulaire DGOS/PF3 n°2012-114 du 13 mars 2012 relative au guide méthodologique pour l'élaboration des contrats et des conventions en télémédecine, non publiée au *JORF*.
[459] Disponible sur [http://www.sante.gouv.fr]. Consulté le 15 mai 2017.

philosophie impulsée par le règlement européen sur la protection des données, fondé en grande partie sur la responsabilisation des responsables de traitement[460].

392. Cette démarche aurait pu, en réalité, être mise en place bien avant l'adoption du règlement européen. Une lecture croisée de l'article 8 et de l'article 25-I-1 de la loi Informatique et Libertés permet de considérer que les traitements de données de santé mis en place dans le cadre d'une activité de télémédecine, permet d'affirmer que ceux-ci n'étaient pas soumis à la procédure d'autorisation mais simplement à la procédure de déclaration. En effet, l'article 25-I-1 de la loi Informatique et Libertés prévoit que « *sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés […] les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8* ». Or, les traitements mis en œuvre dans le cadre d'une activité de télémédecine relèvent, selon nous, des 1° et 2° du II de l'article 8[461].

- L'hébergement agréé des données

393. Comme le prévoit l'article R. 6316-10 du Code de la santé publique, « *les organismes et les professionnels de santé utilisateurs des Technologies de l'Information et de la Communication pour la pratique d'actes de télémédecine s'assurent que l'usage de ces technologies est conforme aux dispositions prévues au quatrième alinéa de l'article L. 1111-8 du Code de la santé publique relatif aux modalités d'hébergement des données de santé à caractère personnel* ».

Les acteurs impliqués dans une activité de télémédecine vont devoir réfléchir aux modalités d'hébergement des données de santé recueillies dans ce cadre. Un des risques, dans l'hypothèse d'une activité qui regroupe plusieurs établissements ou professionnels de santé, est que l'un d'entre eux conserve l'ensemble des données de santé sur son système d'information. La question peut se poser de savoir s'il devra à son tour être hébergeur agréé ?

---

[460] *V.* en ce sens la position de la CNIL sur sa démarche de simplification des formalités, disponible sur [https://www.cnil.fr]

[461] Les 1° et 2° du II de l'article 8 visent « *les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée* » et les « *traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle* ».

Tant qu'il ne conserve que les données de patient qu'il a pris en charge, la réponse est non. Toutefois, dans le cadre d'un réseau de télémédecine, la réponse peut être plus nuancée. Par exemple, dans l'hypothèse où un établissement centralise et conserve l'ensemble des données, mais ne participe pas à toutes les prises en charge par le réseau, il en viendra à être hébergeur de données de santé et devra donc disposer d'un agrément à ce titre. Cette situation doit donc être pensée en amont de la mise en place de l'activité par l'ensemble des acteurs. En effet, comme nous l'avons vu précédemment, la procédure d'hébergement est longue. Le plus simple pour l'ensemble des acteurs est donc de solliciter un hébergeur agréé.

- La convention de coopération entre professionnels

394. Dans certains cas, l'activité de télémédecine va faire appel à une équipe pluridisciplinaire. D'ailleurs, certains actes habituellement réservés aux médecins par exemple, vont, dans le contexte de la télémédecine être reportés sur le personnel paramédical, tels que les infirmiers. Dans ce cas, le projet de télémédecine devra, en plus des différentes conventions citées précédemment, mettre en place le protocole de coopération prévu par l'article L. 4011-1[462] du Code de la santé publique. Cette possibilité d'encadrer légalement ce qui est ni plus ni moins qu'un transfert de tâches, a été introduite par l'article 51 de la loi HPST. Cet article permet à un professionnel, dans le cadre d'un protocole précis, de réaliser des actes qui ne relèvent pas, d'un point de vue strictement réglementaire, de sa compétence.
En pratique, il appartient aux professionnels d'être les initiateurs de cette démarche. Le protocole mis en place entre les professionnels souhaitant s'inscrire dans une démarche de coopération est soumis à validation de l'ARS. Celle-ci vérifie, dans un premier temps, si le protocole correspond bien à un besoin réel de santé constaté au sein de la région. Puis, le protocole est soumis à l'avis de la Haute autorité de Santé (HAS). Le Directeur de l'ARS autorise ensuite la mise en œuvre de ce protocole par voie d'arrêté.

[462] Cet article prévoit : « *Par dérogation aux articles L. 1132-1, L. 4111-1, L. 4161-1, L. 4161-3, L. 4161-5, L. 4221-1, L. 4311-1, L. 4321-1, L. 4322-1, L. 4331-1, L. 4332-1, L. 4341-1, L. 4342-1, L. 4351-1, L. 4361-1, L. 4362-1, L. 4364-1 et L. 4371-1, les professionnels de santé peuvent s'engager, à leur initiative, dans une démarche de coopération ayant pour objet d'opérer entre eux des transferts d'activités ou d'actes de soins ou de réorganiser leurs modes d'intervention auprès du patient. Ils interviennent dans les limites de leurs connaissances et de leur expérience ainsi que dans le cadre des protocoles définis aux articles L. 4011-2 et L. 4011-3[…]* »

395. Cependant, ce dispositif n'a pas reçu le succès escompté. Dans son rapport d'activité de 2013[463] consacré au sujet, la HAS donnait les chiffres suivants : « *au 31 décembre 2013, les ARS ont transmis 71 protocoles à la HAS correspondant aux protocoles reçus depuis 2 ans […] Mais du fait de double saisine pour le même dossier ou de retrait de dossiers par les promoteurs la HAS a donné un avis sur 38 dossiers et 19 dossiers sont en instruction fin 2013. 30 ont reçu un avis favorable avec réserves. Ces réserves portent fréquemment sur les indicateurs proposés (fiches incomplètes ou manquantes), sur les formations nécessaires à l'acquisition de compétences ou sur l'information donnée aux patients*. »

396. En ce qui concerne plus particulièrement la télémédecine, seuls trois protocoles de coopération avaient été mis en place en décembre 2013 : le premier concernant une consultation de mesure de l'acuité visuelle et de la réfraction (dans ce cas, un ophtalmologiste délègue ses compétences à un orthoptiste ou un infirmier diplômé d'état), le deuxième concernant le suivi de patients diabétiques traités par insuline (dans ce cas la prescription des soins est effectué par l'infirmier à la place du médecin) et le dernier concernant le suivi des plaies complexes et/ou à retard de cicatrisation (dans ce cas, le médecin ou le chirurgien délègue ses compétences à un infirmier).

397. Nous ne pouvons que nous étonner du faible nombre de protocoles de coopération mis en place. Cependant, nous ne sommes pas en mesure de dire, faute de recensement précis de l'ensemble des projets de télémédecine existant[464], si ce faible chiffre est dû à l'absence réelle de transfert de compétences dans les activités de télémédecine ou s'il s'agit d'une lacune dans la réalisation des démarches par les responsables de projet. La lourdeur d'une part, et le manque d'adhésion au dispositif, d'autre part, sont certainement les causes de ce faible nombre.

---

[463] HAS, « les protocoles de coopération article 51 de la loi HPST », rapport d'activité 2013, disponible sur [http://www.has-sante.fr]. Consulté le 3 mars 2017.

[464] Le recensement des projets effectués par la DGOS reste global et ne présente pas de manière individuelle l'ensemble des projets existants.

3) Pistes d'évolution

En mai 2015, le groupe de travail GT33 CSIS-CSF[465] a publié un rapport[466] dans lequel il identifie les freins au développement pour ensuite cibler des actions susceptibles d'améliorer le développement de la télémédecine.

398. La première action très concrète consiste en une aide à la qualification d'un projet de télémédecine. Pour cela, le groupe a réalisé un kit de démarrage, composé de cinq fiches pratiques permettant d'identifier de manière claire le projet et de prendre en considération toutes les implications juridiques de celui-ci.

399. La deuxième action proposée est une aide à l'évaluation *a priori* d'un projet. Cette aide intégrerait un dialogue en amont entre les porteurs de projets et l'HAS et la CNAMTS, notamment afin de s'assurer de l'efficience du projet et d'aborder éventuellement la prise en charge par l'Assurance Maladie des futurs actes de télémédecine.

400. La troisième proposition revient sur le processus de contractualisation actuellement prévu par le décret d'octobre 2010. Pour le GT 33, une des pistes serait éventuellement de ne rendre la contractualisation obligatoire que pour les projets expérimentaux financés. A ce sujet, la DGOS a mis en place un groupe de travail, auquel les industriels ont été associés dès la fin de l'année 2014 et un décret refondu et simplifié était annoncé pour la fin du 1er semestre 2015. Toutefois, ce décret a pris du retard et n'est, à l'heure actuelle, toujours pas publié.

401. La quatrième proposition s'inscrit dans la même dynamique que la précédente puisqu'elle consiste en une simplification de l'instruction des protocoles de coopération. Cette démarche serait accompagnée d'une communication, auprès des porteurs de projets, sur l'existence d'un site dédié à la dématérialisation des demandes de validation de protocole.

---

[465] Ce groupe de travail associe les représentants des pouvoirs publics (DGOS, DSSIS, DGE, DGRI, ASIP Santé, ANAP, HAS, CNAMTS, ANSM) et des syndicats industriels (SNITEM, Syntec Numérique) et a pour objectif de permettre l'émergence d'une stratégie industrielle en matière de e-santé (projet nommé « mesure 33 »).

[466] « GT33CSIS-CSF: Permettre l'émergence d'une stratégie industrielle en matière de e-santé, en soutien de la politique de santé publique, en associant les industriels. Lever les freins au déploiement de la télémédecine », Rapport élaboré par le groupe de travail sur la télémédecine réuni dans le cadre du Comité Stratégique de Filière Santé, Mai 2015. Disponible sur [http://www.social-sante.gouv.fr].

402. Le groupe de travail propose, en cinquième intention, de simplifier l'ensemble des démarches administratives obligatoires au niveau régional. Partant du constat que les interlocuteurs des responsables de projets télémédecine sont à la fois nombreux et mal identifiés, il est préconisé la clarification du parcours administratif, qui pourrait passer par l'instauration d'un guichet unique auprès de l'ARS. Enfin, les aspects techniques, et notamment les systèmes d'authentification, doivent être clarifiés et la télémédecine promue, notamment en l'intégrant dans les parcours de soins.

403. Ces propositions, si elles étaient mises en œuvre, permettraient effectivement, selon nous, d'augmenter le développement de projets de télémédecine. Le chantier principal serait alors l'ensemble des simplifications nécessaires en termes de démarches administratives, celles-ci représentant un poids considérable et chronophage pour les porteurs de projets.

§2. L'informatisation des prescriptions médicales, un cadre en construction

404. Le développement des TIC dans la pratique médicale couvre tous les actes médicaux, y compris la prescription médicale. Cela implique deux principes différents, sur lesquelles il est intéressant que nous nous attardions. D'une part, la possibilité d'utiliser l'e-mail pour transmettre une prescription médicale (A) et d'autre part, l'informatisation de l'acte en tant que tel et donc de toutes les étapes prévues dans le circuit du médicament (B).

A. La prescription par voie électronique, une possibilité encore limitée

405. Bien avant l'encadrement de la télémédecine, le législateur s'est penché sur la possibilité de transmettre une prescription médicale par courrier électronique. Elle existe donc depuis 2004 (1), mais elle mériterait aujourd'hui d'être exploitée et développée (2).

1) La prescription par e-mail, une possibilité légalement encadrée

406. C'est la loi du 3 août 2004 relative à l'assurance maladie[467] qui, dans son article 34, a introduit la possibilité de rédiger puis transmettre une ordonnance par courriel. Cependant, cette possibilité est très encadrée afin d'en limiter l'utilisation à certaines situations. L'article 34 de la loi précitée dispose en effet qu' : « *une ordonnance comportant les prescriptions de soins ou de médicaments peut être formulée par courriel dès lors que son auteur peut être dûment identifié, qu'elle a été établie, transmise et conservée dans des conditions propres à garantir son intégrité et sa confidentialité et à condition qu'un examen clinique du patient ait été réalisé préalablement, sauf à titre exceptionnel, en cas d'urgence* ».

407. Plusieurs conditions sont donc posées afin de permettre à un médecin d'envoyer une prescription médicale à un patient sous forme de courrier électronique. Les premières conditions ont trait au document envoyé par voie électronique. En effet, celui-ci, pour être

[467] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, *JORF* n°190, 17 août 2004, p. 14598.

valable, va devoir respecter plusieurs règles permettant d'assurer notamment la sécurité du document. Ainsi, l'auteur de la prescription doit être « *dûment identifié* ». Cette identification pourra passer par l'apposition d'une signature électronique ou par l'utilisation de la carte de professionnel de Santé (CPS). La prescription doit ensuite être établie, transmise et archivée dans des conditions permettant d'assurer son intégrité (le document ne doit pas être modifiable), et sa confidentialité. Finalement, ces conditions ne sont pas nouvelles puisque ce sont celles que nous retrouvons en matière de conservation et de transmission de données médicales sur support électronique.

La dernière condition essentielle à l'envoi d'une prescription électronique est la réalisation préalable d'un examen clinique du patient. Cette précision est importante et non sans conséquences. En effet, cela implique qu'aucune prescription par courriel ne pourra être transmise à l'issue d'un acte de télémédecine au cours duquel aucun examen clinique ne pourrait être réalisé. L'envoi par e-mail d'une prescription médicale pourrait cependant être envisageable dans le cas d'une téléconsultation, au cours de laquelle le médecin serait assisté par un professionnel de santé, présent aux côtés du patient, et dont le rôle serait de réaliser l'examen clinique préalable. Dans cette hypothèse, le médecin pourrait alors ensuite rédiger et envoyer par courriel la prescription médicale. Cette organisation serait, bien entendu, encadrée par un protocole de coopération.

De même, bien que le décret encadrant la télémédecine n'ait pas consacré la téléprescription parmi les actes de télémédecine, alors même que l'article L. 6316-1 du Code de la santé publique prévoit que la télémédecine permet notamment de « *prescrire des produits* », nous pouvons parfaitement envisager la possibilité de recourir à la téléprescription, à l'issue d'un acte de téléconsultation au cours duquel l'examen clinique du patient aura été réalisé[468].

Sous réserve du respect de l'ensemble de ces dispositions, l'envoi d'une ordonnance par courrier électronique est donc envisageable et juridiquement encadré. Il nous faut cependant revenir sur une autre voie possible de transmission d'une ordonnance, qui pose régulièrement difficultés : l'ordonnance faxée.

---

[468] DESMARAIS, Pierre. « La télémédecine, source de nouveaux cas de responsabilité », *Communication Commerce électronique*, septembre 2011, étude n° 16.

408. L'ordonnance faxée n'étant mentionnée dans aucun texte réglementaire, elle n'est ni interdite ni expressément autorisée. Il est évident qu'une ordonnance envoyée par courriel ne peut pas être assimilée à une ordonnance faxée, les deux outils utilisés ne présentant pas les mêmes conditions de sécurité ou de confidentialité. Les modalités prévues à l'article 34 de la loi de 2004 ne peuvent donc pas s'appliquer à la télécopie. Toutefois, cette pratique peut s'envisager, à condition qu'elle s'inscrive dans le cadre légal de toute prescription médicale d'une part, et que le recours à cette pratique soit pleinement justifié, d'autre part.

Comme le prévoit l'article R. 5132-3[469] du Code de la santé publique, l'examen clinique du patient est le préalable obligatoire à toute ordonnance médicale. Le recours à la télécopie devra donc s'inscrire dans ce cadre strict. Toutefois, le respect de cette seule condition n'apparait pas suffisant. Comme l'a souligné la HAS dans ses recommandations relatives aux prescriptions médicamenteuses par téléphone[470], « *un envoi par fax ne peut garantir une complète confidentialité, il est donc recommandé de préférer un envoi par courriel chaque fois que cela est possible*». Ainsi, l'envoi par fax devrait donc rester une exception, utilisée dans des cas d'urgence. La régulation médicale, acte de médecine à part entière, est donc un cadre spécifique dans lequel une ordonnance envoyée par télécopie au pharmacien va pouvoir être acceptée. D'ailleurs, le Conseil National de l'Ordre des Médecins a très tôt précisé les règles dans lesquelles devaient s'inscrire ces pratiques. Ainsi, les différents intervenants doivent être dûment enregistrés et les échanges mémorisés, afin de pouvoir être consultés dans l'hypothèse d'un préjudice ou d'un litige ultérieur.

En tout état de cause, il apparait donc que l'ordonnance faxée, si elle peut être envisagée, doit rester une situation exceptionnelle ou transitoire. Le médecin pourra l'utiliser pour régler des situations d'urgence et non par facilité voire même par complaisance. Cependant, il reste préférable de privilégier l'envoi par courriel, parfaitement encadré.

Aujourd'hui, il serait souhaitable pour certains que cette possibilité de transmission par courriel d'ordonnances soit utilisée pour servir de base à une autre pratique, la e-prescription.

---

[469] « *La prescription de médicaments ou produits destinés à la médecine humaine mentionnés à la présente section est rédigée, après examen du malade […]* »

[470] Prescription médicamenteuse par téléphone (ou téléprescription) dans le cadre de la régulation médicale, p. 4, disponible sur : [http://www.has-sante.fr]. Consulté le 3 mars 2017.

2) Les voies de déploiement de la e-prescription

409. La notion de "e-prescription" désigne une pratique qui recouvre une réalité bien plus large que le simple envoi par courriel des ordonnances. Elle consiste notamment à regrouper l'ensemble des ordonnance électroniques d'un patient afin de constituer une base générale de données le concernant et regroupant l'ensemble des prescriptions médicales qui lui ont été délivrées, qu'il s'agisse de prescriptions de médicaments, de dispositifs médicaux ou encore d'examens de biologie. En France, c'est le Comité de Liaison des Institutions Ordinales (CLIO santé)[471] qui s'est engagé depuis quelques années dans cette démarche (a). Mais cette idée est également prégnante et bien avancée au niveau européen (b).

a) La note d'orientation du CLIO santé

410. Depuis la loi de 2004, aucun texte n'est venu préciser le cadre du développement de l'e-prescription. Ainsi, contrairement à la télémédecine ou au DMP, la e-prescription n'existe pas encore légalement, bien qu'elle faisait partie du plan de développement du DMP.

Voulant s'inscrire dans une démarche d'incitation au déploiement de l'e-prescription, le CLIO santé a rédigé et publié en janvier 2012 une note d'orientation présentant les enjeux de la prescription électronique et formulant des propositions pour la déployer.

Dans cette proposition, validée par ailleurs par sept ordres professionnels, le groupe de travail part de la possibilité, depuis 2004, d'établir une ordonnance par voie électronique, pour proposer ensuite de développer un système de e-prescription, qui reposerait sur des prescriptions rédigées de manière informatique puis déposées dans une base de données des prescriptions. Bien que présentant un projet intéressant et certainement utile pour l'amélioration de la prise en charge du patient et la diminution des risques de contre-indication entre différentes prescriptions, il n'apporte aucune réelle proposition en termes de gouvernance et de structuration juridique de ce projet. La note d'orientation rappelle juste que la CNIL devra être consultée sur ce sujet et préconise de choisir le NIR comme identifiant patient, plus sûr et plus large que l'INS-C. Cependant, le CLIO santé s'en remet à l'ASIP santé pour mettre en place des phases pilotes, en lien avec les ordres professionnels. Rien

[471] Le Comité de liaison des Institutions Ordinales est un comité qui réunit les institutions françaises auxquelles sont obligatoirement inscrits les membres de professions réglementées.

d'innovant donc en ce qui concerne la gouvernance de ce genre de projets. Ceci explique peut-être pourquoi cette note semble être restée lettre morte. En effet, depuis sa publication en janvier 2012, aucune action n'a été mise en œuvre sur cette base.

b) Le projet européen EPSOS

411. Une autre voie de développement a également été envisagée au niveau européen au travers du projet EPSOS. Acronyme de "Smart Open Services for European patients", le projet EPSOS a démarré en 2008. Regroupant initialement 12 pays de l'Union Européenne, 11 autres se sont ajoutés en 2011 lors du lancement de la phase pilote.

Il s'agissait d'un projet cofinancé par l'Union Européenne comportant deux objectifs principaux. D'une part, la mise en place d'un service de e-prescription (service qui comprend la création d'une prescription de médicaments et sa transmission électronique à un pharmacien) et d'un servie de "patient summary" (service qui reprend l'ensemble des données essentielles et pertinentes pour assurer la continuité de la prise en charge d'un patient d'un pays à un autre). D'autre part, une analyse à la fois de l'intérêt et de l'impact sur les pratiques de ces services.

Le but de la phase pilote, menée entre 2011 et 2014, a été de tester l'échange de données entre pays de l'Union Européenne dans ce contexte, en se basant uniquement sur les cadres réglementaires existant dans chaque pays membre, sans en créer de nouveau. En France, une opération pilote avait été mise en place entre 2012 et 2013, s'appuyant sur le programme européen d'échange étudiant ERASMUS et visant à mettre en place le service « Patient SUMMARY »

Le projet, qui a pris fin en juin 2014, présente un bilan positif. Il a notamment permis de définir les bases en termes de gouvernance de ce type de service mais également en termes de contenu nécessaire des dossiers partagés. De plus, bien que la mise en œuvre de services de santé transfrontaliers s'appuyant sur les TIC relève des prérogatives nationales, le projet EPSOS a permis d'instaurer une dynamique efficace en la matière et plusieurs projets européens portant sur l'interopérabilité en e-santé ont été lancés depuis.[472] Le projet EPSOS

[472] eHealth Network.

est donc un exemple réussi de projet de partage de données et de prise en charge informatisée à grande échelle.

Cette dynamique d'informatisation de la prescription ne se cantonne pas à l'envoi de celle-ci. Depuis plusieurs années on observe, au sein des établissements de santé, une évolution tendant à l'informatisation de l'ensemble du circuit du médicament. Cette impulsion résulte principalement des orientations voulues par les pouvoirs publics.

B. La prescription informatisée, une pratique encouragée par les pouvoirs publics

412. Par le biais de plusieurs dispositifs réglementaires, pour la majorité relatifs à la qualité et à la sécurité des soins, le Ministère de la santé incite les établissements à informatiser leur circuit du médicament (1). En parallèle, le législateur montre sa volonté de ne pas laisser cette informatisation sans cadre et a obligé les éditeurs de solutions logicielles à s'engager dans une démarche de certification obligatoire, garante de la sécurité du circuit du médicament (2)

1) L'incitation à l'informatisation du circuit du médicament

413. Le circuit du médicament, qui peut être défini de manière simplifié comme étant le chemin parcouru par le médicament (prescription médicale, dispensation puis administration) est, pour les établissements de santé, encadrés par plusieurs textes différents.

414. L'informatisation du circuit du médicament n'est pas une idée récente. Dans l'optique d'assurer aux patients la sécurité et la qualité de leur prise en charge médicamenteuse, le Ministère de la santé a très vite mis en avant le bénéfice apporté par une informatisation complète de l'ensemble du circuit du médicament, permettant non seulement une meilleure traçabilité, mais également un renforcement indéniable de la sécurité du patient, en évitant la survenance d'événements indésirables. Le premier texte à aborder ce sujet est une circulaire du 2 janvier 1985[473] relative à l'informatisation des systèmes de dispensation des médicaments. Plusieurs autres textes vont suivre mais le texte majeur en la matière est l'arrêté du 31 mars 1999 relatif à la prescription, la dispensation et à l'administration des

[473] Circulaire n° 658/DPhM du 2 janvier 1985 relative à l'informatisation des systèmes de dispensation, non publiée au *JORF*.

médicaments soumis à la réglementation des substances vénéneuses dans les établissements de santé[474]. Ce texte prévoit notamment la possibilité pour une prescription d'être rédigée, conservée et transmise de manière informatisée, sous réserve, d'une part, de pouvoir identifier son auteur et, d'autre part, de pouvoir l'éditer sur support papier si nécessaire. L'informatisation du circuit du médicament continue alors sa progression.

Cependant, l'ensemble des textes publiés à ce sujet entre 1985 et 1999 sont des circulaires, n'ayant aucune incidence juridique en tant que telle, ou des arrêtés, pris par le ministre ou le secrétaire d'Etat dédié à la santé. Le cadre mis en place n'avait donc pas ou peu de force contraignante vis-à-vis des responsables du circuit du médicament.

415. Le décret n° 2005-1023 du 24 août 2005 relatif au contrat de bon usage des médicaments et des produits et prestations mentionné à l'article L. 162-22-7 du Code de la sécurité sociale[475] va venir changer ce paysage normatif. En effet, l'article 4 de ce texte prévoit que les établissements de santé doivent souscrire à des engagements relatifs aux médicaments ou aux produits et prestations, sous la forme d'un programme pluriannuel d'actions, celui-ci devant porter *a minima* sur un certain nombre de points, dont l'informatisation du circuit du médicament fait partie. Ainsi, c'est désormais dans le cadre du contrat de bon usage[476], signé avec l'ARS, que les établissements de santé vont organiser l'informatisation de la prescription médicale.

416. La loi HPST va également être à l'origine d'une impulsion en ce sens. En effet, en faisant de la qualité et de la sécurité des soins une priorité de la loi, le législateur, de manière indirecte, incite les établissements de santé à continuer l'informatisation de leur circuit du médicament. D'autres textes vont suivre et intègrent la qualité de la prise en charge médicamenteuse du patient dans la gestion globale des risques à l'hôpital. C'est le cas

---

[474] Arrêté du 31 mars 1999 relatif à la prescription, à la dispensation et à l'administration des médicaments soumis à la réglementation des substances vénéneuses dans les établissements de santé, les syndicats interhospitaliers et les établissements médico-sociaux disposant d'une pharmacie à usage intérieur mentionnés à l'article L. 595-1 du Code de la santé publique, *JORF* n°77, 1er avril 1999, p. 4854.

[475] Décret n° 2005-1023 du 24 août 2005 relatif au contrat de bon usage des médicaments et des produits et prestations mentionné à l'article L. 162-22-7 du Code de la sécurité sociale, *JORF* n°198, 26 août 2005, p. 13526.

[476] Le CBU est un contrat conclu entre l'ARS et un établissement de santé pour une durée de trois à cinq ans. Il a pour but principal de sécuriser le circuit du médicament. En cas de respect de ses engagements, l'établissement de santé se voit assuré un taux de remboursement de 100% par l'assurance maladie pour les spécialités pharmaceutiques et les produits et prestations mentionnés à l'article L. 162-22-72 du Code de la sécurité sociale. Dans le cas contraire, le taux de remboursement peut être réduit à 70%.

notamment le décret du 12 novembre 2010[477] relatif à la lutte contre les événements indésirables associés aux soins ou encore de l'arrêté du 6 avril 2011[478] relatif au management de la qualité de la prise en charge médicamenteuse, qui présente l'informatisation comme un gage d'amélioration de la sécurité de la prise en charge médicamenteuse. Cet arrêté est d'ailleurs intéressant et mérite que nous nous y attardions. Il précise, dans son article 3, que « *l'informatisation des processus de prise en charge médicamenteuse est une des condition essentielle de sa sécurisation* ». Pour le législateur, il est donc clair que la qualité et la sécurité de la prise en charge médicamenteuse du patient passent par l'informatisation du circuit du médicament. Sans être pour autant une obligation légale opposable aux établissements, la formule permet au législateur d'orienter fortement les établissements de santé vers une informatisation. Pour compléter ces textes et accompagner au mieux les établissements dans cette démarche de sécurisation, la DGOS a publié un guide intitulé "Qualité de la prise en charge médicamenteuse - outils pour les établissements de santé"[479]. Celui-ci rappelle également à plusieurs occasions, la nécessité de l'informatisation du circuit du médicament. Il précise notamment que le programme "hôpital numérique", dans sa feuille de route 2012-2016 pour les systèmes d'information hospitaliers, « *incite l'ensemble des établissements de santé à atteindre un socle minimal de maturité sur 5 domaines prioritaires dont la prescription électronique* »[480].

417. Ainsi, pour les pouvoirs publics, l'informatisation n'est pas une fin en soi, mais un outil que les établissements de santé se devront d'utiliser s'ils souhaitent respecter leurs obligations légales en matière de qualité et de sécurité de la prise en charge médicamenteuse. Cependant, cette informatisation ne doit pas reposer sur n'importe quelle solution technique si l'on souhaite qu'elle atteigne son but. C'est pourquoi, désormais, les éditeurs de logiciels de prescription médicale doivent être certifiés.

---

[477] Décret n° 2010-1408 du 12 novembre 2010 relatif à la lutte contre les événements indésirables associés aux soins dans les établissements de santé, *JORF* n°0265, 16 novembre 2010, p. 20428.
[478] Arrêté du 6 avril 2011 relatif au management de la qualité de la prise en charge médicamenteuse et aux médicaments dans les établissements de santé, *JORF* n°0090, 16 avril 2011, p. 6687.
[479] DGOS, « Qualité de la prise en charge médicamenteuse - outils pour les établissements de santé », février 2012, disponible sur [http://www.sante.gouv.fr]. Consulté le 3 mars 2017.
[480] *Id.*, p. 12.

2) La certification obligatoire des logiciels de prescription médicale

418. La loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé[481] a rendu obligatoire la certification des logiciels d'aide à la prescription. Ainsi, désormais, « *ces certifications sont rendues obligatoires pour tout logiciel dont au moins une des fonctionnalités est de proposer une aide à l'édition des prescriptions médicales ou une aide à la dispensation des médicaments dans des conditions prévues par décret en Conseil d'Etat et au plus tard le 1er janvier 2015.* »[482]
Ce texte a été complété par le décret n° 2014-1359 du 14 novembre 2014[483], qui précise l'étendue de cette obligation. Il est intéressant de noter que la certification ne concerne que la fonctionnalité d'aide à la prescription. Un logiciel comportant d'autres fonctionnalités ne devra donc être certifié que pour la partie aide à la prescription. La procédure de certification est établie par la HAS, qui a la charge d'élaborer les référentiels.

419. A ce sujet[484], la certification de ces logiciels répond à un objectif triple : garantir la conformité des logiciels à certaines exigences en termes de sécurité, de conformité et d'efficience. Dans le respect du souci de transparence, qui guide l'ensemble de la loi de 2011, les certifications ne sont pas réalisées par la HAS, mais par des organismes certificateurs, devant eux-mêmes faire l'objet d'une accréditation préalable[485]. La responsabilité de la réalisation de cette certification incombe, bien entendu, aux éditeurs des logiciels. De leur côté, les établissements n'ont pas d'obligation légale de faire appel à un éditeur certifié. Toutefois, il nous semble que cette solution est bien évidemment celle à privilégier par les établissements. De plus, de par la forte obligation de sécurité et de qualité de la prise en charge médicamenteuse qui pèse sur les établissements, le fait de choisir une solution non certifiée pourrait engager leur responsabilité en cas de préjudice.

---

[481] Loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé, *JORF* n°0302, 30 décembre 2011, p. 22667.
[482] Article L. 161-38 du Code de sécurité sociale.
[483] Décret n° 2014-1359 du 14 novembre 2014 relatif à l'obligation de certification des logiciels d'aide à la prescription médicale et des logiciels d'aide à la dispensation prévue à l'article L. 161-38 du Code de la sécurité sociale, *JORF* n°0264, 15 novembre 2014, p. 19255
[484] *V.* en ce sens, la foire aux questions de la HAS portant sur les LAP. Disponible sur [http://www.has-sante.fr]. Consulté le 3 mars 2017.
[485] Cette accréditation est, quant à elle, réalisée par le comité français d'accréditation (COFRAC).

420. Cependant, comme le reconnait la HAS, cette certification présente certaines limites. Ainsi, elle n'aborde pas la problématique de l'intégration des Logiciels d'Aide à la Prescription (LAP) dans les Systèmes d'Information Hospitaliers. Les LAP sont donc certifiés individuellement, mais leur qualité, sécurité, ne sont plus assurées, une fois intégré au sein du SIH d'un établissement. Cela s'explique notamment par le fait que les normes d'interopérabilité entre logiciels ne sont pas, à l'heure actuelle, arrêtées. Par ailleurs, la certification, même si elle peut constituer pour les pharmaciens un levier en termes de respect de la réglementation applicable en matière de médicament, ne doit pas être le seul outil utilisé. En effet, l'intégration de l'ensemble des contraintes juridiques existantes en la matière, au sein du logiciel, ne laisserait plus aucune place aux initiatives, parfois nécessaires notamment en cas d'urgence. Un tel logiciel générerait donc plus de risques, ce qui n'est pas souhaitable. La certification ne peut donc pas conduire, à elle seule, au respect de l'ensemble des contraintes juridiques actuelles pesant sur le circuit du médicament, sous peine d'avoir l'effet inverse.

421. Toutefois, les logiciels d'aide à la prescription sont régulièrement pointés du doigt. Ainsi, le quotidien "Le Parisien"[486] a fait part, en 2013, des défaillances d'un LAP, présumé responsable du décès d'une patiente au centre hospitalier de Versailles en 2011. Les conclusions de cet article reposaient sur un rapport rendu le 4 mars 2013 par la Commission Régionale de Conciliation et d'Indemnisation d'Ile de France, dans le cadre d'une procédure engagée suite au décès d'une patiente en novembre 2011 au centre hospitalier de Versailles. La patiente serait décédée, selon la famille, suite à une prescription d'amoxicilline, antibiotique auquel elle était allergique, mention par ailleurs précisée au sein du dossier médical de la patiente. Or, pour les experts de la CRCI, cette mention n'aurait pas été répercutée dans le système informatique de prescription de médicaments. Cette erreur aurait entrainé, selon la Commission, une perte de chance de survie de la patiente de 80 %. Toujours selon ce rapport, les LAP, même s'ils permettent une clarification des prescriptions, n'assurent pas une sécurité suffisamment fine en matière d'allergies notamment.

A l'heure actuelle, ces outils ne peuvent donc pas être considérés comme totalement fiables et le contrôle manuel par les professionnels de santé reste nécessaire.

---

[486] *V.* en ce sens, dépêche TIC santé du 12 juillet 2013, « Polémique sur les logiciels d'aide à la prescription hospitaliers suite à un décès », disponible sur [http://www.ticsante.com]. Consulté le 3 mars 2017.

Conclusion de section

422. Les TIC occupent aujourd'hui une part majeure dans la prise en charge des patients. Leur utilisation permet l'amélioration de la qualité des soins dispensés aux patients et ce, à plusieurs titres. D'un côté, les soins et techniques de pointe deviennent plus accessibles pour certains patients isolés géographiquement ou dont la condition (personne âgée, handicapée, voire même personne détenue) ne leur permet pas d'accéder aux établissements de santé bénéficiant de ces techniques. D'un autre côté, les établissements de santé sécurisent, grâce à l'informatique, leur circuit du médicament, afin d'éviter les événements indésirables.

423. Cependant, l'intervention du législateur dans ces pratiques, bien que nécessaire, ne doit pas être trop stricte. En effet, le droit ne peut pas devenir bloquant, au risque de provoquer les effets inverses de ceux souhaités. Il faut donc trouver le juste milieu entre intégration des progrès techniques et encadrement juridique de ceux-ci, ce qui peut s'avérer parfois délicat pour le législateur.

Section 2. Prise en charge médicale et TIC : des règles de responsabilité bousculées

424. Le développement de nouvelles pratiques médicales, induites par l'introduction des TIC dans la prise en charge des patients, va venir bousculer les règles de responsabilité établies jusqu'alors. En effet, même si les principes fondamentaux qui dirigent le droit de la responsabilité médicale vont demeurer inchangés, ces règles classiques vont toutefois devoir être adaptées aux spécificités liées aux TIC (Paragraphe 1). Par ailleurs, l'introduction des TIC va induire l'entrée en jeu de règles spécifiques et celles-ci vont devoir être prises en compte et articulées avec les règles classiques (Paragraphe 2).

§1. Droit des usagers et responsabilité médicale : l'adaptation du droit commun

425. Par principe, les patients bénéficient tous des mêmes droits fondamentaux, établis par la loi Kouchner et ce, peu importe la façon dont ils vont être pris en charge. Cependant, du fait de l'introduction des TIC dans la prise en charge, les obligations à la charge des professionnels de santé vont être renforcées (A). Par ailleurs, bien que les règles de responsabilité applicables vont rester les mêmes, les risques d'application vont être multipliés (B).

A. Information et consentement du patient : une obligation maintenue et renforcée

426. L'introduction des TIC modifie les modalités d'exercice de la médecine. Pour autant, les finalités d'un acte médical, même exercé à distance, restent les mêmes.

Ainsi, la télémédecine étant juridiquement définie comme étant un acte médical, le droit commun s'appliquant à l'exercice médical va trouver à s'appliquer à cette activité. Le patient bénéficie des droits classiques définis au sein de la loi Kouchner et notamment le droit d'être informé sur les soins qu'il va recevoir et d'y consentir de manière libre et éclairé.

Toutefois, l'utilisation des TIC va nécessiter une information du patient renforcée et spécifique à ce sujet. Ainsi, il apparait que le patient pris en charge dans le cadre d'une activité médicale exercée par le biais des TIC va être en réalité destinataire d'une double information : une information relative à l'acte médical en lui-même, et une information relative à l'acte de télémédecine en tant que pratique dématérialisée (1). Cependant, se pose la question de la mise en œuvre de ces droits quand la prise en charge implique les TIC (2).

1) L'obligation classique étendue aux spécificités des TIC

427. Devant les particularités propres à la télémédecine, il est logique de s'interroger sur le maintien des obligations classiques des professionnels de santé en matière d'information du patient et de recueil de son consentement. Cette interrogation n'est pas récente et, en 2009, la HAS[487], dans ses recommandations relatives aux prescriptions médicamenteuses par téléphone, avait apporté quelques précisions à ce sujet. Ainsi, elle avait indiqué que les spécificités de la régulation médicale devaient être prises en compte afin d'alléger l'obligation d'information du professionnel intervenant à distance. Toutefois à l'époque, c'était bien la situation d'urgence plus que la dématérialisation de l'acte qui justifiait cette souplesse[488]. Depuis, le législateur est intervenu et, bien que le décret télémédecine ne comporte que peu de dispositions relatives à l'information et au consentement du patient, ces dispositions ont le mérite d'être assez claires. Ainsi, comme le rappelle l'article R 6316-2 du Code de la santé publique : « *les actes de télémédecine sont réalisés avec le consentement libre et éclairé de la personne, en application notamment des dispositions des articles L. 1111-2 et L. 1111-4.* ». Le texte vise expressément l'article L. 1111-2[489] du Code de la santé publique relatif à

[487] HAS, « Recommandations professionnelles : Prescription médicamenteuse par téléphone (ou téléprescription) dans le cadre de la régulation médicale », février 2009, disponible sur [http://www.has-sante.fr]. Consulté le 3 mars 2017.

[488] BOURDAIRE-MIGNOT, Camille. « Téléconsultation : quelles exigences ? Quelles pratiques ? », *RDS*, 2011, pp. 1003-1013.

[489] Cet article dispose que: « *toute personne a le droit d'être informée sur son état de santé. Cette information porte sur les différentes investigations, traitements ou actions de prévention qui sont proposés, leur utilité, leur urgence éventuelle, leurs conséquences, les risques fréquents ou graves normalement prévisibles qu'ils comportent ainsi que sur les autres solutions possibles et sur les conséquences prévisibles en cas de refus. Lorsque, postérieurement à l'exécution des investigations, traitements ou actions de prévention, des risques nouveaux sont identifiés, la personne concernée doit en être informée, sauf en cas d'impossibilité de la retrouver. Cette information incombe à tout professionnel de santé dans le cadre de ses compétences et dans le respect des règles professionnelles qui lui sont applicables. Seules l'urgence ou l'impossibilité d'informer peuvent l'en dispenser.* »

l'obligation d'information du professionnel de santé ainsi que l'article L. 1111-4[490] relatif à la co-décision[491] et donc, au consentement aux soins. Il ne fait dès lors aucun doute que le législateur a voulu s'assurer de l'application des dispositions relatives à l'information et au consentement du patient aux actes de télémédecine. D'ailleurs, comme le souligne à juste titre Pierre DESMARAIS[492], c'est bien cette obligation de consentement préalable à l'exercice de la télémédecine, qui distingue cette pratique médicale nouvellement reconnue du simple avis recueilli par un professionnel auprès d'un confrère[493]. Ainsi, les règles classiques applicables à l'exercice médical vont trouver à s'appliquer à la télémédecine, le décret ne modifiant pas le droit commun de l'exercice médical. Le patient pris en charge dans le cadre d'un acte de télémédecine devra donc recevoir « *une information loyale, claire et appropriée portant sur les différentes investigations, traitements ou actions de prévention proposés, leur utilité, leur urgence éventuelle, leurs conséquences, les risques fréquents ou graves normalement prévisibles qu'ils comportent, les autres solutions possibles ainsi que les conséquences possibles en cas de refus* ». De même, le patient devra être informé des nouveaux risques identifiés postérieurement aux actes réalisés.

428. Cependant, la particularité de la télémédecine tient principalement à la dématérialisation des échanges par le biais de l'utilisation des TIC. Dans ce contexte, le patient va devoir être non seulement informé sur sa prise en charge par le biais d'un dispositif de télémédecine, mais également sur le traitement informatisé de ses données de santé et leur partage entre plusieurs professionnels de santé.

Le traitement des données de santé à caractère personnel est encadré par les dispositions de la loi Informatique et Libertés. Les données de santé sont considérées par ce texte comme étant des données sensibles bénéficiant, à ce titre d'un encadrement spécifique. Toutefois, ce sont bien les dispositions générales de la loi qui vont imposer une information du professionnel de santé au patient.

---

[490] Cet article prévoit 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*. »

[491] Sur l'importance de la co-décision en matière de télémédecine, *V.* notamment BOURDAIRE-MIGNOT, Camille. « Téléconsultation : quelles exigences ? Quelles pratiques ? », *RDS*, 2011, *op. cit.*

[492] DESMARAIS, Pierre. « « La télémédecine, source de nouveaux cas de responsabilité. », *Communication commerce électronique*, n° 9, septembre 2011, étude n° 16

[493] Article R. 4127-32 du Code de la santé publique.

Ainsi, l'article 32 de la loi Informatique et Libertés prévoit que la personne concernée par les données traitées (dans notre cas le patient) doit recevoir une information précise à ce sujet et notamment : l'identité du responsable du traitement, sa finalité, les différents destinataires des données, ainsi que les droits dont il dispose aux termes de la loi Informatique et Libertés. Il s'agit donc d'un droit essentiel pour le patient puisque c'est celui qui conditionne, non seulement son accès aux autres droits dont il dispose (notamment droit d'accès aux données et de rectification), mais également celui qui, comme pour l'acte médical, va lui permettre de consentir ou non au traitement de ses données et ce, de manière éclairée. Un bémol, toutefois, doit être apporté à ce sujet. En effet, la loi Informatique et Libertés prévoit certains cas dans lesquels le consentement de la personne concernée ne sera pas nécessaire. Il s'agit notamment du cas du traitement mis en place pour répondre à une obligation légale (c'est le cas, par exemple, de la mise en place d'un dossier médical, rendu obligatoire par l'article R. 1112-2 du Code de la santé publique).

429. Certains professionnels de santé craignent cette information supplémentaire qui devra être donnée au patient, celle-ci pouvant se montrer difficile du fait de la technicité de la matière, mais également chronophage[494]. De plus, il leur est nécessaire de diffuser une information claire en deux temps : d'abord, celle relative à l'acte de soins, puis celle relative à l'utilisation du procédé de télémédecine.

430. En ce qui concerne le partage des données du patient, le décret prévoit que « *les professionnels participant à un acte de télémédecine peuvent, sauf opposition de la personne dûment informée, échanger des informations relatives à cette personne, notamment par le biais des TIC* ». Rien de réellement nouveau dans cette disposition, puisqu'il s'agit ici d'une application du secret partagé tel que défini à l'article L. 1110-4 du Code de la santé publique. Le patient devra donc être informé du partage de ces informations par le bais des TIC, mais également des personnes avec lesquelles elles seront partagées afin de pouvoir s'y opposer s'il le souhaite. L'information due au patient en matière de télémédecine est donc renforcée, puisqu'à l'information classique relative à l'acte médical en lui-même et à ses conséquences, s'ajoute l'information relative à l'acte de télémédecine en tant que pratique faisant appel aux TIC.

---

[494] MORLET-HAÏDARA, Lydia. RAHAL-LÖFSKOG Délia. « La télémédecine et la protection des données de santé par la loi Informatique et Libertés », *RGDM*, n° 44, 2012, p. 341.

431. Enfin, en ce qui concerne plus particulièrement le consentement du patient, la question de la possibilité pour celui-ci de choisir ou non son télémédecin pourrait être soulevée. Toutefois, il y a lieu de vite éluder cette question. En effet, comme le souligne à juste titre Caroline LE GOFFIC[495] dans son étude sur le sujet, un médecin a la possibilité de recourir à un tiers compétent, afin que le patient reçoive les soins les plus adaptés et fondés sur les notions acquises de la science[496]. Dès lors, le médecin requérant doit, il est vrai, recueillir le consentement du patient au sujet de la pratique de la télémédecine, mais il n'aura pas à obtenir son consentement quant au choix du médecin requis.

2) La mise en œuvre des droits des patients

a) La question de la forme de l'information

432. La question qui se pose à nous ici est de savoir comment la télémédecine va pouvoir s'acquitter de son devoir d'information dans le cadre d'une relation totalement dématérialisée. Selon les dispositions de l'article L. 1111-2 du Code de la santé publique, l'information « *est dispensée au cours d'un entretien individuel* ». A cela s'ajoutent les dispositions du Code de déontologie médicale qui précisent que l'information dispensée doit être claire, loyale et appropriée[497]. Enfin, la charte du patient hospitalisé prévoit quant à elle que l'information se doit d'être « *simple, accessible, intelligible et loyale* ».

433. Ces dispositions peuvent, au premier abord, poser problème. En effet, la télémédecine présente la particularité, dans certains cas, de dématérialiser la relation existant entre le professionnel et son patient : ceux-ci n'ont plus réellement de lien direct et s'adressent l'un à l'autre par le biais des outils informatiques. Comment, dans ce cas, le respect d'un entretien individuel, loyal et intelligible, va-t-il être possible ? De même, comment s'assurer que le patient a bien reçu une information adaptée, à la fois à sa situation, mais aussi à ses capacités de compréhension ? Pour certains auteurs, l'obligation de délivrer l'information au cours d'un

---

[495] LE GOFFIC, Caroline. « Consentement et confidentialité à l'épreuve de la télémédecine », RDSS, 2011, pp. 987- 995.

[496] L'article R. 4127-32 du Code de la santé publique dispose « *dès lors qu'il a accepté de répondre à une demande, le médecin s'engage à assurer personnellement au patient des soins consciencieux, dévoués et fondés sur les données acquises de la science, en faisant appel, s'il y a lieu, à l'aide de tiers compétents*. »

[497] L'article 35 du code de déontologie médicale prévoit que « *le médecin doit à la personne qu'il examine, qu'il soigne ou qu'il conseille, une information loyale, claire et appropriée sur son état, les investigations et les soins qu'il lui propose. Tout au long de la maladie, il tient compte de la personnalité du patient dans ses explications et veille à leur compréhension* ».

entretien individuel ne pose pas de réel problème, la notion d'entretien devant s'entendre, selon eux, de manière large pour y inclure les formes électroniques de communication[498]. Il est en réalité nécessaire de revenir sur chacune des activités de télémédecine prévues par le décret d'octobre 2010 afin de tenter d'éclaircir ce point.

434. Pour la téléexpertise, la question ne pose pas réellement de problème. Cette activité s'apparente en réalité à la possibilité pour le professionnel de santé de faire appel à un autre professionnel plus spécialisé si la prise en charge le nécessite. Il s'agit d'une règle prévue au Code de déontologie médicale qui s'impose au médecin[499]. Dans ce cas, le patient n'est pas pris en charge par le biais d'un acte totalement dématérialisé puisque la relation à distance n'a lieu qu'entre deux professionnels de santé. Il pourra donc recevoir l'information qui lui est due dans les conditions classiques et exprimer le consentement relatif à sa prise en charge auprès du médecin requérant. Il en va de même pour la téléassistance : dans ce cas, le patient n'est pas pris en charge à distance mais c'est bien le professionnel qui est assisté par un autre professionnel de façon dématérialisée.

435. Dans le cadre de la réponse en matière de régulation médicale, la particularité de la situation, à savoir l'urgence, fait que cette question ne se pose pas réellement, le professionnel se trouvant alors dans une des situations exceptionnelles lui permettant de ne pas remplir son obligation d'information ni de recueillir le consentement préalable du patient.
Dans le cas de la télésurveillance, la question peut être très rapidement réglée. En effet, ce genre d'activité supposera *a minima* une consultation préalable avec le patient au cours de laquelle le professionnel pourra donc l'informer sur l'acte, le dispositif de télémédecine, le traitement de ses informations personnelles mais également, comme le dispose le décret, le former si nécessaire aux outils et au recueil de ses données. En effet, il est prévu, lorsque la situation l'impose, que le patient soit formé ou préparé à l'utilisation du dispositif de télémédecine.

436. Enfin, la téléconsultation reste la pratique qui pose en réalité le plus de problèmes à ce sujet. En ce qui concerne l'entretien individuel, il est vrai qu'il pourra toujours avoir lieu,

---

[498] *V.* notamment en ce sens LE GOFFIC, Caroline. « Consentement et confidentialité à l'épreuve de la télémédecine », Revue de droit sanitaire et social, 2011, *op. cit.*
[499] Article R. 4127-32 du Code de la santé publique.

même si c'est par le biais d'une webcam. Toutefois, la dématérialisation des relations entre le patient et son médecin ne doit pas pour autant conduire celui-ci à prendre une trop grande distance avec son patient. Il devra donc s'assurer qu'il a bien délivré une information répondant aux obligations légales. Certains auteurs parlent en effet de risque de « *standardisation de l'information* » du fait de la dématérialisation des échanges. C'est cet écueil qu'il faudra veiller à éviter[500]. En tout état de cause, la preuve de l'information sera d'autant plus importante qu'il n'y a pas eu de rencontre formelle entre patient et médecin.

b) La preuve de l'information et du recueil du consentement

437. Dans le cadre de la télémédecine, la question de la preuve, que ce soit de la délivrance de l'information ou de l'obtention du consentement, peut poser certaines difficultés. Le problème ne réside pas vraiment dans les modalités de preuve de l'information qui, en réalité, ne vont pas différer que l'on soit dans le cadre d'un acte de télémédecine ou un acte médical plus "classique". En effet, la charge de la preuve en la matière repose sur le professionnel de santé, qui devra conserver la trace de la délivrance de son information. A ce sujet, la loi[501] comme la jurisprudence[502] ont posé le principe de la preuve de l'information par tous moyens. Ainsi, les écrits peuvent constituer un début de preuve et les échanges de courriels pourront l'être également. Le problème réside ici dans les nouveaux modes de preuves induits par l'utilisation des TIC.

438. La première question qui se pose est celle de l'enregistrement de la téléconsultation en elle-même. Certains auteurs avancent cette possibilité, sous réserve de respecter certaines obligations préalables. Il nous semble toutefois que cette possibilité doive être écartée, pour des raisons à la fois légales et éthiques. En effet, d'un point de vue strictement légal, les dispositions de la loi Informatique et Libertés et notamment le respect du principe de proportionnalité entre le traitement et le but recherché, ne nous semblent pas autoriser un tel enregistrement. De même, d'un point de vue éthique, on comprend très vite qu'un tel enregistrement va fragiliser le colloque singulier et la relation de confiance qui doit exister entre médecin et patient. En revanche, une trace informatique de la consultation pourra être conservée, sous réserve de respecter les différentes obligations de déclarations auprès de la

---

[500] BOURDAIRE-MIGNOT, Camille. « Téléconsultation : quelles exigences ? Quelles pratiques ? », *op. cit.*, p. 1005.
[501] Article L. 1111-2 du Code de santé publique
[502] Cass. 1ère civ, 25 février 1997, n° 94-19.685. Defrénois 1997, p. 751, note J.L. AUBERT.

CNIL. Cette trace pourra donc constituer un début de preuve, en permettant par exemple, de démontrer la durée de la consultation. Le médecin devra donc continuer de préciser, au sein du dossier médical, le contenu de l'information qu'il a délivrée et, éventuellement, la compléter par un document écrit transmis par e-mail. Dans le cadre d'une activité de télémédecine, il appartient, selon nous, au médecin d'être vigilant et de constituer, tout au long de la prise en charge à distance de son patient, un faisceau d'indices, qui permettra d'apporter la preuve de l'information dans l'hypothèse d'un contentieux.

439. Le professionnel devra être d'autant plus attentif à la délivrance de ces informations que la jurisprudence se montre de plus en plus stricte à ce sujet, la Cour de Cassation ayant fait du défaut d'information un préjudice autonome, et le Conseil d'Etat ayant développé la notion de préjudice d'impréparation.

En effet, dans une décision en date du 3 juin 2010[503], la Cour de cassation a consacré l'autonomie du préjudice résultant du défaut d'information. Désormais, l'absence d'information claire et loyale du patient préalablement à l'exécution d'un acte médical constitue un préjudice à part entière qui, comme le précisait la Haute juridiction, ne peut rester sans réparation. Le Conseil d'Etat est quant à lui venu consacrer dans une décision du 10 octobre 2012[504], la notion de préjudice d'impréparation : « *considérant qu'indépendamment de la perte de chance de refuser l'intervention, le manquement des médecins à leur obligation d'informer le patient des risques encourus ouvre pour l'intéressé, lorsque ces risque se réalisent, le droit d'obtenir réparation des troubles qu'il a pu subir du fait qu'il n'a pas pu se préparer à cette éventualité, notamment en prenant certaines dispositions personnelle […]* ». Pour la Haute juridiction administrative, le défaut d'information constitue une perte de chance de se préparer aux risques possibles liés à l'intervention et doit donc être réparé à ce titre. Les droits des patients pris en charge par un dispositif à distance, telle que la télémédecine, restent les mêmes et sont même renforcés sur certains aspects. C'est la même logique qui va trouver à s'appliquer en ce qui concerne les règles existantes en matière de responsabilité.

---

[503] Cass. 1ère civ, 3 juin 2010, n° 09-13.591. A. LEGOUX. *Gaz. Pal*., 2010, pp. 9-13 ; P. SARGOS. « Deux arrêts historiques en matière de responsabilité médicale générale et de responsabilité particulière liée au manquement d'un médecin à son devoir d'information », *D*., 2010, pp. 1522-1526.

[504] CE, 10 octobre 2012, Michel C., n°350426, F. VIALLA. *JCP G*, 2012, p. 1252 ; C. LANTERO. *AJDA*, 2012, p. 2231.

B. Responsabilité médicale : des règles classiques aux risques d'application multipliés

440. Les actes médicaux pratiqués par le biais des TIC, qu'il s'agisse de la télémédecine ou de la prescription informatisée, restent des actes médicaux à part entière et juridiquement reconnus comme tels. De ce fait, il est logique que les règles relatives à la mise en cause de la responsabilité des professionnels et établissements de santé soient les mêmes que celles applicables aux actes médicaux non dématérialisés (1). Toutefois, les spécificités de la télémédecine, notamment le développement de pratiques pluridisciplinaires, amènent à s'interroger sur la répartition des responsabilités entre les différents acteurs (2) qu'ils s'agissent des médecins, des personnels paramédicaux ou même des patients.

1) La responsabilité médicale, une responsabilité pour faute

441. « *Il n'y a pas lieu de créer un régime de responsabilité spécifique autour de la télémédecine* »[505]. Pour la DGOS, il ne fait aucun doute que le régime de droit commun applicable en matière de responsabilité médicale va trouver à s'appliquer à la télémédecine, sans qu'il y ait lieu de clarifier voire même créer de nouvelles règles.

442. Très tôt, la jurisprudence judiciaire a considéré qu'un médecin était responsable des dommages causés à un patient et ce, sur le fondement des articles 1240[506] et 1241[507] du Code civil. Le dommage causé par le médecin à son patient était donc réparable sur le terrain de la responsabilité délictuelle. Cette position a été modifiée par le très célèbre arrêt Mercier du 20 mai 1936[508], par lequel la Haute juridiction est venue affirmer que la relation qui s'établissait entre un médecin et un patient était une relation contractuelle. Ainsi, le non-respect par le médecin d'une de ses obligations engageait alors sa responsabilité contractuelle. Cette position a ensuite été confirmée par plusieurs arrêts, rappelant que les médecins n'engageaient leur responsabilité contractuelle qu'en cas de faute. Ce contrat était un contrat

---

[505] « La télémédecine n'a pas besoin d'un régime de responsabilité professionnelle spécifique, selon la DGOS », dépêche Tic-santé, 15 mai 2012, disponible sur : [http://www.ticsante.com]. Consulté le 3 mars 2017.

[506] « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer* »

[507] « *Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence* ».

[508] Cass. 1ère civ., 20 mai 1936, Mercier, *JCP*, 1936, 1079.

synallagmatique, de droit privé. Ainsi, il pesait des obligations sur chacune des parties. Toutefois, ce contrat n'était valable que pour les soins dispensés par un médecin libéral ou par un médecin exerçant en établissement privé. Dans le cas d'un médecin hospitalier, exerçant en établissement public de santé, on considérait le patient comme étant un usager du service public et dès lors, il relevait d'une situation statutaire[509]. C'est d'ailleurs toujours le cas aujourd'hui. La responsabilité contractuelle du médecin a toutefois continué de coexister avec la possibilité de mettre en œuvre sa responsabilité délictuelle dans certains cas. Ainsi, en cas d'absence de contrat médical *ab initio*[510] ou dans l'hypothèse de son annulation,[511] le patient pouvait tout de même mettre en cause la responsabilité délictuelle du médecin.

443. Le Conseil d'Etat, pour sa part, a longtemps reconnu la responsabilité pour faute du service public hospitalier, distinguant toutefois les fautes simples[512] des fautes lourdes[513]. Cependant, avec l'arrêt BIANCHI[514], la Haute juridiction a admis une possibilité de responsabilité sans faute du service public hospitalier, quand l'exécution de l'acte médical nécessaire au diagnostic ou au traitement du patient présentait un risque, certes connu, mais dont la réalisation était exceptionnelle.

444. La loi du 4 mars 2002[515] unifie le régime de responsabilité médicale, en instaurant un principe de responsabilité pour faute et ce, peu importe que la prise en charge se fasse dans un cadre privé ou public. C'est le principe posé à l'article L. 1142-1 du Code de la santé publique selon lequel : « *hors le cas où leur responsabilité est encourue en raison d'un défaut d'un produit de santé, les professionnels de santé mentionnés à la quatrième partie du présent Code, ainsi que tout établissement, service ou organisme dans lesquels sont réalisés des actes individuels de prévention, de diagnostic ou de soins ne sont responsables des conséquences dommageables d'actes de prévention, de diagnostic ou de soins qu'en cas de faute* ». Il

---

[509] CE, 11 janvier 1991,Mme Biancale, n° 93348, *AJDA*, 1991, p. 479.
[510] Cass. 1ère civ, 20 février 1979, *D*. 1980 p. 171 obs. PENNEAU.
[511] TGI Paris, 3 juin 1979, *D*, 1980, p. 136.
[512] A titre d'exemple, un défaut dans l'organisation du service était considéré comme une faute simple, que l'établissement public de santé se devait de réparer (CE, 26 juin 1959, Rouzet, Rec., 1959, p. 305).
[513] Faute réservée aux actes techniques (CE, 8 novembre 1935, veuve Loiseau, Rec., 1935, p1019).
[514] CE, Ass., 9 avril 1993, Bianchi, n°69336, *RFDA*, 1993, p. 573, concl. S. DAËL ; *RDP*, 1993, p. 1099, note M. PAILLET ; *Rev. Adm*. 1993, p. 561, note P. FRAISSEX.
[515] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, *JORF* du 5 mars 2002, p. 4118.

appartiendra alors au patient qui s'estime victime d'un dommage d'apporter la preuve d'une faute et ce, par tous moyens.

En termes de fautes, celles-ci peuvent être très diverses et porter tant sur la réalisation du soin, que sur le défaut dans l'information préalable du patient. Les fautes peuvent également être strictement médicales, ou parfois résulter d'un dysfonctionnement dans l'organisation du service. Dans le cas particulier de la prise en charge d'un patient en établissement public de santé, par principe, l'établissement devra réparer la faute commise par ses préposés, sauf en cas de faute détachable du service[516].

2) La répartition de la responsabilité entre les différents acteurs de la télémédecine

445. Lors d'un acte de télémédecine, plusieurs scénarios peuvent se mettre en place impliquant, dans la prise en charge du patient, des médecins, des professionnels de santé et parfois même le patient lui-même. La réparation des responsabilités sera différente selon l'acte réalisé (téléexpertise ou téléconsultation par exemple) ou les professionnels impliqués.
La doctrine a beaucoup écrit à ce sujet[517] et plusieurs hypothèses de répartition des responsabilités se sont développées. Celles-ci sont d'ailleurs parfois assez différentes, que l'on se situe du côté du droit privé ou du droit public.
446. Dans le cadre de la pratique de la télémédecine, et plus spécifiquement dans le cas d'actes de téléexpertise ou de téléassistance, il est possible de faire un parallèle avec la situation dans laquelle un médecin demande l'avis d'un confrère. D'une manière générale,

---

[516] La faute détachable a été définie par une décision Tribunal des conflits (Arrêt Pelletier 3 juillet 1873) qui prévoit que la faute détachable est une « *faute médicale plus que lourde, d'une gravité exceptionnelle, et inexcusable, ou n'ayant aucun rapport avec l'activité médicale* ». A titre d'exemple, le Conseil d'Etat, dans sa décision n°213931 du 28 décembre 2001, a reconnu la qualification de faute personnelle détachable du service, pour un médecin chef de service de radiologie qui avait tardé délibérément à révéler une erreur médicale commise dans son service. Sur la faute détachable du service, *V*. notamment : LEFEVRE, Valérie. « La faute détachable du service et la critique d'un médecin sur le travail de l'un de ses confrères dans un établissement de santé ; Note sous Cour de cassation, première Chambre civile, 20 février 2008, Monsieur X contre Mesdames Y, Z et A. et Monsieur B, pourvoi numéro 06-21.980 », *Gaz. Pal*., n° 282-283, 2008, pp. 40-41 ; KLEITZ-BACHELET, Clémentine. « Médecin hospitalier et faute détachable du service », RLDC, n° 48, 2008, p. 27.

[517] *V*. notamment en ce sens : CORGAS-BERNARD, Cristina. « Responsabilité civile médicale et nouvelles pratiques numériques : l'exemple de la télémédecine », *LPA*, n° 162, 2014, pp. 27-30 ; FRAYSSINET, Marie-Hélène. « La faute dans l'organisation et le fonctionnement du service à l'épreuve de la télésanté », *RGDM*, n° 44, 2012, pp. 313-331 ; GRYNBAUM, Luc. « La responsabilité des acteurs de télémédecine », *RDSS*, n° 6, 2011, pp. 996-1002 ; FORGERON, Jean-François, « Les applications de télémédecine : des responsabilités médicales traditionnelles aux responsabilités techniques nouvelles », *Gaz. Pal*., n° 287, 2001, pp. 20-22. ; ROUSSEL, Bruno. « Les applications de télémédecine : des responsabilités médicales traditionnelles aux responsabilités techniques nouvelles », *Communication commerce électronique*, n° 1, 2011, p. 2.

une majorité des auteurs considèrent qu'il existe une responsabilité du médecin qui se trouve auprès du patient, du fait du médecin qui exerce à distance[518]. La téléexpertise est alors considérée comme une aide à la décision médicale[519] et l'acte reste sous la responsabilité du médecin qui a pris en charge le patient, ce qui implique donc une responsabilité exclusive de ce dernier. Finalement, il s'agit ici de l'application des dispositions de l'article R. 4127-69 du Code de la santé publique, qui prévoit que « *l'exercice de la médecine est personnel ; chaque médecin est responsable de ses décisions et ses actes* ». Effectivement, dans le cas spécifique de la téléexpertise, c'est bien au médecin demandeur, qui se trouve à proximité du patient et qui prend en charge ce dernier, qu'il reviendra de prendre la décision médicale, en se basant sur les préconisations du médecin téléexpert.

447. Toutefois, il faut souligner que l'article R. 4127-64 du Code de la santé publique précise quant à lui que « *lorsque plusieurs médecins collaborent à l'examen ou au traitement d'un malade, ils doivent se tenir mutuellement informés, chacun des praticiens assume ses responsabilités personnelles et veille à l'information du malade* ». A la lumière de cette autre disposition du Code de la santé publique, il apparait que médecin requérant et médecin requis devraient naturellement voir leurs responsabilités partagées en cas de dommage subi par le patient. A noter que, classiquement, la jurisprudence retient la responsabilité solidaire des intervenants quand un médecin décide de prendre un avis auprès d'un confrère, spécialiste dans son domaine[520].

448. C'est d'ailleurs, à ce jour, la solution retenue par les juges administratifs en ce qui concerne la pratique de la télémédecine, et plus spécifiquement la pratique de la téléexpertise[521]. En l'espèce, il s'agissait d'un patient hospitalisé au sein d'un centre hospitalier suite à un traumatisme crânien puis autorisé à sortir, le scanner ne révélant aucun traumatisme. Il est hospitalisé de nouveau un mois plus tard à la suite de céphalées inhabituelles et de vomissements. Un nouveau scanner est réalisé et un avis demandé au service de neurochirurgie du Centre Hospitalier Universitaire (CHU) de Grenoble, par le biais

---

[518] CONTIS, Mailen. CROEL, Jean-Marc. « Le droit des obligations à l'épreuve de la télémédecine », *PUAM*, 2006. *V.* également en ce sens, PIDOUX, Estelle. « La responsabilité médicale au regard de la télétransmission et de la télémédecine », *LPA*, n° 149, 2000, pp. 5-11.
[519] *V.* notamment en ce sens, FLAVIN, Patrick. « De la responsabilité encourue dans le cadre de la télémédecine », *Revue hospitalière de France*, n° 537, 2010, p. 56-57.
[520] CAA Bordeaux, 10 octobre 1998, n° 97BX01978.
[521] TA Grenoble, 21 mai 2010, n°0600648.

d'une vidéotransmission des images. Le CHU de Grenoble informe le centre hospitalier qu'il ne dispose pas de place pour accueillir le patient, mais que l'état de celui-ci permettait d'attendre pour réaliser l'opération de drainage de l'hématome découvert. L'état du patient se dégrade le jour suivant mais le CHU maintient son avis initial. Le patient tombe dans le coma. Il est ensuite transféré dans un autre établissement, dans lequel il décède. En se basant sur les expertises médicales réalisées, le TA de Grenoble retient une erreur de diagnostic dans l'interprétation du scanner lors de la réadmission du patient. Alors que le CHU invoque un doute sur la réception de deux planches d'images par son service de neurochirurgie et fait part de son interrogation sur la qualité de celles-ci, le TA pointe le fait qu'aucun élément du dossier ne permet d'établir que les médecins qui les ont reçues et interprétées ont émis, à un moment de la prise en charge, des doutes quant à leur caractère complet et précis. Pour les juges du fond, l'erreur de diagnostic est constitutive d'une faute commune aux deux établissements et engage donc leur responsabilité solidaire. Le TA a également dû statuer sur l'appel en garantie formé par le CH de Sallanches contre le CHU de Grenoble. Les juges du fond rappellent à cette occasion que les centres hospitaliers généraux ne sont pas dotés de moyens spécialisés en neurochirurgie et sont donc amenés à demander l'avis de services spécialisés. Le TA relève ensuite que les télétransmissions d'images n'ont pas donné lieu à des comptes rendus écrits et qu'à aucun moment, les médecins qui ont reçu et interprété les images n'ont émis de doute sur leur qualité. Dès lors, pour le tribunal, le CHU a commis une faute vis-à-vis du CH et doit le garantir de l'ensemble de la condamnation prononcée à son encontre.

449. Il s'agit, selon la doctrine, d'une décision[522] qui préfigure la manière dont la responsabilité des différents intervenants dans le cadre d'une activité de télémédecine pourrait être appréciée par les juges. Avec cette décision, les juges s'orientent vers une responsabilité solidaire des deux médecins intervenant dans la prise en charge du patient. D'ailleurs, il faut noter que la responsabilité solidaire des intervenants, dans le cas d'un médecin prenant un avis auprès d'un spécialiste, avait déjà été retenue auparavant[523].

[522] FLAVIN, Patrick. « De la responsabilité encourue dans le cadre de la télémédecine », *op. cit.*
[523] CAA, Bordeaux, *op. cit.*

Toutefois, il nous faut souligner ici la sévérité de cette décision[524]. En effet, les juges ne se contentent pas de retenir une responsabilité solidaire mais estiment que le CHU, de par sa position d'expert en la matière, se doit de garantir la condamnation du CH. Il appartiendrait donc au téléexpert de s'assurer de la qualité des données qu'il reçoit avant de dispenser son avis. Il doit prendre en compte les limites inhérentes à la pratique et solliciter les informations complémentaires en cas de doute, sous peine de voir sa responsabilité pleinement engagée en cas de préjudice.

450. Une dernière question relative à la responsabilité du médecin dans le cadre de la télémédecine doit encore être soulevée : celle de l'existence éventuelle d'une obligation médicale d'utiliser la télémédecine. En effet, l'article R. 4127-32 du Code de la santé publique fait peser sur le médecin l'obligation de moyens suivante : « *dès lors qu'il a accepté de répondre à une demande, le médecin s'engage à assurer personnellement au patient des soins consciencieux, dévoués et fondés sur les données acquises de la science, en faisant appel, s'il y a lieu, à l'aide de tiers compétents* ». Il s'agit ici de l'obligation légale et déontologique pesant sur tout médecin de faire appel à des tiers compétents. Avec le développement de la télémédecine et, plus particulièrement, de la téléexpertise, il serait possible d'envisager que cette obligation soit étendue à l'utilisation des TIC et notamment de la télémédecine. Un médecin pourrait donc voir sa responsabilité engagée s'il est établi qu'il avait la possibilité d'avoir recours à la télémédecine et qu'il ne l'a pas fait. Toutefois, à l'heure actuelle et au vu du développement de la pratique, il nous semble compliqué de faire peser sur un médecin une telle obligation de moyens.

§2. Télémédecine et responsabilité : des règles spécifiques à prendre en considération

451. L'introduction des TIC dans la prise en charge des patients nous amène à réfléchir sur la nouvelle répartition des responsabilités. En effet, les logiciels vont devenir un outil de la prise en charge médicale à part entière, et ses éventuelles défaillances ne vont pas être sans

[524] *V*. également en ce sens FLAVIN, Patrick. « De la responsabilité encourue dans le cadre de la télémédecine », *op. cit*, p. 57.

conséquence (A). Par ailleurs, il nous faut également nous pencher sur la responsabilité d'un nouvel acteur entrant dans la prise en charge du patient : le tiers technologique (B).

A. Défaillance des logiciels et responsabilités

452. Dans le cadre de l'informatisation constante de la prise en charge médicale, les logiciels informatiques sont devenus un des outils principaux des établissements de santé. Toutefois, cela n'est pas sans conséquence sur les règles applicables en matière de responsabilité médicale. En effet, en introduisant ce nouvel outil, les établissements augmentent les risques de dommage en cas de défaillance de celui-ci. Il leur est donc nécessaire de se pencher sur la question de la réparation des responsabilités. Pour cela, il nous faut nous tourner vers le régime de responsabilité applicable en matière de produits défectueux (2), après avoir pris le soin de se pencher plus spécifiquement sur la qualification juridique des logiciels utilisés (1).

1) Qualification juridique des logiciels

453. Avant 2010 et la transposition en droit français des dispositions issues de la directive européenne 2007/47/CE[525], seuls les logiciels nécessaires au bon fonctionnement d'un dispositif médical étaient considérés comme étant des dispositifs médicaux. L'article L. 5211-1 du Code de la santé publique prévoyait alors : « *on entend par dispositif médical tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels intervenant dans son fonctionnement, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens* ». A l'époque, un logiciel ne pouvait obtenir cette qualification que par association à un dispositif médical.

[525] Directive 2007/47/CE du parlement européen et du conseil du 5 septembre 2007 modifiant la directive 90/385/CEE du Conseil concernant le rapprochement des législations des États membres relatives aux dispositifs médicaux implantables actifs, la directive 93/42/CEE du Conseil relative aux dispositifs médicaux et la directive 98/8/CE concernant la mise sur le marché des produits biocides, JOUE L247/21, 21 septembre 2007.

454. L'ordonnance n° 2010-250 du 11 mars 2010[526] relative aux dispositifs médicaux et transposant les dispositions de droit européen en droit français, a élargi le champ des logiciels pouvant être considérés comme étant des dispositifs médicaux. Désormais, selon les dispositions de l'article L. 5211-1 du Code de la santé publique, sont des dispositifs médicaux : « *tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Constitue également un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques* ».

Ainsi, un logiciel seul, ayant une finalité thérapeutique ou diagnostique, pourra être qualifié de dispositif médical et se voir ainsi appliquer les dispositions relatives à l'encadrement des dispositifs médicaux, que ce soit en matière de sécurité, de contrôle ou de responsabilité. Par ailleurs, comme nous avons pu le voir précédemment, cela permettra de déterminer quel régime de responsabilité sera applicable. Cette classification est donc importante.

455. Toutefois, l'identification va devoir se faire au cas par cas. Ainsi, un simple logiciel de gestion du dossier patient ne pourra pas être considéré comme un dispositif médical, tandis qu'un logiciel d'aide à la prescription, effectuant un calcul de dose de médicament à partir d'une base de données propre au patient, pourra être qualifié de dispositif médical.
En ce qui concerne plus spécifiquement la télémédecine, il nous faut différencier les logiciels nécessaires à la communication à distance, qui ne pourront pas être considérés comme étant des dispositifs médicaux, et les applications ayant pour finalité de piloter des dispositifs médicaux à distance (dans le cadre de la télésurveillance, notamment).

[526] Ordonnance n° 2010-250 du 11 mars 2010 relative aux dispositifs médicaux, *JORF* n°0060 du 12 mars 2010, p. 4870.

456. L'Agence Nationale de Sécurité du Médicament (ANSM)[527] chargée notamment de garantir la sécurité des produits de santé, a apporté, dans une décision rendue le 12 avril 2015[528], quelques précisions quant à la qualification de dispositif médical pour un logiciel. En effet, l'ANSM a suspendu la mise sur le marché d'un logiciel qui n'était pas revêtu du marquage CE, obligation à laquelle doivent répondre les dispositifs médicaux. Il s'agissait d'un logiciel d'enregistrement et de stockage de données issues d'examens médicaux du patient, accompagné d'un module de compression et d'enregistrement d'images médicales au format "waaves". C'est ce module spécifique qui a posé problème à l'ANSM, celle-ci considérant que ce module, aidant le médecin qui devait procéder à un examen, tombait sous le coup de la définition des dispositifs médicaux de classe 2 et devait, de ce fait, en respecter les exigences.

2) Responsabilité du fait des produits défectueux

457. Dans le cadre de l'utilisation de logiciels, dispositifs médicaux, par des établissements de santé, ceux-ci peuvent être amenés à endosser le rôle de prestataire de service vis-à-vis du patient. Or, en la matière, les règles de répartition des responsabilités entre fournisseur et producteur n'ont pas toujours été très claires.

458. L'articulation des règles applicables du fait de la défaillance des produits de santé a longtemps été difficile à appréhender. D'un côté, le régime européen impose de rechercher de manière prioritaire la responsabilité du producteur du produit défectueux et, d'un autre côté, le régime français, issu d'une construction jurisprudentielle, prévoit la responsabilité sans faute de l'établissement de santé, en tant que prestataire du produit défectueux. Il apparait donc difficile d'articuler les deux régimes applicables.

---

[527] L'Agence nationale de sécurité du médicament et des produits de santé (ANSM) a été créée par la loi du 29 décembre 2011 relative au renforcement de la sécurité sanitaire des médicaments et des produits de santé. Elle s'est substituée à l'Agence française de sécurité sanitaire du médicament et des produits de santé (Afssaps) dont elle a repris les missions, droits et obligations. Il s'agit d'un établissement public, placé sous la tutelle du Ministère chargé de la santé.

[528] Décision du 12 janvier 2015 portant suspension de mise sur le marché, de mise en service, d'exportation et de distribution, du produit Infocament, intégrant un module de compression d'images au format Waaves, fabriqué et mis sur le marché par la société CIRA.

459. En effet, la directive européenne 85/374[529], transposée par la loi n° 98-389 du 19 mai 1998, a créé un régime spécial de responsabilité sans faute du fait des produits défectueux. Ainsi, l'article 1245 du Code civil prévoit que « *Le producteur est responsable du dommage causé par un défaut de son produit, qu'il soit ou non lié par un contrat avec la victime* ».

Dès lors, en vertu de cette directive, le producteur est responsable de la défectuosité d'un produit, même en l'absence de faute. Le fournisseur peut, quant à lui voir sa responsabilité recherchée, soit sur le fondement de la responsabilité sans faute, à condition que le producteur ne soit pas connu, soit sur le fondement de la responsabilité contractuelle ou délictuelle. Cette directive n'écarte toutefois pas la possibilité pour ce régime de coexister avec des régimes de responsabilité spéciaux qui pourraient exister en droit interne à condition que ce régime existe au moment de la notification de la directive[530].

460. Par ailleurs, en droit français, le Conseil d'Etat a instauré une responsabilité du service public hospitalier du fait de la défaillance des produits et appareils de santé[531]. Classiquement, avant cette décision, la jurisprudence distinguait la mauvaise utilisation d'un produit de santé de sa défaillance. Ainsi, si aucune erreur d'utilisation n'était imputable à l'équipe médicale, le juge considérait qu'il n'était pas possible de retenir une faute dans l'organisation du service[532]. Puis, la jurisprudence est devenue plus favorable aux patients et les juges[533] ont eu tendance à s'orienter vers un régime de présomption de la faute[534]. Enfin, avec son arrêt en date du 9 juillet 2003, la Haute juridiction administrative a instauré un véritable régime de responsabilité sans faute du fait de la défaillance des produits de santé. Désormais, le service public hospitalier est responsable des conséquences dommageables pour les usagers d'une défaillance d'un produit ou appareil de santé qu'il utilise, même en l'absence de faute de sa part et ce, sans préjudice de son recours en garantie à l'encontre du producteur. Pour reprendre les termes de Jérôme PEIGNE, « *l'établissement de santé n'intervient plus comme*

---

[529] Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux, *JOUE* n° L 210 du 7 août 1985, pp. 29 – 33.
[530] Article 1 de la directive 85/374/CEE.
[531] CE, 9 juillet 2003, APHP c/ Marzouk, n°220437, Rec., 2003, p. 338 ; *Droit Administratif*, n° 11, novembre 2003, comm. 226.
[532] CE, 14 décembre 1984, Centre Hospitalier de Melun, n° 37563.
[533] *V*. notamment en ce sens CAA Bordeaux, 9 mai 1989, Centre Hospitalier de Castelnaudary, n° 89 BX00002; CAA paris, 11 février 1992, Administration générale de l'Assistance publique à Paris, n° 90PA00256.
[534] PEIGNE, Jérôme. « Les tribulations de la responsabilité hospitalière du fait des produits de santé défectueux », *RDSS*, 2011, pp. 95-104.

l'auteur d'un diagnostic ou le dispensateur d'un traitement, mais comme le fournisseur au patient d'un produit dont il doit répondre »[535].

461. Toutefois, la Cour administrative d'appel de Lyon[536] a été amenée à se poser la question de la compatibilité de la directive européenne avec la jurisprudence du Conseil d'Etat. Dès lors, « *dans l'hypothèse de l'incompatibilité entre les deux régimes de responsabilité, La Cour Administrative d'appel de Lyon devait se demander si le régime jurisprudentiel défini par le Conseil d'Etat pouvait être considéré comme un régime "spécial" préexistant au sens de l'article 1 précité de la directive, de sorte que les deux régimes pourraient coexister de sorte que la victime pourrait , selon ce qui lui est plus favorable, opter pour l'un ou l'autre* »[537]. Ainsi, dans sa décision du 23 mars 2010, la Cour Administrative d'Appel de Lyon rappelle d'abord que lorsqu'un centre hospitalier fournit un produit défectueux à un patient, mais que son producteur est connu, seul ce dernier est responsable des dommages causés par le produit défectueux. Elle considère alors que le régime instauré par le Conseil d'Etat ne peut pas être considéré comme étant un régime spécial de responsabilité au sens de l'article 13 de la directive et écarte alors l'application de la jurisprudence MARZOUK au cas qui lui était soumis. Puis, dans une décision du 4 octobre 2010[538], le Conseil d'Etat, qui était confronté à un problème similaire, a décidé de surseoir à statuer jusqu'à ce que la Cour de justice de l'Union européenne se prononce sur la question suivante : « *compte tenu des dispositions de son article 13, la directive 85/374/CEE du 25 juillet 1985 permet-elle la mise en œuvre d'un régime de responsabilité fondé sur la situation particulière des patients des établissements publics de santé, en tant qu'il leur reconnait notamment le droit d'obtenir de ces établissements, en l'absence même de faute de ceux-ci, la réparation des dommages causés par la défaillance des produits et appareils qu'ils utilisent, sans préjudice de la possibilité pour l'établissement d'exercer un recours en garantie contre le producteur ?* »

---

[535] PEIGNE, Jérôme. « Les tribulations de la responsabilité hospitalière du fait des produits de santé défectueux », *op. cit*. p. 96.
[536] CAA Lyon, 23 mars 2010, M.F c/ CHU de Chambéry, n° 06LY01195.
[537] VINET, Camille. « Responsabilité de l'hôpital du fait des produits défectueux ? », *AJDA*, 2010, p. 1485-1487.
[538] CE, 4 octobre 2010, Centre hospitalier universitaire de Besançon, n° 327449.

462. Dans une décision en date du 21 décembre 2011[539], la CJUE, en clarifiant le champ d'application de la directive 85/374 du 25/05/1985 relative à la responsabilité du fait des produits défectueux, apporte des précisions quant à la responsabilité des établissements publics de santé en tant que prestataires de service.

Le litige opposait le CHU de Besançon à un patient au sujet de l'indemnisation de brûlures qui lui avait été causé par un matelas chauffant dont le système de régulation de température était défectueux. Par jugement du 27 mars 2007, le CHU avait été condamné par le TA de Besançon à réparer le dommage causé au patient en lui versant la somme de 9000 Euros (ainsi que 5974,99 Euros à la CPAM du Jura). L'appel que le CHU avait formé à l'encontre de cette décision ayant été rejeté, il s'était donc pourvu en cassation et le CE avait décidé de surseoir à statuer. La CJUE a considéré que: « *la responsabilité d'un prestataire de service qui utilise, dans le cadre d'une prestation de services telles que des soins dispensés au milieu hospitalier, des appareils ou des produits défectueux dont il n'est pas le producteur au sens de la directive 85/374 et cause, de ce fait, des dommages au bénéficiaire de la prestation ne relève pas du champ d'application de cette directive. Cette dernière ne s'oppose dès lors pas à ce qu'un Etat membre institue un tel régime , tel que celui en cause au principal, prévoyant la responsabilité d'un tel prestataire à l'égard des dommages ainsi occasionnés, même en l'absence de toute faute imputable à celui-ci, à condition, toutefois, que soit préservée la faculté pour la victime et/ou ledit prestataire de mettre en cause la responsabilité du producteur sur le fondement de ladite directive lorsque se trouvent remplies les conditions prévues par celle-ci.* »

463. Ainsi, la juridiction européenne renforce ici les droits des usagers puisque ceux-ci auront la possibilité de mettre en cause à la fois la responsabilité de l'établissement de santé, en sa qualité de prestataire de service sur le fondement de la responsabilité du service public hospitalier du fait de la défaillance des produits et appareils de santé, mais également la responsabilité du producteur du produit de l'appareil défaillant, sur le fondement de l'article 1245 du Code civil. Dans l'hypothèse d'un logiciel qualifié de dispositif médical, qui se révélerait défectueux, ce sont donc ces dispositions qui trouveraient à s'appliquer.

---

[539] CJUE, arrêt de la Cour (grande chambre) du 21 décembre 2011. Centre hospitalier universitaire de Besançon contre Thomas Dutrueux et Caisse primaire d'assurance maladie du Jura. Demande de décision préjudicielle: Conseil d'État - France. Affaire C-495/10.

Mais l'utilisation des TIC dans la prise en charge médicale n'induit pas seulement l'utilisation de nouveaux outils. Elle est également synonyme de l'arrivée de nouveaux acteurs.

B. Nouveaux acteurs et nouvelles responsabilités

« *Le CNOM attire donc l'attention sur le fait que les prestataires techniques susceptibles d'intervenir dans une application de télémédecine sont nombreux : fabricants de matériels, mais aussi fournisseurs de solutions logicielles, opérateurs de télécommunications, sociétés de maintenance. Chacun d'eux porte la responsabilité correspondant à sa prestation.*»[540]

464. Comme l'indique, à juste titre, le CNOM dans son livre blanc sur la télémédecine, la télémédecine et même, plus généralement, l'utilisation des TIC dans la prise en charge du patient a, pour conséquence de faire intervenir plusieurs prestataires techniques dans la mise en place, l'organisation et la réalisation de l'acte médical. Ainsi, désormais un nouvel acteur intervient, susceptible lui aussi d'engager sa responsabilité en cas de dommage : le tiers technologique. Cette notion, bien que couramment utilisée, n'a pas de réelle définition légale. D'ailleurs, le décret télémédecine d'octobre 2010 reste muet à son sujet. Il faut donc, une fois de plus, nous tourner vers les règles de droit commun afin de tenter de délimiter les responsabilités de ce tiers technologique, dans l'hypothèse où un patient subirait un préjudice imputable à une défaillance du matériel ou à l'installation informatique utilisée.

465. Un logiciel d'aide à la prescription ou un dispositif de télémédecine perdent leur intérêt et peuvent même devenir dangereux s'ils sont mal utilisés par les professionnels de santé. Nous ne nous attarderons pas ici sur les hypothèses d'utilisation inadéquate (ignorance des dispositifs de sécurité par exemple) ou négligente (absence de contrôle de la prescription du LAP par le professionnel de santé), qui entraineraient la mise en cause de sa responsabilité par les juges. Nous préférons étudier ici l'hypothèse d'une mauvaise utilisation liée à un défaut d'information ou de formation de la part du tiers technologique.

---

[540] Livre blanc du CNOM sur la télémédecine, 2009, p 12, disponible sur [http://www.conseil-national.medecin.fr]. Consulté le 15 mai 2017.

466. En ce qui concerne la responsabilité médicale du tiers technologique, certains auteurs ont très tôt imaginé de soumettre le fournisseur de matériel à l'obligation de conseil renforcé[541]. En effet, le caractère innovant des solutions et applications proposées par ces prestataires, ainsi que le caractère "profane" des professionnels de santé comme des établissements de santé en la matière renforce, selon la doctrine, l'obligation de conseil pesant sur le tiers technologique.

Cette théorie nous semble, au premier abord, très logique. Elle est finalement l'application aux TIC en santé, des règles classiques applicables en droit de la consommation[542] et développées depuis longtemps par la jurisprudence. Tout comme le médecin est redevable d'une obligation d'information vis-à-vis de son patient, le tiers technologique serait quant à lui redevable d'une obligation de conseil et d'information vis-à-vis du médecin. Cette obligation d'information va même plus loin, puisque son respect passe également par l'obligation, pour le vendeur, de se renseigner. En effet, celui-ci se doit s'informer au sujet de l'usage que l'acheteur entend faire du produit destiné à la vente[543]. A charge, pour l'acheteur, d'informer le vendeur d'un éventuel usage inhabituel de la chose vendue qu'il envisagerait d'effectuer[544]. Ce devoir d'information est même, pour les juges de la Haute juridiction, un devoir de conseil : le vendeur ne doit pas se contenter de renseigner l'acheteur sur le produit, il doit également accompagner cette information de conseils, notamment au sujet du caractère adapté du bien par rapport aux besoins de l'acheteur.

---

[541] FORGERON, Jean-François. BELAY, Nathalie. « Les applications de la télémédecine : des responsabilités médicales traditionnelles aux responsabilités techniques nouvelles », *Gaz. Pal*., 16 octobre 2001, n° 289, p. 20.

[542] L'article L. 111-1 du Code de la consommation prévoit que : « *avant que le consommateur ne soit lié par un contrat de vente de biens ou de fourniture de services, le professionnel communique au consommateur, de manière lisible et compréhensible, les informations suivantes :*
1° Les caractéristiques essentielles du bien ou du service, compte tenu du support de communication utilisé et du bien ou service concerné ;
2° Le prix du bien ou du service, en application des articles L. 113-3 et L. 113-3-1 ;
3° En l'absence d'exécution immédiate du contrat, la date ou le délai auquel le professionnel s'engage à livrer le bien ou à exécuter le service ;
4° Les informations relatives à son identité, à ses coordonnées postales, téléphoniques et électroniques et à ses activités, pour autant qu'elles ne ressortent pas du contexte, ainsi que, s'il y a lieu, celles relatives aux garanties légales, aux fonctionnalités du contenu numérique et, le cas échéant, à son interopérabilité, à l'existence et aux modalités de mise en œuvre des garanties et aux autres conditions contractuelles. La liste et le contenu précis de ces informations sont fixés par décret en Conseil d'Etat. ».

[543] Cass. com, 1er décembre 1992, n° 90-18238 : « *tout vendeur d'un matériel doit, afin que la vente soit conclue en connaissance de cause, s'informer des besoins de son acheteur et informer ensuite celui-ci des contraintes techniques de la chose vendue et de son aptitude à atteindre le but recherché* ».

[544] Cass. 1ère civ. 20 juin 1995, n° 93-15801.

Cependant, ce raisonnement repose en partie sur le faible niveau d'expérience des professionnels en la matière. Or, avec le développement rapide de ces solutions, ainsi que leur utilisation croissante, il nous faut nous poser la question de la relativité du caractère profane des professionnels en la matière. En effet, aujourd'hui certains établissements, en lien direct avec les médecins, sont à l'origine de la conception de solutions innovantes ; dès lors, est-il toujours légitime d'envisager une obligation de conseil renforcée. Quand Jean-François FORGERON et Nathalie BELAY ont développé leur raisonnement, en 2001, il reposait notamment sur le postulat suivant : « *le faible développement sur le marché des solutions de télémédecine induit un faible niveau d'expérience des professionnels de santé intéressés, et accroît corrélativement le périmètre de l'obligation de conseil des prestataires.* ». Or ce n'est clairement plus le cas aujourd'hui. Dès lors, peut-on toujours considérer aujourd'hui les professionnels de santé et surtout, les établissements de santé, comme des "profanes", c'est-à-dire comme de simples consommateurs, en matière de TIC en santé ?

467. Jusqu'à la loi du 17 mars 2014, dite loi HAMON[545], il n'existait pas de définition légale de la notion de consommateur. Cette loi a introduit au Code de la consommation un article préliminaire qui prévoit que : « *au sens du présent code, est considérée comme un consommateur toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale* ». Cependant, cette définition ne concerne que les personnes physiques et non les personnes morales. Quid de celles-ci ? Pour répondre à cette question, il nous faut nous tourner vers la jurisprudence. Ainsi, la Haute juridiction civile, en s'appuyant sur la notion de « non-professionnel » que l'on peut retrouver au sein du Code de la consommation[546], a reconnu, dans un arrêt du 15 mars 2005[547], que les personnes morales n'étaient pas exclues du dispositif légal de protection contre les clauses abusives. Pour la jurisprudence, une personne morale peut donc être considérée comme étant un non-professionnel, notion toutefois distincte de celle de consommateur, mais pouvant bénéficier à ce titre, de certaines protections prévues par le Code de la consommation. Le critère retenu pour qualifier une personne morale d'acheteur professionnel ou non professionnel est celui du lien de l'achat avec l'activité exercée. La personne morale qui, pour

[545] Loi n° 2014-344 du 17 mars 2014 relative à la consommation, *JORF* n°0065 du 18 mars 2014, p. 5400.
[546] Article L. 132-1 du Code de la consommation.
[547] Cass, 1ère civ, 15 mars 2005, n° 02-13285, D. 2005, *AJ*, p. 887, obs. RONDEY, Céline.

les besoins de son activité, conclurait un contrat dont l’objet ne relève pas de l’activité qu’elle exerce, est donc considérée comme non professionnelle.

Dans notre cas, un établissement de santé, qui, pour la prise en charge de ses patients, conclut un contrat avec un prestataire informatique pourrait donc être considéré comme non professionnel et, à ce titre, bénéficier de la protection contre les clauses abusives.

Conclusion de section

468. La prise en charge à distance des patients, par le biais des TIC, n'induit pas l'existence de nouveaux droits et c'est bien le droit commun applicable à tout acte médical qui va trouver à s'appliquer aux activités telles que la télémédecine ou la prescription informatisée. Les règles de responsabilité médicale restent également inchangées. Néanmoins, l'introduction des TIC induit l'intervention, au sein de la pratique médicale, de nouveaux outils mais également de nouveaux acteurs qui doivent être pris en compte. De ce fait, les règles de responsabilité applicables peuvent s'en trouver bousculées, notamment dans leur répartition entre les différents acteurs.

La difficulté, pour les établissements de santé, va résider dans l'identification des différentes règles applicables, qui, comme nous l'avons vu, sont nombreuses et dont l'articulation n'est pas toujours aisée à appréhender.

Conclusion du chapitre

469. Les TIC servent aujourd'hui à la prise en charge à distance des patients et les actes réalisés dans ce cadre bénéficient d'une véritable et solide reconnaissance juridique. Cependant, le droit peine parfois à trouver sa place dans cette organisation. En effet, il ne peut pas devancer la technique, au risque de la freiner. Mais il ne peut pas trop tarder non plus à venir poser un cadre nécessaire au bon développement de ces pratiques. Dans le cas de la télémédecine, le législateur a tenté d'être le plus concis et précis à la fois, certainement pour ne pas alourdir une pratique déjà bien en place depuis une vingtaine d'années. Cependant, la procédure institutionnelle mise en place n'a pas l'effet escompté, étant semée de lourdeurs administratives. La simplification des démarches, mais également la clarification du cadre financier de l'activité, sont deux pistes à explorer afin que la télémédecine puisse s'épanouir comme il se doit.

470. Les établissements de santé sont également fortement incités à s'attaquer à un autre chantier important, celui de l'informatisation du circuit du médicament. Mais les établissements de santé et les professionnels de santé, ne doivent pas oublier qu'ils disposent, depuis plus de dix ans maintenant, de la possibilité de dématérialiser leurs prescriptions médicales. Cette possibilité est malheureusement trop peu exploitée à ce jour. Du point de vue de la responsabilité médicale, ces pratiques ne changent rien aux fondamentaux applicables en droit de la santé. Cependant, il faut aujourd'hui prendre en compte les nouveaux outils à disposition des professionnels de santé que sont les logiciels médicaux, ainsi que les nouveaux acteurs que sont les tiers technologiques, dans l'application des règles de responsabilité.

Conclusion du titre

471. L'utilisation des TIC dans la pratique médicale permet la dématérialisation des échanges avec le patient. Les établissements de santé développent ainsi leurs DME, permettant le partage des données informatisées du patient. Dans ce contexte, un seul DME bénéficie d'un cadre juridique qui lui est propre : le DMP. Fruit de la volonté du législateur de mettre en place un dossier médical partagé au niveau national, dont le patient serait titulaire, ce projet ambitieux n'a cependant pas réussi à trouver sa place, après plus de dix ans d'existences et plusieurs relances.

472. La dématérialisation de la prise en charge du patient conduit également au développement de pratiques médicales à distance comme la télémédecine. Ces pratiques évoluent d'ailleurs dans un cadre juridique assez clair. Cependant, même si les règles en matière de droit du patient et de responsabilité médicale restent inchangées, leur application peut se trouver quant à elle modifier, de nouveaux outils et de nouveaux acteurs entrant en jeu. Les établissements de santé doivent donc appréhender ces nouvelles activités dans leur globalité afin de comprendre l'ensemble des conséquences juridiques qu'elles peuvent impliquer.

Conclusion de la première partie

« *Le droit n'est pas perplexe ni désarçonné devant l'innovation, il la réduit au déjà connu* »[548].

473. Les TIC, outils en constantes évolutions, induisent de nombreux avantages qualitatifs et financiers en terme de prise en charge médicale, ceci n'est plus à démontrer. Mais ils induisent également des risques (notamment en ce qui concerne la confidentialité des données et la protection de la vie privée du patient) et sont, à l'évidence, sources de grands bouleversements pour la pratique médicale. Dans ce contexte, le développement croissant de la dématérialisation de la prise en charge du patient a conduit le législateur à se pencher sur ces pratiques. Exercice difficile pour ce dernier, qui doit se soucier de créer un cadre propice au développement de ces pratiques, tout en veillant à protéger les droits fondamentaux des patients et à assurer aux établissements et aux professionnels de santé la sécurisation de leurs activités. Or, à l'heure actuelle, le cadre juridique applicable à l'utilisation des TIC dans la pratique médicale ne permet pas d'assurer cet équilibre délicat. Les établissements de santé peuvent rapidement se perdre dans les méandres des différentes règles de droit général et de droit spécial qui trouvent à s'appliquer et certains projets se trouvent freinés ou restreints.

474. Bien que nous ne considérions pas qu'il soit nécessaire de créer un cadre juridique spécifique à l'utilisation des TIC en santé, une rénovation du cadre juridique pourrait être entreprise. Cependant, les voies de sécurisation des pratiques en la matière sont multiples et l'ensemble doit être repensé dans sa globalité.

[548] LYON-CAEN, Gérard. « Débat autour de l'arrêt Nikon France », Semaine Sociale Lamy, nº 1046, 15 octobre 2001. Disponible sur [http://lamyline.lamy.fr]. Consulté le 16 janvier 2017.

SECONDE PARTIE

LES VOIES DE SECURISATION DE L'UTILISATION DES TIC A L'HOPITAL

« *Les transformations induites par l'avènement du numérique dans la santé doivent cependant s'accomplir dans un cadre de confiance renouvelé et adapté* ».[549]

475. Le succès du développement de l'utilisation des TIC dans la pratique médicale dépend de plusieurs facteurs. Une technique suffisamment mûre pour être mise en place, un modèle économique viable et satisfaisant pour l'ensemble des acteurs, un cadre juridique adapté en font partie. La confiance des utilisateurs - patients et professionnels - vis-à-vis des outils est également l'un des facteurs essentiels au bon développement des TIC en santé. Aujourd'hui pourtant, un français sur deux exprime leur méfiance vis-vis des pratiques de santé dématérialisée, craignant une menace pour le secret médical[550]. De même, certains professionnels de santé se montrent encore réticents à l'utilisation des TIC, qui bouleversent des pratiques ancrées depuis bien longtemps[551]. Pourtant, la confiance et l'adhésion des professionnels et des établissements de santé à ces nouvelles pratiques est essentielle pour pouvoir les diffuser et les faire évoluer. Pour assurer un développement serein et pérenne de l'utilisation des TIC en santé, les établissements de santé doivent pouvoir œuvrer dans un contexte sécurisé et donc rassurant. Or, aujourd'hui, l'informatisation croissante de la pratique médicale crée de nombreuses interrogations juridiques, éthiques et déontologiques, auxquelles les établissements et les professionnels de santé n'ont pas toujours de réponse fiable. De même, le manque de vision globale du développement de l'utilisation des TIC dans la pratique médicale ne permet pas de donner aux différentes initiatives le poids et les ressources nécessaires à leur développement pérenne.

476. Ce contexte d'insécurité pour les établissements de santé n'est pas sans issue et plusieurs voies existent pour permettre de sécuriser l'utilisation des TIC en santé. La première voie repose sur les pouvoirs publics et leur capacité à impulser cette démarche de sécurisation, en prenant le soin d'offrir aux TIC en santé une gouvernance forte d'une part (chapitre premier) et en rénovant le cadre juridique applicable (chapitre second). La seconde voie de sécurisation repose sur les établissements de santé eux-mêmes, qui, au cœur des pratiques, sont les plus à-même de les sécuriser (chapitre premier). En la matière, l'exemple du CHRU de Lille peut être exposé (chapitre second).

---

[549] CNOM. « Dématérialisation des documents médicaux », 2010, p. 4.
[550] « E-santé, la médecine à l'ère du numérique », *Science et santé*, n° 29, 2016, p. 33.
[551] *Ibid*.

TITRE 1

L'IMPULSION DE LA SECURISATION AU NIVEAU NATIONAL

« *Faute d'une volonté politique forte et constante sur une durée suffisante et d'une gouvernance unifiée, l'e-santé et ses usages semblent donc condamnés à progresser de façon chaotique, au gré des annonces.* »[552]

477. Les pouvoirs publics ont un rôle essentiel à jouer en ce qui concerne le développement des TIC en santé. En effet, dans le contexte particulier de la santé, fortement régulé, l'action des pouvoirs publics en la matière est essentielle[553]. Ainsi, une des voies de sécurisation de l'utilisation des TIC dans la pratique médicale repose sur l'impulsion que les pouvoirs publics pourront donner en la matière.

Régulièrement, l'absence d'une autorité forte de pilotage en matière de développement des TIC dans la pratique médicale est pointée du doigt. Or, il s'agit d'un élément essentiel pour s'assurer de la mise en œuvre d'une action coordonnée. C'est pourquoi la priorité doit être aujourd'hui donnée à la pérennisation d'une gouvernance solide en matière de TIC en santé (chapitre premier).

En parallèle, le cadre juridique de l'utilisation des TIC en santé doit être repensé. Comme nous l'avons constaté, il nous faut aujourd'hui « *recourir à une multitude de codes différents pour aborder dans sa globalité la seule question des systèmes d'information de santé* »[554]. Ceci est alors source d'insécurité juridique pour les acteurs et notamment les établissements de santé. Une rénovation de ce cadre juridique s'impose donc (chapitre second).

---

[552] ROBIN, Jean-Yves. « L'urgence numérique. Faire de la France un leader de l'e-santé. », *L'Harmattan*, 2015. p. 168.
[553] *Ibid.*
[554] ROBIN, Jean-Yves. « L'urgence numérique. Faire de la France un leader de l'e-santé. », *op. cit.* p. 193.

Chapitre 1

Une gouvernance forte des systèmes d'information en santé, une priorité

« *Administrer n'est pas gouverner et l'e-santé a plus besoin d'être gouvernée qu'administrée* »[555].

478. Cette citation de Jean-Yves ROBIN, ancien directeur de l'ASIP santé, n'est pas anodine. Elle est révélatrice du problème majeur dans le développement de l'e-santé en France. En invoquant ce qu'il appelle la « *tentation gestionnaire* » de l'Etat en matière d'e-santé, l'auteur souligne l'absence d'une réelle conduite par l'Etat des projets d'e-santé, pourtant nécessaire à un développement efficace et cohérent.

Afin que l'e-santé en France se développe de manière unifiée et pérenne, une impulsion, mais également un cadre national doivent être instaurés. Or, la cartographie actuelle de la gouvernance apparait comme complexe, voire parfois illisible (Section I) et il est essentiel que des choix clairs soient rapidement effectués et un équilibre trouvé afin d'instaurer une gouvernance efficace (Section II).

[555] ROBIN, Jean-Yves. « L'urgence numérique. Faire de la France un leader de l'e-santé », *op. cit.*, p. 88.

Section 1. L'éparpillement notable de la gouvernance actuelle

479. En matière d'organisation de la gouvernance de l'e-santé, l'Etat a passé son temps à éparpiller les rôles et les pouvoirs (Paragraphe I) en fonction des différents projets. Aujourd'hui, bien qu'une gouvernance refondue soit en place, la visibilité sur les projets en cours et leur gestion reste délicate (Paragraphe 2).

§1. Des difficultés pour instaurer une gouvernance stable et efficace

480. La question de la gouvernance des projets d'e-santé en France fait débat depuis de nombreuses années. Le chantier n'est pas des moindres puisqu'il s'agit d'encadrer, de conduire et de mener à termes des projets relatifs à des systèmes d'informations (SI) différents (SI des médecins de ville, SI hospitaliers, SI de l'assurance maladie). Notons cependant que tout au long de notre développement, nous nous attacherons plus particulièrement à la gouvernance des systèmes d'information de santé hospitaliers, bien que les systèmes d'information de santé recouvrent un domaine bien plus large.

Avant d'étudier les critiques qui ont pu être formulées au sujet des choix de gouvernance des systèmes d'information de santé hospitaliers (B), il nous est nécessaire de faire un point sur l'historique en la matière (A). Il s'agira ensuite d'exposer, pour conclure, les propositions d'évolution qui ont pu être faites (C).

A. L'évolution de la gouvernance des systèmes d'information en santé en France

481. De manière schématique, la mise en place de la gouvernance des systèmes d'information en santé (SIS) a conduit à l'émergence de deux types d'acteurs : d'une part, les structures de coordination (1) et d'autre part, les structures opérationnelles (2).

1) Les structures de coordination

482. Très tôt, le Ministère de la santé avait souhaité encadrer le développement de l'informatique en santé. A titre d'exemple, l'informatisation des hôpitaux publics avait fait l'objet de deux circulaires[556]prônant l'intérêt d'assurer une cohérence nationale en termes de gouvernance, mais également de données partagées et donc d'interopérabilité. Pourtant, le pilotage global des politiques d'informatisation du secteur de la santé avait été, dès 2007, considéré comme défaillant par la commission des finances du Sénat[557]. Ce constat faisait suite à un contrôle de la Cour des comptes sur l'interopérabilité des systèmes d'information en santé[558], ainsi qu'au chapitre X du rapport annuel de la Cour des comptes sur l'application des lois de financement de la sécurité sociale, paru en septembre 2007 et portant sur « le partage des données entre les systèmes d'information »[559].

483. En 2009, deux rapports[560], commandés par le Ministre de la santé de l'époque, Madame Roselyne BACHELOT-NARQUIN, présentaient également un regard assez dur sur l'état des lieux de la gouvernance des systèmes d'information de santé en France. Pour comprendre la raison de ces critiques, il est important de revenir sur les acteurs prenant part, à cette époque, à la gouvernance des systèmes d'information de santé hospitaliers.

a) La Mission pour l'informatisation du système de santé

484. La Mission pour l'informatisation du système de santé (MISS), créée en 1997, quelques temps après le Conseil Supérieur des Systèmes d'Information de Santé[561] (CSSIS)[562], avait pour mission de coordonner l'ensemble des projets relatifs à

---

[556] Circulaire n°16 du 18 novembre 1982 ; circulaire n° 275 du 6 janvier 1989 relative à l'informatisation des hôpitaux publics, non parue au *JORF*.

[557] JÉGOU, Jean-Jacques. « Systèmes d'information de santé : le diagnostic est posé, le traitement s'impose », rapport d'information fait au nom de la commission des finances, n° 35, *Sénat*, 2007.

[558] Cour des comptes, « L'interopérabilité des systèmes d'information en santé », référé n° 46485, observations définitives adressées au Ministre de la santé et des solidarités, 2006.

[559] Cour des Comptes, « La sécurité sociale », rapport annuel, chapitre X, 2007.

[560] GAGNEUX, Michel. « Refonder la gouvernance de la politique d'informatisation du système de santé - Douze propositions pour renforcer la cohérence et l'efficacité de l'action publique dans le domaine des systèmes d'information de santé », *La documentation Française*, 2009 et FIESHI, Marius, « La gouvernance de l'interopérabilité sémantique est au cœur du développement des systèmes d'information en santé », *La Documentation Française*, juin 2009.

[561] Décret n° 97-20 du 14 janvier 1997 portant création d'un Conseil supérieur des systèmes d'information de santé, *JORF* n°12 du 15 janvier 1997, p. 712.

[562] Ce conseil, qui avait pour mission d'émettre des recommandations et des avis sur les problèmes liés à la production, à la transmission et aux modalités d'exploitation des informations relatives aux soins et à la santé des personnes, a été mis en sommeil en 2000. L'article 5 du décret n°2003-462 du 21 mai 2003 relatif aux

l'informatisation du système de santé, en lien notamment avec les différentes directions du ministère concerné. Pour ce faire, un chargé de mission pour l'informatisation du système de santé avait été nommé. Trois champs prioritaires avaient été identifiés dans ses missions : les projets relatifs à la CPS, le projet SESAM-Vitale et l'informatisation du poste de travail des professionnels de santé[563].

485. Dans le cadre de son contrôle[564] portant sur l'interopérabilité des systèmes d'information en santé, la Cour des comptes s'était intéressée à la MISS qui, sur le papier tout du moins, faisait figure d'organe central dans la gouvernance de l'informatisation du système de santé. Cependant, il est très vite apparu que la MISS n'était pas en capacité de remplir les missions qui lui avaient été confiées. Cela résultait, d'une part, d'un manque de légitimité et, d'autre part, d'un manque de moyens. Le manque de légitimité a d'ailleurs été souligné au long des différents rapports relatifs à l'informatisation du système de santé. Alors que l'IGAS, dans son rapport de 2002, soulignait que « *le positionnement de la mission [avait] souffert de la non invitation, sauf exception, du chargé de mission aux réunions du comité des directeurs du ministère de la santé* »[565], la Cour des comptes quant à elle estimait que « *la mission [apparaissait] plus comme un organe facilitateur […] que comme une unité normative* »[566].
Par ailleurs, entre 2004 et 2006, la MISS a pâti d'une absence de direction, le chargé de mission ayant quitté son poste et n'ayant été remplacé que tardivement. Finalement, le décret n° 2011-496 du 5 mai 2011 portant création d'une délégation à la stratégie des systèmes d'information de santé auprès des ministres chargés de la santé, de la sécurité sociale, des solidarités et de la cohésion sociale[567] est venu supprimer la MISS, qui avait fini par devenir une coquille vide.

b) Le Conseil supérieur des systèmes d'information de santé

---

dispositions réglementaires des parties I, II et III du Code de la santé publique a finalement abrogé le décret créant le CSSIS, le faisant disparaitre par la même occasion.

[563] Cour des Comptes, « La sécurité sociale », rapport annuel, *op. cit*., p. 35.

[564] Cour des comptes, « L'interopérabilité des systèmes d'information en santé », *op. cit.*

[565] IGAS, « Evaluation du système d'information des professionnels de santé », rapport n° 2002-142, novembre 2002, p. 40.

[566] Cour des comptes, « L'interopérabilité des systèmes d'information en santé », *op. cit.*,p. 36.

[567] Décret n° 2011-496 du 5 mai 2011 portant création d'une délégation à la stratégie des systèmes d'information de santé auprès des ministres chargés de la santé, de la sécurité sociale, des solidarités et de la cohésion sociale, *JORF* n° 0105, texte n°31.

486. Créé en 1997[568], le Conseil supérieur des systèmes d'information de santé (CSSIS), placé auprès du Ministre de la santé, avait pour missions principales *« d'émettre des recommandations et des avis sur les problèmes liés à la production, à la transmission et aux modalités d'exploitation des informations relatives aux soins et à la santé des personnes »*[569], mais également, et il s'agissait selon nous de sa mission essentielle, de veiller *« à la cohérence, à la sécurité et au caractère évolutif des programmes d'intérêt général dont il est amené à connaître, notamment en ce qui concerne les outils d'aide à la pratique médicale et les réseaux destinés aux échanges d'information de santé »*[570]. En parallèle de ces fonctions, le CSSIS avait la possibilité de proposer au Ministre de la santé de faire procéder à des études ou investigations par l'IGAS. Cependant, il n'a pas utilisé l'ensemble des moyens qui étaient à sa disposition.

Après trois années d'exercice, pourtant assez riches, et trois rapports d'activité, le mandat des membres arrivait à terme et sa composition n'a pas été renouvelée. Ainsi, l'activité du CSSIS a été mise en sommeil, et cet organe disparaitra définitivement lors de la création de la DSSIS.

2) Les structures opérationnelles

A côté des structures dédiées à la coordination, existaient des structures plus opérationnelles.

a) Le groupement pour la modernisation du système d'information hospitalier

487. Le groupement pour la modernisation du système d'information hospitalier (GMSIH), dont la convention constitutive avait été approuvée par arrêté ministériel en date du 23 février 2000[571], avait pour mission de « *concourir, dans le cadre général de la construction du système d'information de santé, à la mise en cohérence, à l'interopérabilité, à l'ouverture et à la sécurité des systèmes d'information utilisés par les établissements de santé membres* ». Initialement constitué pour une durée de cinq ans, il a ensuite été prorogé de deux années

[568] Décret n° 97-20 du 14 janvier 1997 portant création d'un Conseil supérieur des systèmes d'information de santé, *JORF* n°12 du 15 janvier 1997, p. 712.
[569] *Id.*, Article 1er.
[570] *Ibid.*
[571] Arrêté du 23 février 2000 relatif à la nomination d'un commissaire du Gouvernement auprès du groupement d'intérêt public dénommé « Groupement pour la modernisation du système d'information hospitalier », *JORF* n°49 du 27 février 2000, p. 3082.

supplémentaires par un arrêté du 5 octobre 2004[572]. Comme le prévoyait l'article L. 6113-10 du Code de la santé publique applicable à l'époque[573], le GIP était composé des établissements publics de santé volontaires[574]. Par ailleurs, les représentants des membres du GIP à l'assemblée générale et au conseil d'administration étaient désignés par les organisations représentatives des établissements membres[575].En termes d'activité, la convention constitutive du groupement exposait clairement qu'il n'était « *n'est ni développeur ni maître d'ouvrage d'applicatifs* ». Comme le souligne la Cour des comptes dans son rapport, le GMSIH apparaissait donc plutôt comme un « *centre de ressources et d'expertise constitué en vue d'élaborer des orientations stratégiques* »[576]. Le GMSIH s'est également révélé avoir un rôle d'intermédiaire entre la Direction de l'Hospitalisation de l'Offre de Soins (DHOS)[577], à l'initiative des projets, et les établissements de santé, en charge de l'exécution de ces projets.

---

[572] Arrêté du 5 octobre 2004, *JORF* n° 256 du 3 novembre 2004, p. 18563.

[573] « *Un groupement pour la modernisation du système d'information hospitalier est chargé de concourir, dans le cadre général de la construction du système d'information de santé, à la mise en cohérence, à l'interopérabilité, à l'ouverture et à la sécurité des systèmes d'information utilisés par les établissements de santé qui en sont membres. Sous réserve des dispositions du présent article, il est soumis aux dispositions de l'article 21 de la loi n° 82-610 du 15 juillet 1982 d'orientation et de programmation pour la recherche et le développement technologique de la France. La convention constitutive du groupement est approuvée par un arrêté des ministres chargés de la santé et des affaires sociales. Ce groupement est constitué pour une durée qui ne peut excéder sept ans, sous la forme d'un groupement d'intérêt public entre des établissements publics de santé volontaires. Les établissements de santé privés peuvent y adhérer. Les organisations représentatives des établissements membres du groupement figurant sur une liste arrêtée par le ministre chargé de la santé désignent les représentants des membres à l'assemblée générale et au conseil d'administration. Les représentants désignés par l'organisation représentative des établissements publics de santé disposent de la majorité des voix au sein de chacune de ces instances […]* »

[574] Arrêté du 23 février 2000 portant approbation de la convention constitutive d'un groupement d'intérêt public, *JORF* n°49 du 27 février 2000, p. 3081.

[575] Arrêté du 17 décembre 1999 pris en application de l'article L. 710-8 du Code de la santé publique et relatif aux organisations chargées de désigner les représentants des établissements de santé membres du groupement pour la modernisation du système d'information hospitalier au sein des organes délibérants dudit groupement, *JORF* n°297 du 23 décembre 1999, p. 19108.

[576] Cour des Comptes, « La sécurité sociale », *op. cit*., p. 45.

[577] Direction de l'Hospitalisation et de l'Offre de Soins, devenue la Direction Générale de l'Offre de Soins depuis le décret n° 2010-271 portant organisation de la direction générale de l'offre de soins, *JORF* n°0063 du 16 mars 2010, texte n° 36.

b) La Mission Nationale d'Appui à l'Investissement Hospitalier

488. La Mission nationale d'appui à l'investissement hospitalier (MAINH) a été créée dans le cadre de la mise en œuvre du plan hôpital 2007 par arrêté du ministère de la santé[578]. Cette mission était chargée « *d'accompagner techniquement le programme de rénovation du patrimoine hospitalier prévu dans le plan « Hôpital 2007* ».[579]

Elle était placée sous la direction d'un directeur détaché auprès de l'ARH Ile-de-France, qui en assurait la gestion administrative et financière. L'arrêté n'apporte aucun détail supplémentaire quant à son fonctionnement et ses missions. Dans les faits, cette mission a piloté le plan hôpital ainsi que les budgets qui lui étaient dédiés. En 2005, un arrêté a étendu ses compétences aux systèmes d'information hospitaliers[580].

La MAINH a été très vite critiquée sur son organisation. Ainsi, la Cour des comptes, dès 2006, pointait du doigt son rattachement administratif à l'ARH d'Ile-de-France ainsi que son positionnement direct auprès du Ministre de la santé. Ce rapport soulignait également la problématique de l'éclatement des compétences et des responsabilités entre, d'une part, la DHOS et, d'autre part, la MAINH en matière d'organisation et de gestion des systèmes d'information hospitaliers. Cette absence de partage clair et précis des responsabilités, ajoutée à une absence de précisions quant aux liens existants entre DHOS et MAINH a compliqué le processus décisionnel et a fragilisé la cohérence globale de l'action de l'Etat sur ce sujet.

Dans son rapport de novembre 2007 sur l'interopérabilité, la Cour des Comptes soulignait la possible redondance de la MAINH avec le GMSIH.

Malgré la mise en place d'un protocole de coopération entre les deux structures, ainsi que la réunion trimestrielle d'un comité de pilotage, le pilotage des SIH par le biais de ces structures s'est révélé chronophage et consommateur de ressources tant humaines que financières.

---

[578] Arrêté du 27 mars 2003 portant désignation du directeur et organisation de la mission nationale d'appui à l'investissement hospitalier, *JORF* du 2 avril 2003, p. 5817.
[579] *Ibid.*
[580] Arrêté du 1er juillet 2005 modifiant l'arrêté du 27 mars 2003 portant désignation du directeur et organisation de la mission nationale d'appui à l'investissement hospitalier, *JORF* du 5 août 2005, texte n° 62.

La MAINH et le GMSIH ont finalement disparu pour laisser place en 2011 à la Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS), qui constitue désormais la seule structure de coordination des politiques relatives aux systèmes d'information de santé.

c) Les GIP DMP et CPS

489. Suite à la création du DMP par la loi du 13 août 2004[581], le Groupement de préfiguration du DMP (communément appelé GIP-DMP) a vu le jour. Ce groupement, composé de l'Etat, de la Caisse nationale d'assurance maladie des travailleurs salariés et de la Caisse des dépôts et consignations, et dont la convention constitutive a été approuvée par un arrêté du 11 avril 2005[582]avait pour mission principale de préparer les dispositions qui permettraient à l'organisme gestionnaire du DMP d'être opérationnel. Ses fonctions étaient donc temporaires, dans l'attente de la mise en place d'une structure pérenne. Il fut d'ailleurs initialement créé pour une durée très courte puisque sa convention constitutive prévoyait sa disparition au 31 décembre 2005.

Cependant, un arrêté du 28 décembre 2005[583] a prorogé la vie de ce GIP jusqu'au 30 juin 2007, étant par ailleurs précisé qu'il avait « *vocation à cesser d'exister dès que l'organisme gestionnaire du dossier médical personnel aura été mis en place et sera en mesure d'accomplir ses missions* ». En effet, face au retard considérable pris dans la mise en place du DMP, les pouvoirs publics n'ont pas eu d'autre choix que de maintenir ce GIP. La Cour des comptes, lors de son contrôle des comptes et de la gestion du GIP, avait eu l'occasion de mettre en exergue le décalage qui existait entre, d'une part, l'ampleur du projet et, d'autre part, le peu de moyens accordées à ce que la Cour qualifiait de « *petite structure* » (65 emplois et 23 millions d'euros de dépenses en 2007)[584]. A l'occasion de ce contrôle, plusieurs points négatifs avaient été relevés. Il était notamment reproché au GIP son autonomie trop limitée, l'Etat intervenant plus que de raison dans son fonctionnement, ainsi que sa gouvernance déficiente, résultant directement de cette intervention constante de l'Etat.

---

[581] Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie, *JORF* n°0190 du 17 août 2004, p. 14598.
[582] Arrêté du 11 avril 2005 portant approbation de la convention constitutive d'un groupement d'intérêt public, *JORF* n°85 du 12 avril 2005, p. 6547.
[583]Arrêté du 28 décembre 2005 portant approbation des modifications apportées à la convention constitutive du groupement de préfiguration du dossier médical personnel *JORF* n°304 du 31 décembre 2005, p. 20903.
[584] « La gestion du GIP Dossier médical personnel », rapport public annuel de la Cour des comptes, février 2009, pp. 135-151.

Par ailleurs, les faiblesses de la maîtrise d'ouvrage, pourtant au cœur de ses missions et le manque d'intérêt du GIP pour la qualité et la sécurité du système, avaient également été soulignées.

Ce rapport est toutefois intervenu, comme la Cour le souligne elle-même, à un moment où « *les pouvoirs publics prenaient enfin conscience de l'irréalisme du projet et décidaient d'attendre le résultat des missions d'enquêtes avant de le relancer* »[585]. Parmi ces missions d'enquête, on retrouve notamment le Rapport de la mission de relance du DMP, rendu en avril 2008 par Michel GAGNEUX[586] ou encore le Rapport sur le dossier médical personnel présenté par Pierre LABORDES au Sénat en avril 2009[587]. Ces deux rapports dressaient un bilan mitigé du DMP et préconisaient une relance du projet comprenant une refonte de sa gouvernance et de son organisation générale.

Ces rapports ne sont pas les seuls à s'être attardés sur le sujet et entre 2007 et 2009, plusieurs institutions se sont penchées sur la problématique de la gouvernance des systèmes d'information de santé. En est ressorti un bilan assez critique de l'organisation en place.

B. Un bilan mitigé

490. La Cour des comptes, en étudiant la question de l'interopérabilité des systèmes d'information (1) et l'IGAS (2) ont eu l'occasion d'observer la gouvernance des systèmes d'information de santé de manière assez précise.

1) Les rapports de la Cour des comptes

La Cour des comptes s'est penchée à plusieurs reprises sur la question de l'interopérabilité des systèmes d'information de santé, études menant irrémédiablement à s'interroger sur l'état de la gouvernance des projets d'e-santé en France.

---

[585] *Id.*, p. 135.

[586] GAGNEUX, Michel. « Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé », *La Documentation Française*, 2008.

[587] ETIENNE, Jean-Claude. LABORDES, Pierre. « Le dossier médical personnel (DMP) : quel bilan d'étape pour quelles perspectives ? », rapport fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, *Sénat*, n° 567, 2009.

491. A l'occasion d'un contrôle portant sur l'interopérabilité des systèmes d'information en santé d'abord, la Cour avait conclu que les conditions nécessaires à l'amélioration de l'interopérabilité n'étaient pas réunies et ce, en grande partie, à cause d'un défaut de pilotage central. Dans son référé à l'attention du Ministre de la santé et des solidarités, le Premier Président de la Cour des comptes relevait que « *face à des acteurs multiples, aux intérêts non convergents, l'Etat n'a pas su organiser un pilotage efficace* ». La Cour reconnaissait ici le contexte compliqué auquel l'Etat était confronté mais n'oubliait pas pour autant de rappeler que l'absence de lisibilité de la politique menée par le Ministère de la santé en la matière n'avait cessé d'être pointée du doigt depuis le début des années 2000. Au moment de son contrôle, la Cour déplorait ainsi l'inexistence d'un document de cadrage, opposable aux différentes directions du ministère mais également à l'ensemble des acteurs concernés par le système d'information en santé et reprenant les grandes orientations de ce que devrait être ce système d'information[588].

492. A l'occasion de son rapport annuel sur l'application des lois de financement ensuite, rendu en septembre 2007, la Cour des comptes avait consacré un chapitre au partage des données entre les systèmes d'information de santé. Cela avait été l'occasion pour la juridiction d'émettre une recommandation touchant plus particulièrement à la problématique de la gouvernance des systèmes d'information en santé. Elle avait alors préconisé de réduire le nombre d'opérateurs des systèmes d'information en santé et renforcer le pilotage stratégique par le Ministère. Pour la Cour, il apparaissait de manière évidente, et à juste titre selon nous, que l'amélioration de la gouvernance passerait obligatoirement par une simplification de l'organigramme des acteurs concernés mais surtout par une reprise en main par l'Etat du pilotage global du système d'information de santé afin d'en assurer la cohérence générale. Un pilotage stratégique fort par le Ministère, appuyé par des structures opérationnelles efficaces et réduites en nombre apparaissait comme la solution de l'amélioration de la gouvernance des systèmes d'information en santé. C'est par ailleurs, comme nous le verrons, la solution adoptée lors de la refonte de la gouvernance à partir de 2009.

[588] Cour des comptes, « L'interopérabilité des systèmes d'information en santé », *op. cit.*, p. 23.

2) Le rapport de l'IGAS

493. L'IGAS, dans le cadre de son activité 2006, a été amené à se pencher sur l'organisation et sur le pilotage des organismes en charge du développement des systèmes d'information de santé[589]. Sa feuille de route était alors très claire : elle devait « *procéder […] à l'audit de l'organisation du pilotage de ces dispositifs en vue de vérifier leur cohérence d'ensemble et d'évaluer la qualité du pilotage de chaque structure ainsi que l'efficacité et la cohérence du pilotage global du système par l'Etat*. »[590] Cet audit s'est donc intéressé pleinement à la gouvernance des systèmes d'information de santé, et il en a résulté des recommandations concrètes et efficaces, certaines ayant d'ailleurs été mises en œuvre depuis lors.

494. L'intérêt principal de cette étude de l'IGAS réside, selon nous, dans l'analyse fine qui y est faite du pilotage des différents organismes intervenant dans la gouvernance et la mise en place des systèmes d'information en santé. En effet, comme nous l'avons vu, plusieurs types de structures ont coexisté allant des "missions", émanations directes du Ministère, aux GIP, formule principalement privilégiée par l'Etat. Le choix du groupement, révélateur de la volonté de faire travailler ensemble deux acteurs essentiels du système de santé (le Ministère de la santé et l'assurance maladie) a permis à l'Etat de s'engager dans des projets et d'en garder le contrôle, pendant que la CNAMTS les finançait. Par exemple, comme le relève l'IGAS, « *la création du GIP-DMP permet-elle à l'Etat de financer sur des ressources de l'assurance maladie un projet répondant d'abord à des objectifs de santé publique* ». Nous ajouterons également que ce choix est plus que stratégique en termes d'affichage politique. En effet, un projet comme celui du DMP par exemple, qui serait entièrement financé et géré par l'Assurance maladie, serait alors considéré principalement comme un projet de régulation des dépenses et de contrôle des professionnels, alors que ce même projet, géré par un GIP dont l'Etat est membre, redevient un projet de santé publique, au service des usagers du système de santé avant tout.

---

[589] IGAS, « Audit de l'organisation et du pilotage des organismes œuvrant à l'informatisation du système de santé », *op. cit.*
[590] *Id*, p. 1.

495. Néanmoins, cette multiplication des projets et des GIP les gérant a multiplié les représentations de l'Etat, qui s'est, de fait, éparpillé. Il a par ailleurs été constaté un cloisonnement entre les différentes directions du Ministère en charge de la tutelle des différents GIP. Ainsi, aucune coordination n'était assurée entre la DHOS, la Direction de la Sécurité Sociale (DSS) ou encore la Direction Générale de la Santé (DGS), alors qu'une mise en commun de leurs personnel spécialisé, de leurs expertises mais également une définition d'objectifs communs aurait été souhaitable. Enfin, l'ensemble de ces structures, concentrées sur un projet technique précis, a développé des compétences et expertises techniques pointues, au prix d'une certaine redondance entre les structures elles-mêmes, alors qu'une mutualisation aurait été plus efficiente et économique.

Cette conception "verticale" de la réalisation des projets[591] a finalement affaibli l'efficacité de la gouvernance en place.

C. Les propositions GAGNEUX et FIESHI

496. Missionné par le Ministre de la santé de l'époque, Madame Roselyne BACHELOT-NARQUIN, Michel GAGNEUX, alors Président du Groupement d'Intérêt public DMP, a rendu un rapport en mai 2009 comportant « *12 propositions pour renforcer la cohérence et l'efficacité de l'action publique dans le domaine des systèmes d'information de santé* »[592]. Pour l'inspecteur général des affaires sociales, ce sont bien les diverses problématiques rencontrées lors des tentatives de développement du DMP qui ont mis en exergue la faiblesse de la gouvernance du système d'information en santé. Il ressortait de ce rapport qu'une gouvernance efficace et cohérente devait reposer sur une stratégie nationale globale en matière de systèmes d'information de santé. L'ensemble des objectifs, mais également des schémas directeurs des projets, de leur cohérence et de leurs budgets, devait émaner de l'échelon national. Michel GAGEUX proposait pour cela, de mettre en place un conseil national des systèmes d'information de santé, dont la compétence serait étendue à l'ensemble du champ de la santé et possédant une légitimité forte (en étant notamment institué par la loi

[591] GRATIEUX Laurent, OLLIVIER Roland. « Audit de l'organisation et du pilotage des organismes œuvrant à l'informatisation du système de santé », *IGAS*, p. 10.
[592] GAGNEUX, Michel. « Refonder la gouvernance de la politique d'informatisation du système de santé - Douze propositions pour renforcer la cohérence et l'efficacité de l'action publique dans le domaine des systèmes d'information de santé », *op. cit.*

et présidé par le Ministre de la santé). Par ailleurs, le rapport, soulignant l'inadéquation des moyens et prérogatives de la MISS avec ses objectifs, proposait la disparition de la mission et la création au sein du ministère, d'une Direction de la stratégie et de la prospective des systèmes d'information de santé. Pour Michel GAGNEUX, seule une direction placée au niveau exécutif et disposant de l'expertise et de la légitimité nécessaire serait capable de fédérer l'ensemble des acteurs impliqués afin de mettre en place une politique cohérente[593]. Le rapport insistait enfin sur la nécessité de développer et professionnaliser la maîtrise d'ouvrage, qui devait s'organiser à la fois à l'échelon national et plus spécifiquement au niveau des directions techniques du Ministère de la santé, mais également au niveau régional et plus particulièrement des ARS.

497. Le Professeur Marius FIESHI, quant à lui, a rendu en juin 2009 un rapport intitulé « La gouvernance de l'interopérabilité sémantique est au cœur du développement des systèmes d'information en santé »[594]. Ce rapport axait son étude sur l'opportunité de l'utilisation de systèmes terminologiques communs dans le cadre du développement de l'informatisation du système de santé, et ce afin d'améliorer notamment la prise en charge des patients. A l'occasion de son étude du sujet, sur laquelle nous aurons l'occasion de revenir au cours de nos travaux, le Professeur FIESHI a abordé la question de la gouvernance des systèmes d'information. Son constat était très simple : pour lui, le Ministère ne s'était pas suffisamment préoccupé de la question de la cette gouvernance. A l'appui de ce constat, il citait divers rapports pour conclure sur une critique sans appel : « *en l'absence de schéma directeur, un ensemble de projets ne conduit pas à un système* »[595]. En effet, l'organisation existante lors de la rédaction de ce rapport était basée sur des projets successifs, menés de manière indépendante et sans maîtrise d'ouvrage commune, donc sans gouvernance réelle.

498. Ces deux rapports, publiés à quelques mois d'intervalles, ont permis d'amorcer une refonte de la gouvernance, à l'initiative du Ministère de la santé. En effet les propositions du rapport de Michel GAGNEUX ont conduit la ministre de la santé à le missionner afin de conduire une mission de préfiguration, en lien avec le secrétaire général des ministères

---

[593] *Id.*, p. 6.
[594] FIESHI, Marius, « La gouvernance de l'interopérabilité sémantique est au cœur du développement des systèmes d'information en santé », *La Documentation Française*, juin 2009.
[595] *Id.*, p. 30.

chargés des affaires sociales, afin de créer et installer, notamment la délégation à la stratégie des systèmes d'information de santé.

Cette nouvelle gouvernance montre cependant elle aussi quelques limites.

§2. Un manque de visibilité sur la gouvernance des projets en cours

499. Face aux critiques émises, et dans un souci d'assurer une gestion cohérente des SIS, la refonte à partir de 2009 de l'organisation liée à leur gouvernance a permis d'aboutir à un nouvel organigramme (A). Néanmoins, celui-ci montre encore aujourd'hui quelques limites, rendant difficile la visibilité sur les projets en cours (B).

A. Le nouvel organigramme de la gouvernance des SIS

500. Comme auparavant, la structure est restée schématiquement la même, à savoir des structures d'appui opérationnelles (2), en charge de la maîtrise d'ouvrage de certains projets et une structure de coordination (1), dotée cette fois-ci d'une légitimité et de moyens d'action plus forts que ses prédécesseurs.

1) Une structure de coordination : la délégation à la stratégie des systèmes d'information de santé

501. Pour plus de lisibilité mais également d'efficacité, la MISS et le CSSIS ont disparu pour laisser place à la Délégation à la Stratégie des Systèmes d'Information de Santé (DSSIS) placée sous l'autorité du secrétariat général des ministères chargés des affaires sociales. Préfigurée par Michel GAGNEUX, cette délégation a toutefois mis du temps à voir le jour. Presque un an et demi se sont en effet écoulés entre la lettre de mission et le décret du 5 mai 2011 instaurant la délégation[596]. L'article 2 de ce décret lui accorde sept missions importantes et conséquentes que sont l'animation et l'élaboration des priorités nationales en matière de SI santé et médico-social, la participation aux organes de pilotage national, la préparation des

[596] Décret n° 2011-493 du 5 mai 2011 relatif à la prise en compte des incidences énergétiques et environnementales des véhicules à moteur dans les procédures de commande publique, *JORF* n°0105 du 6 mai 2011, p. 7751.

décisions du Conseil national de pilotage des ARS, la coordination des actions des différents acteurs en la matière (Etat, assurance maladie, agences, établissements de santé, CNSA.), la tutelle de l'ASIP santé, l'orientation et la coordination de l'action à l'échelle européenne et internationale, et, enfin, assurer la maîtrise d'ouvrage des systèmes d'information centraux et déconcertés des ministères.

502. Cependant, le décret n° 2013-727 du 12 août 2013 portant création, organisation et attributions d'un secrétariat général des Ministères chargés des affaires sociales[597] vient repréciser, dans son article 10, les missions de la DSSIS. Ainsi, la mission de maîtrise d'ouvrage des systèmes d'information des services centraux disparait. Celle-ci est reprise par une nouvelle direction, la direction des systèmes d'information du secrétariat général. Cette modification souligne une volonté de séparer la gestion des systèmes d'information de santé de la gestion du système d'information du Ministère, les enjeux, les expertises et les acteurs n'étant pas les mêmes.

503. Présentée par le Ministère des Affaires sociales et de la santé[598] comme une structure légère s'appuyant sur l'ASIP santé, la DSSIS a un rôle majeur de coordination générale des acteurs intervenant dans l'organisation et la mise en place des systèmes d'information de santé. C'est également à elle qu'il revient de donner l'impulsion générale en termes de développement des projets, notamment en leur donnant le cadre nécessaire à leur bon développement. Ainsi, lors de sa mise en place, la DSSIS avait à cœur[599], avant toute chose, d'instaurer des bases solides en matière de prérequis nécessaires au développement d'une politique forte et efficace en des systèmes d'information en santé, à savoir un cadre juridique fiable, une gestion coordonnée des référentiels et assurer la sécurité des systèmes d'information en santé.

Malheureusement, comme nous le constaterons dans la suite de nos travaux, à l'heure actuelle ces trois points majeurs ne sont pas résolus.

---

[597] Décret n° 2013-727 du 12 août 2013 portant création, organisation et attributions d'un secrétariat général des ministères chargés des affaires sociales, *JORF* n°0188 du 14 août 2013, texte n° 4.
[598] Présentation générale de la DSSIS, disponible sur [http://social-sante.gouv.fr]. Consulté le 15 avril 2016.
[599] « Système d'information de Santé : la DSSIS trace les axes prioritaires », Interview de Philippe BURNEL, DSIH e-santé, 2012, disponible sur [http://www.dsih.fr]. Consulté le 15 avril 2016.

2) Des structures opérationnelles en appui

a) L'ASIP Santé

504. L'Agence des Systèmes d'Information Partagés en santé est un groupement d'intérêt public, dont la convention constitutive a été approuvée par un arrêté en date du 8 septembre 2009[600], et placée sous la tutelle de l'Etat. Ce groupement, composé dans un premier temps de l'Etat (représenté par le Ministère de la santé), la CNAMTS et la caisse des dépôts et consignation, est aujourd'hui composé de l'Etat, la CNAMTS et la Caisse nationale de solidarité pour l'autonomie.

Le GIP, né de la réunion du GIP-DMP, du GIP-CPS assure, selon sa convention constitutive sept missions qui sont les suivantes : la maîtrise d'ouvrage des projets de systèmes d'information en santé qui lui sont délégués par ses membres ; la réalisation et le déploiement du Dossier Médical Personnel (DMP) et la maîtrise d'ouvrage de son hébergement ; la définition, la promotion et l'homologation de référentiels, standards, produits ou services contribuant à l'interopérabilité, la sécurité et l'usage des systèmes d'information de santé et de la télésanté, ainsi que la surveillance de leur bonne application ; la maîtrise d'ouvrage et la gestion, dans le cadre des missions qui lui sont déléguées, des annuaires et référentiels nationaux regroupant les identités et informations associées relatives aux professionnels de santé, ainsi qu'aux services et établissements de santé et du secteur médico-social ; la certification, la production, la gestion et le déploiement de la Carte de Professionnel de Santé (CPS) et, plus généralement, de dispositifs assurant les fonctions d'identification, d'authentification, de signature permettant aux professionnels de santé de faire reconnaître, dans les conditions de sécurité et de confidentialité requises, leur identité et leurs qualifications professionnelles par les systèmes d'information et d'échanges électroniques qu'ils utilisent ; l'accompagnement et l'encadrement des initiatives publiques et privées concourant à son objet (notamment sous forme de conventions d'assistance à maîtrise d'ouvrage ou de conventions de partenariat) ; la participation à la préparation et à l'application des accords ou projets internationaux dans le domaine des systèmes de partage et d'échange de l'information de santé, à la demande du ministre ou des ministres compétents.

[600] Arrêté du 8 septembre 2009 portant approbation de la convention constitutive d'un groupement d'intérêt public, *JORF* n°0213 du 15 septembre 2009, p. 15096.

Ce groupement a vu le jour suite aux différents rapports qui pointaient les défaillances de la gouvernance en place en matière des systèmes d'information de santé. L'ASIP Santé résulte de la volonté de l'Etat de renforcer la maîtrise d'ouvrage publique des systèmes d'information, mais également d'instaurer un mode d'action efficace dans le domaine. Comme l'indiquait le communiqué de presse du 16 septembre 2009 à ce sujet, « *l'ASIP est né de la volonté […] d'installer une agence d'Etat référente et fédératrice de l'e-santé en France* »[601].

505. Pour l'ensemble des industriels regroupés au sein du LESISS (Les Entreprises des Systèmes d'Information Sanitaires et Sociaux – LESISS), l'ASIP est « *un pilote clairement identifié qui œuvre dans un esprit de concertation.* »[602]. L'ASIP peut en effet s'enorgueillir de plusieurs réussites en matière de systèmes d'information de santé (publication de référentiels d'interopérabilité, définition d'un identifiant national de santé (INS), création du répertoire des professionnels de santé (RPPS), création de l'offre de service DMP), là où ses prédécesseurs n'avaient malheureusement pas réussi à mener à bien leur mission.

506. Cependant, bien que très active dans ses premières années de vie, l'ASIP s'est vite retrouvée bloquée dans plusieurs projets et notamment en ce qui concerne le DMP. Comme le soulignait Michel GAGNEUX, dans le rapport d'activité de l'ASIP de 2012, « *force est de reconnaître que l'action de l'agence ne peut plus être, depuis la fin de l'année 2011, à la hauteur de ces finalités. Projet emblématique, le Dossier Médical Personnel (DMP) a été mis en service avec succès en phase de test dans quatre régions dès le début de 2011, mais son déploiement n'a pu être engagé. Notre pays a plus que jamais besoin d'une politique nationale cohérente et constante, fondée sur une vision de long terme de notre système de santé à la fois mobilisatrice et fédératrice, et sur une stratégie d'action claire et pertinente* »[603].

---

[601] Communiqué disponible sur [http://www.portailtelesante.org] consulté le 15 avril 2016.
[602] Rapport d'activité de l'ASIP santé, 2009, p. 29, disponible sur [http://esante.gouv.fr] consulté le 19 mars 2017.
[603] Rapport d'activité 2012 de l'ASIP santé, p. 1, disponible sur [http://esante.gouv.fr], consulté le 15 avril 2016.

507. Avec le transfert de la gestion et de la mise en place du DMP à la CNAMTS, par la loi de modernisation de notre système de santé[604], l'ASIP a perdu l'une de ses missions principales, à laquelle elle travaillait, depuis sa création. Sa convention constitutive sera certainement modifiée en ce sens. Elle se recentre donc sur de nouveaux projets, dont la mise en œuvre de la messagerie sécurisée de santé, la modernisation des systèmes d'information des SAMU ou encore le déploiement des répertoires opérationnels des ressources[605].

b) L'agence Nationale d'Appui à la Performance

508. L'agence Nationale d'Appui à la Performance (ANAP), née en 2009 de la réunion du GMSIH, de la MAINH et de la Mission nationale d'expertise et d'audit hospitaliers, a repris l'ensemble des missions qui leur été confiées. Elle s'est, par ailleurs, vu confier d'autres missions par la loi HPST et notamment celle d'appuyer les établissements de santé, les établissements médico-sociaux et les ARS en vue d'améliorer leur performance. Institué par la loi HPST, ce GIP[606] a été créé le 23 octobre 2009, date de publication de l'arrêté d'approbation de sa convention constitutive.

509. Cette agence a un rôle global d'accompagnement des établissements sanitaires et médico-sociaux dans leurs démarches d'amélioration de leur performance. Parmi son large portefeuille d'activités se trouve ainsi les systèmes d'information. Contrairement à d'autres agences, l'ANAP ne participe aucunement à l'édiction de normes techniques ou règlementaires dans le domaine. De même, elle n'est pas habilitée à délivrer des autorisations ou des avis. Son rôle est strictement limité à l'accompagnement et au conseil des établissements, en leur fournissant un appui ponctuel mais également en établissant des méthodologies et des référentiels partageables à tous les établissements. L'ANAP remplit également des missions d'audit et d'évaluation des projets hospitaliers, notamment dans le domaine informatique. A titre d'exemple, en 2015, l'ANAP, en lien avec la DGOS, a travaillé

---

[604] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte 1, article 96.

[605] La mise en place du répertoire Opérationnel des Ressources – ou ROR- est prévue par l'article D. 6124-25 du Code de la santé publique. Le ROR est un outil de description des ressources de l'offre de soins pour une région dont l'objectif est de proposer une information exhaustive de l'offre de soins régionale et extra-régionale. En mai 2012, l'ASIP santé a été missionnée par la DGOS pour définir et mettre en œuvre un programme permettant de doter l'ensemble des régions d'un service ROR cohérent à l'échelle nationale, en s'inspirant notamment des ROR fonctionnel. Puis, en 2015, la mission de l'ASIP a évolué. Désormais, elle a en charge de rendre interopérable les ROR en place afin de permettre l'accès à l'offre de soin d'une région à une autre, et déployer un ROR interopérable dans les régions qui n'en seraient pas encore pourvues.

[606] Ce GIP est composé de l'Etat, l'Union des caisses d'assurance maladie, la caisse nationale de solidarité pour l'autonomie et les fédérations représentatives des établissements de santé et médicaux sociaux.

au déploiement du programme hôpital numérique et notamment à la réduction des freins structurels au bon déploiement des systèmes d'information de santé[607].

B. Les limites de cette nouvelle organisation

510. Bien que grandement rénovée, la nouvelle gouvernance des systèmes d'information de santé présente encore quelques lacunes et mérite que l'on s'interroge à son sujet. Ainsi, il nous parait important de nous intéresser au choix effectué par l'Etat de créer une agence afin de lui déléguer ses missions (1), avant d'exposer le manque de visibilité sur certains projets qui perdure aujourd'hui (2).

1) Le schéma de gouvernance choisi par l'Etat

511. L'Etat a fait le choix de confier la maîtrise d'ouvrage des projets à une agence spécialisée, formée sous forme de GIP, tandis qu'une délégation dédiée aux SIS, placée sous l'autorité du secrétariat aux affaires sociales se charge de veiller à la bonne coordination de l'ensemble. A première vue, cet organigramme simplifié semble plus efficient. Cependant, ce choix mérite que l'on s'y attarde, pour tenter de mieux le comprendre.

a) L'ASIP, une nouvelle venue dans le paysage des agences de l'Etat.

512. L'Etat a fait le choix de créer une agence afin de lui confier le soin d'assurer la maîtrise d'ouvrage des SIS. Comme l'a souligné le Conseil d'Etat dans son étude annuelle consacrée à la notion d'Agence[608], ce phénomène de recours régulier aux agences par l'Etat a posé quelques difficultés juridiques. En effet, cette notion d'agence peut parfois être difficile à cerner. Il n'en existe pas de définition juridique précise.

513. L'étude du Conseil d'Etat, pour sa part, s'oriente vers une définition *a contrario* en préférant d'abord préciser ce que ne sont pas les agences (ni des autorités administratives indépendantes, ni de simples opérateurs) avant de tenter de définir ce qu'elles sont : des acteurs opérationnels, qui assurent des missions que l'Etat ne peut assurer lui-même, une

[607] Rapport d'activité 2015 de l'ANAP, p. 7, disponible sur [http://www.anap.fr], consulté le 17 avril 2016.
[608] Conseil d'Etat, « Les agences : une nouvelle gestion publique ? », étude annuelle, Septembre 2012, 18 questions / 18 réponses.

« *réponse managériale à l'incapacité supposée de l'Etat de faire face à ses missions* »[609]. Les agences ont par ailleurs la particularité de ne pas présenter un statut unique et l'on peut trouver des GIP, des GIE, des établissements publics ou encore, bien que cela soit plus rare, des associations. L'étude du Conseil d'Etat, partant de ce constat, a tenté de proposer les statuts les plus adéquats en fonction des types de missions exercées par les agences, le statut d'établissement public étant préconisé en priorité et celui de GIP dans les cas où l'agence serait amenée à « *expérimenter des formes nouvelles de gestion* ».

514. Dans le cas de l'ASIP, c'est ce qui a motivé l'Etat à choisir la formule du GIP. En effet, l'Etat souhaitant associer la CNAMTS à la gestion et surtout au financement des projets menées par l'ASIP, n'a pas pu s'orienter vers l'établissement public, qui aurait sous-entendu un financement intégral par l'Etat, ce qu'il n'était pas en mesure de faire. La forme d'Agence quant à elle présente l'avantage de séparer la définition des politiques publiques et, dans notre cas, des grandes orientations nationales en matière de systèmes d'information en santé, de leur mise en œuvre, par un organisme qui pourra être jugé sur ses résultats et en être tenu responsable. Quand l'on s'attarde sur les quatre critères dégagés par le Conseil d'Etat pour justifier la création d'une agence[610](l'efficience, l'expertise, le partenariat et la neutralité), il nous apparait clairement que l'ASIP y répond pleinement. Le choix de créer une « agence » dédiée à cette mission apparait donc opportun tout comme celui d'un GIP.

b) L'ASIP, un GIP sous tutelle

515. Il nous faut également nous interroger sur le contrôle exercé par l'Etat sur cette Agence. En effet, en tant que GIP dont l'Etat est membre, l'ASIP pourrait se voir placée sous le contrôle d'un commissaire du gouvernement. Cependant, à l'heure actuelle, l'Etat n'a pas fait ce choix. C'était d'ailleurs déjà le cas à l'époque des GIP-DMP et GIP-CPS et l'IGAS avait souligné ce choix de l'Etat de ne pas user de son pouvoir. De manière pratique, un commissaire du gouvernement est chargé de contrôler les activités ainsi que la gestion du GIP. Il a également un rôle d'intermédiaire entre les instances du GIP et les autorités chargées de l'approbation de la convention constitutive du GIP. De même, il a pour mission de veiller au respect des dispositions applicables au groupement et participe à toutes ses instances, au

[609] Jacky RICHARD « Réfléchir aux agences, c'est réfléchir à l'Etat », AJDA, 2012, p 1660
[610] Conseil d'Etat, « Les agences : une nouvelle gestion publique ? », *op. cit.*, p. 12.

sein desquelles il dispose d'une voix consultative. L'Etat a cependant prévu de placer l'ASIP sous la tutelle de la DSSIS.

516. Notion issue du droit civil, la tutelle a pu être définie, en droit administratif, comme « *l'ensemble des pouvoirs limités accordés par la loi à une autorité supérieure sur les agents décentralisés et sur leurs actes dans un but de protection de l'intérêt général* »[611]. Il s'agissait, en pratique, d'une vérification de la légalité du fonctionnement des établissements publics, qu'ils soient locaux ou nationaux, une fois les décisions prises en totale liberté et non pas d'une participation à la gestion de l'établissement. L'autorité de tutelle disposait bien de pouvoirs d'annulation ou d'approbation sur les actes émanant des établissements, bien qu'elle ne puisse pas pour autant modifier les actes soumis à approbation[612].

Depuis la loi du 2 mars 1982[613], le législateur a mis fin aux tutelles exercées par l'Etat sur les décisions prises par les collectivités territoriales et a transformé le contrôle *a priori* (contrôle hiérarchique) qui existait en un contrôle a posteriori des décisions prises. Cette tutelle est donc devenue principalement un contrôle *a posteriori* de la légalité des actes des établissements publics. Ainsi, l'autorité de l'État, après réception des actes les rendant exécutoires de plein droit, à déférer au tribunal administratif les actes de l'autorité territoriale qu'elle estime devoir être annulés. La tutelle est finalement une contrepartie à l'autonomie qui est accordée aux établissements publics. En pratique, l'autorité de tutelle va, selon les cas, disposer de moyens plus ou moins étendus de contrôle sur l'établissement. Sachant que selon le célèbre adage, il n'y a pas de tutelle sans texte et pas de tutelle au-delà des textes, les pouvoirs de l'autorité de tutelle et leur étendue vont donc dépendre de ce qu'aura prévu le législateur en la matière. Aussi, la tutelle d'un établissement public ne se présume pas et l'autorité investie de ce pouvoir ne pourra pas dépasser les limites strictement prévues par les textes. Nous pouvons donc en déduire que le texte instaurant une tutelle devra préciser les mesures que l'autorité de tutelle pourra prendre ainsi que ses domaines d'intervention.

---

[611] MASPETIOL et LAROQUE, La tutelle administrative, 1930, *Sirey*, p. 10.
[612] CE, 24 juin 1970, *min. Anciens combattants et victimes de guerre c/ Lepeltier*, Rec., 1970, p. 430.
[613] Loi n° 82-213 du 2 mars 1982 relative aux droits et libertés des communes, des départements et des régions, *JORF* du 3 mars 1982, p. 730.

517. Ceci étant rappelé, il nous est nécessaire de nous interroger sur cette tutelle de l'ASIP par la DSSIS. Dans un premier temps, il nous faut réfléchir à la possibilité pour un GIP d'être placé sous la tutelle de l'Etat.

En effet, comme l'a rappelé le Tribunal des Conflits, les GIP sont des personnes publiques, soumises à un régime particulier, prévu par la loi et ne sont donc pas soumis de plein droit aux lois et règlements régissant les établissements publics[614]. Nous pouvons en déduire que la tutelle d'un GIP n'est pas, comme pour un établissement public, chose automatique. Cependant, nous pouvons aisément comprendre ici, au vu de la particularité du GIP en question, auquel l'Etat a confié une mission qui lui incombait, l'intérêt d'être soumis à sa tutelle.

Dans un second temps, il nous apparait légitime de nous interroger sur le caractère suffisant des dispositions prévoyant la tutelle de l'ASIP. En effet, celles-ci sont assez simples puisque le décret n° 2013-727 du 12 août 2013 portant création, organisation et attributions d'un secrétariat général des ministères chargés des affaires sociales[615] prévoit simplement que « *la délégation à la stratégie des systèmes d'information de santé a pour missions […] d'assurer la tutelle sur le groupement d'intérêt public dénommé "Agence des systèmes d'information partagés de santé"* », ni plus, ni moins. Aucune précision n'est apportée quant aux limites de cette tutelle et rien ne vient nous éclairer sur le pouvoir de contrôle que possède la DSSIS sur l'ASIP. A titre d'exemple, il nous est impossible de savoir si tous les actes pris par l'ASIP devront être communiqués à la DSSIS ou simplement les décisions les plus importantes émanant de son assemblée délibérante.

La portée de cette tutelle et donc du contrôle exercé par l'Etat sur l'ASIP à l'heure actuelle nous semble donc trop peu précis. Par ailleurs, face à cette tutelle, certes prévue par un texte, mais trop peu détaillée, nous pouvons nous questionner sur son efficacité. Ainsi, il nous apparait qu'un commissaire du gouvernement aurait eu un rôle, si ce n'est plus efficace, en tous cas plus précis.

---

[614] TC, 14 février 2000, *GIP Habitat et interventions sociales pour les mal-logés et les sans-abri*s, Rec., p. 748.
[615] Décret n° 2013-727 du 12 août 2013 portant création, organisation et attributions d'un secrétariat général des ministères chargés des affaires sociales, *JORF* n°0188 du 14 août 2013, texte n° 4.

2) Un manque de visibilité des projets en cours

518. Malgré une gouvernance rénovée et une certaine apparence d'unicité, grâce notamment à l'ASIP santé, force est de constater qu'il reste difficile de faire la cartographie précise des projets relatifs aux SIS en cours et surtout de leur gestion. Jean-Yves ROBIN, ancien directeur de l'ASIP Santé souligne dans son ouvrage consacré à l'état des lieux du numérique en santé en France[616], l'absence de vision globale de la gestion des projets, qui amène naturellement à un manque de visibilité des projets en cours. Ainsi, il tente de dresser un état des lieux des projets afin de démontrer l'éparpillement des moyens et des initiatives en la matière. Dans les faits, il est effectivement difficile de dresser un état des lieux exhaustif des projets d'e-santé, tous domaines confondus, actuellement en cours. L'exercice se complique quand il est question de rechercher les pilotes des projets.

519. Si l'on reprend l'analyse de Jean-Yves ROBIN, on constate que de nombreux projets sont en cours, pilotés par autant d'organismes différents qu'il y a de projets[617]. Ainsi, à titre d'exemple, l'informatique des professionnels de santé ambulatoire est pilotée par la CNAMTS tandis que les systèmes d'information hospitaliers sont gérés au niveau de la DGOS. L'appel à projets Territoires de Soins Numériques est quant à lui également piloté par la DGOS mais nécessite le concours des ARS et un suivi de la Caisse des Dépôts et des Consignations. Le DMP était jusqu'à très récemment piloté par l'ASIP santé, mais a été réattribué à la CNAMTS[618]. Par ailleurs, le Comité stratégique de filière, piloté par le Ministère de l'économie, consacre certains de ses travaux à l'e-santé, tout comme le Conseil National du Numérique. Enfin, sans entrer dans le détail, précisons toutefois que la Direction Générale de la Santé, placée auprès du Ministère de la santé, pilote de manière directe une trentaine de projets, dont l'aboutissement peut être parfois très long faute de ressources suffisantes.

Ce rapide état des lieux dressé par Jean-Yves ROBIN permet de constater facilement à quel point les ressources et les efforts en matière d'e-santé sont éparpillés. Car bien sûr,

---

[616] ROBIN, Jean-Yves. « L'urgence numérique. Faire de la France un leader de l'e-santé », *L'Harmattan*, 2015, p. 57.
[617] *Ibid.*
[618] Article 96 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte 1.

aucune coordination n'est assurée entre les différents projets, ce qui, d'une part, ne permet pas de mutualiser les moyens et les expertises entre les projets et, d'autre part, crée un cloisonnement entre les différentes initiatives, ce qui, sur le long terme, amène à des projets évoluant en parallèle, là où il aurait été nécessaire de les construire et les développer en concordance. Dès lors, les outils proposés aux professionnels de santé, en ambulatoire ou en secteur hospitalier, ne présentent ni logique, ni l'efficacité escomptée.

Conclusion de la section

520. Il apparait compliqué pour l'Etat d'organiser une gouvernance stable et cohérente des SIS. Ce constat s'explique en partie par l'historique du sujet. En effet, tant que le Ministère de la santé n'avait pas réalisé l'ampleur de la problématique et la nécessité d'assurer une politique unifiée en la matière, les projets se sont développés de manière indépendante et à différents échelons, avec plus ou moins de succès. Ainsi, la gouvernance initiale des SIS, qui regroupait, d'une part, des structures d'appui et de coordination, en charge d'impulser des projets majeurs et, d'autre part, des structures plus opérationnelles s'est très vite révélée complexe et incohérente. En a résulté de nombreuses critiques, notamment de la part de la Cour des comptes et de l'IGAS, ces deux instances s'accordant sur l'absence de lisibilité de la gouvernance et sur l'éparpillement notable de l'Etat en la matière. Dès 2009, le Ministre de la santé s'est donc inscrit dans une démarche d'évolution de cette gouvernance, inspirée par les recommandations concrètes émise pas des spécialistes de la question.

521. Dans le cadre de la refonte de cette gouvernance, le choix de confier à une agence, l'ASIP santé, la maîtrise d'ouvrage des projets relatifs aux SIS, sous la tutelle d'une délégation placée auprès du Ministère de la santé, n'est pas sans poser quelques petites interrogations. Cependant, cette nouvelle gouvernance se révèle, dans l'ensemble, plus efficace et pertinente que la précédente même si, aujourd'hui encore, il est compliqué d'avoir une vue d'ensemble des projets en cours et dresser une cartographie de l'ensemble des acteurs intervenants dans les projets SIS reste un défi difficile à relever.

Section 2. Les défis à relever pour une gouvernance efficace

522. L'Etat doit aujourd'hui relever deux défis majeurs s'il souhaite améliorer la gouvernance actuelle des SIS. Ces défis sont de nature différente mais d'une importance égale. Le premier, technique, concerne l'interopérabilité des systèmes d'information (paragraphe 1). Le deuxième, à la fois politique et organisationnel, concerne la définition de la place des acteurs régionaux dans la gouvernance des SIS (paragraphe 2).

§1. L'interopérabilité des SI, un chantier prioritaire

523. L'interopérabilité des systèmes d'information, concept que nous tâcherons de définir précisément au cours de notre réflexion, apparait comme le chantier principal à mener à bien aujourd'hui afin d'assurer une gouvernance stable des SIS. Sans interopérabilité, point de salut pour les SIS, car celle-ci apparait comme étant la clef de voûte d'un système cohérent, communiquant, unifié et donc, efficace. Cette problématique, très ancienne en matière de SIS (A), semble parfois difficile à résoudre, malgré certains projets majeurs développés à ce sujet (B)

A. Enjeux d'une problématique ancienne

524. Cette notion d'interopérabilité, notion très technique, ne dispose pas de définition légale correctement établie (1). Pour tenter d'atteindre cette interopérabilité, nécessaire à la bonne communication des SIS entre eux, plusieurs conditions techniques doivent être préalablement mises en place (2), et suppose bien évidemment que les SIS soient développés à partir de normes standardisées (3).

1) Périmètre de l'interopérabilité

525. Il peut apparaître difficile d'appréhender cette notion d'interopérabilité. De manière technique, elle peut être définie comme la capacité de matériels, de logiciels ou de protocoles de fonctionner ensemble et à partager des informations[619].

526. La Cour des Comptes, dans son rapport relatif à l'interopérabilité des systèmes d'informations s'était, bien entendu, essayé à cet exercice de définition, préalable nécessaire à son étude. Il en était ressorti la définition suivante : « *dans le domaine des systèmes d'information, l'interopérabilité peut être entendue comme une propriété des systèmes permettant à deux ou plusieurs agents (automates ou utilisateurs final) d'échanger de l'information et d'en comprendre le sens, indépendamment des bases technologiques utilisées et sans faire appel à une intervention humaine au cours de la chaine de communication, que cette communication soit synchronisée (comme le téléphone) ou désynchronisée (comme la messagerie)* »[620]

Juridiquement, ce concept n'est pas réellement circonscrit. Il apparait pourtant bien dans plusieurs textes législatifs[621]. Au long de notre développement, nous nous appuierons donc sur cette définition donnée par la Cour des comptes, qui permet, selon nous, d'appréhender les enjeux techniques de cette notion assez facilement.

2) Préalables nécessaire à l'interopérabilité

L'interopérabilité des systèmes d'information nécessite que certaines conditions essentielles soient réunies afin d'être correctement mise en place.

a) Une identification unifiée des patients.

527. En toute logique, pour que des informations puissent être échangées au sujet d'un patient, il faut que celui-ci puisse être identifié correctement. Cela suppose donc une identification fiable et unifiée au sein des différents systèmes d'information, fiabilité qui ne

---

[619] Définition du Larousse.
[620] Cour des comptes, « L'interopérabilité des systèmes d'information en santé », *op. cit.*, p. 5.
[621] *V.* notamment en ce sens l'article 43 de la loi n° 99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle, *JORF* n°0172 du 28 juillet 1999, p. 11229.

peut être assurée par les simples noms, prénoms et date de naissance pour des raisons évidentes d'identitovigilances. C'est dans cette optique que le législateur, en 2007, avait prévu qu'un « *identifiant de santé des personnes prises en charge par un professionnel de santé ou un établissement de santé […] est utilisé, dans l'intérêt des personnes concernées et à des fins de coordination et de qualité des soins pour la conservation, l'hébergement et la transmission des informations de santé* ».[622] Alors que le Ministère de la santé s'orientait vers une utilisation du NIR à cette fin, la CNIL, dans un rapport 20 février 2007[623], préconisait pour sa part, la création à partir du NIR d'un identifiant spécifique non signifiant. Dans le cadre de ses missions, l'ASIP Santé s'est ainsi vue confier la délicate mission de mettre en œuvre cet identifiant. Dans un premier temps, l'agence a développé une solution permettant la mise en œuvre d'un identifiant national de santé dit "calculé" (INS-C). Celui-ci pouvait ainsi être intégré par les éditeurs de logiciels de professionnels de santé dans leurs solutions techniques. Cependant, cet INS-C n'a pas eu le succès escompté et bien que cet identifiant devait être temporaire, afin de faciliter la mise en place d'un INS définitif (appelé INS-aléatoire), l'étape ultime n'a jamais été franchie.

528. La loi de modernisation de notre système de santé résoud cette difficulté puisqu'elle modifie l'article L. 1111-8-1 au Code de la santé publique qui prévoit désormais que *« le numéro d'inscription au répertoire national d'identification des personnes physiques est utilisé comme identifiant de santé des personnes pour leur prise en charge à des fins sanitaires et médico-sociales, dans les conditions prévues à l'article L. 1110-4. »*. Cette disposition est définitivement entrée en vigueur, comme nous l'avons vu précédemment, depuis la publication du décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé [624].

Par ailleurs, pour éviter toute discordance avec les dispositions de la loi Informatique et Libertés, la Loi Touraine a pris le soin de préciser que « *les dispositions de la loi n° 78-17*

---

[622] Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le Code de la santé publique (dispositions réglementaires), JORF n°113 du 16 mai 2007, p. 9362.

[623] Rapport du groupe de travail relatif à l'évaluation de la doctrine de la CNIL en matière d'utilisation du NIR, 20 février 2007. Disponible sur [https://www.cnil.fr]. Consulté le 17 avril 2016.

[624] Décret n° 2017-412 du 27 mars 2017 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques comme identifiant national de santé, *JORF* n°0075 du 29 mars 2017, texte n° 23.

du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prescrivant une procédure particulière d'autorisation à raison de l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques dans un traitement de données à caractère personnel ne sont pas applicables aux traitements qui utilisent ce numéro exclusivement dans les conditions prévues au présent I. »

529. Finalement, faute d'identifiant de santé satisfaisant, le législateur a retenu la solution du NIR, plus sécurisé et déjà en place. Comme le souligne l'ASIP santé[625], « *le déploiement actuel des SI de santé autour du patient et de la notion de parcours impose en effet de faire le choix d'un identifiant simple, pérenne, fiable et, dans un contexte budgétaire très contraint, de privilégier l'efficacité à des solutions coûteuses. Le numéro de sécurité sociale, ou « NIR », présente ces caractéristiques.* ».

b) L'identification des professionnels

530. A l'instar des patients, l'identification des professionnels de santé au sein du SIS permet la justification de leur identité, assure la traçabilité de leurs accès et permet, *a fortiori*, le contrôle du respect du secret professionnel.

531. C'est le système de carte de professionnel de santé (CPS) qui, aujourd'hui, a pour mission d'assurer cette identification. Cependant, comme nous avons pu le voir précédemment dans nos développements, cette carte rencontre un succès mitigé[626], notamment au sein des établissements de santé, et sa mise en place demeure assez longue. Sur le terrain, nombreux sont les établissements de santé qui ont mis en place des cartes alternatives, certaines comportant un système de signature électronique reconnue de type RGS 2 étoiles[627].

---

[625] « Projet de loi de santé : les apports en matière de dématérialisation des données de santé », article consultable sur [http://esante.gouv.fr], consulté le 22 mars 2016.

[626] Au sein des établissements hospitaliers, à ce jour, 237 075 cartes de la famille des CPx sont actives dont 100 064 cartes CPS.

[627] Au CHRU de Lille par exemple, une carte d'établissement, distribué à tous les professionnels est déployée depuis 2011. Depuis 2015, certaines d'entre elles comportent un système de signature électronique de type RGS 2 étoiles.

3) La normalisation des systèmes : la condition technique essentielle

532. Il est impossible d'aborder la notion d'interopérabilité sans parler de la normalisation des échanges informatisés. En effet, pour être interopérables, deux systèmes devront être basés sur les mêmes normes, afin de s'assurer que les données échangées soient compréhensibles et exploitables. En matière de SIS, cette normalisation est double car elle concerne à la fois l'aspect informatique mais également l'aspect médical, dans le sens où les données reportées au sein des dossiers informatiques ne devront permettre aucune interprétation contraire. Les termes et éventuels codes utilisés devront être donc normalisés[628].

533. Cette notion de normalisation est encadrée par le décret n° 2009-697 du 16 juin 2009 relatif à la normalisation[629]. Sa définition est prévue à l'article 1 du décret : « *la normalisation est une activité d'intérêt général qui a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques, relatives à des produits, à des services, à des méthodes, à des processus ou à des organisations. Elle vise à encourager le développement économique et l'innovation tout en prenant en compte des objectifs de développement durable.* »

534. En France, c'est l'Association Française de Normalisation (AFNOR)[630] qui a pour mission de mettre en œuvre la normalisation et de la promouvoir. Dans ce but, elle dispose d'un pouvoir d'élaboration et d'homologation des normes, quels qu'en soit les domaines. Une norme est par principe d'application volontaire, même si certains textes réglementaires peuvent les rendre obligatoires[631]. Cependant, comme le relevait la Cour des Comptes dans son rapport, « *nombre de conventions techniques permettant d'assurer l'interopérabilité se*

---

[628] Nous pensons ici particulièrement au PMSI et à la codification des actes médicaux.

[629] Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation, JORF n°0138 du 17 juin 2009, p.9860. Ce texte est pris en application des directives 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information et 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur, ensemble la notification n° 2008/0042/F du 1er février 2008 adressée à la Commission des Communautés européennes

[630] L'AFNOR est l'organisme français en charge de la normalisation, mais il existe également des organismes internationaux, tel que l'ISO (International Standards Organisation – Organisation internationale de normalisation), L'ANSI (American National Standards Institute), le CEN (Comité Européen de Normalisation).

[631] Article 17 du décret n° 2009-697 du 16 juin 2009 relatif à la normalisation, *JORF* n°0138 du 17 juin 2009, p. 9860.

sont imposées de fait, étant donné l'importance industrielle de leurs promoteurs »[632]. Ainsi, le poids et l'influence des industriels en matière de normalisation n'est pas négligeable.

B. L'interopérabilité, une problématique insoluble ?

535. Nombreux ont été et, perdurent encore aujourd'hui, les freins à la mise en place de l'interopérabilité des systèmes d'information en santé. La Cour des comptes les avait déjà relevés en son temps, tout comme l'IGAS et aujourd'hui, le constat reste malheureusement le même Pourtant, des solutions ont été envisagées et des chantiers sont en cours (1). Mais certaines limites restent aujourd'hui très présentes (2)

1) Le cadre d'interopérabilité des SIS

536. Afin de s'assurer que les conditions d'interopérabilité des systèmes sont réunies, il est essentiel de mettre en place des référentiels d'interopérabilité. C'est ce qu'a prévu l'ordonnance du 8 décembre 2005[633] en soulignant qu'un « *référentiel général d'interopérabilité fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information* »[634]des administrations de l'Etat, des collectivités territoriales, des établissements publics à caractère administratif et des organismes de sécurité sociale[635]. Le référentiel général d'interopérabilité a été approuvé par l'arrêté du 9 novembre 2009 portant approbation du référentiel général d'interopérabilité.

537. Dans le domaine plus spécifique des systèmes d'information en santé, c'est à l'ASIP Santé que revient d'assurer la mise en place de l'interopérabilité. En effet, rappelons que cette agence a notamment pour mission de définir, promouvoir et homologuer des référentiels contribuant à l'interopérabilité, à la sécurité et à l'usage des systèmes d'information de santé et de la télésanté ainsi que de favoriser le développement des systèmes d'information partagés dans le domaine de la santé et du secteur médico-social, afin de développer la coordination et la qualité des soins (dont la télémédecine), la prévention, la veille et l'alerte sanitaire.

---

[632] Cour des comptes, « L'interopérabilité des systèmes d'information en santé », *op. cit.*, p. 7.
[633] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, *JORF* du 9 décembre 2005, p. 18986.
[634] *Id.*, article 11.
[635] *Id.*, article 1er.

538. C'est dans ce contexte que l'ASIP Santé a élaboré le cadre d'interopérabilité des systèmes d'information de santé (CI-SIS). L'objectif principal du CI-SIS est de définir les règles permettant l'interopérabilité des SIS en santé. Cette interopérabilité se situe à deux niveaux différents : d'une part, l'interopérabilité technique qui va permettre le partage des données de santé en favorisant les flux et les échanges et, d'autre part, l'interopérabilité des contenus métiers, afin de permettre le traitement des données et leur compréhension. D'une manière générale, le CI-SIS est basé sur des normes internationales en matière de SIS, ponctuellement adaptées aux spécificités françaises quand cela est nécessaire.

539. Récemment, l'ASIP santé a revu et corrigé entièrement la gouvernance de ce cadre d'interopérabilité. La nouvelle gouvernance du CI-SIS a été présentée en novembre 2015 aux utilisateurs, aux industriels et aux partenaires institutionnels. Cette rénovation résulte d'une volonté de l'ASIP d'adapter le CI-SIS aux évolutions des usages en matière de SIS mais également de s'adapter aux évolutions des normes internationales sur lesquelles le CI-SIS s'appuie en majeure partie. Pour cela, les acteurs de SIS santé ont été fortement sollicités et leurs besoins en matière d'interopérabilité ont été recueillis. Enfin, la loi de modernisation de notre système de santé est venue ajouter[636] un article L. 1110-4-1 au Code de la santé publique, qui renforce le poids des référentiels d'interopérabilité puisqu'il précise la chose suivante : « *afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés.* »

540. Cependant à l'heure actuelle, bien que ces référentiels soient prêts et disponibles sur le site de l'ASIP Santé, ils n'ont toujours pas été, comme la loi l'exige, approuvé par arrêté du

[636] Article 96 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte 1.

ministre de la santé. Ainsi, nous comprenons très vite l'ambiguïté de la situation : les établissements de santé sont supposément contraints d'adopter des solutions respectant des règles d'interopérabilité validées par le ministère de la santé s'ils souhaitent conserver ou échanger par voie informatique des données de santé, mais le ministère tarde à fournir cet arrêté. La situation est donc actuellement en suspens.

Il ne s'agit pas du seul frein au bon développement de l'interopérabilité des SIS et des obstacles, majoritairement techniques, subsistent encore aujourd'hui.

2) Les obstacles au développement de l'interopérabilité.

541. Comme le rapport d'information du député Jean-Yves JEGOU le signalait déjà en 2007[637], plusieurs types d'obstacles existent à un réel aboutissement de l'interopérabilité des SIS. Les constats effectués il y a presque dix ans sont aujourd'hui encore valables, même s'il est vrai que les obstacles techniques ont été considérablement réduits.

542. Le premier obstacle technique majeur est bien entendu l'existence ou plutôt, à l'heure actuelle, l'inexistence d'un identifiant patient unique et unifié. Jusque très récemment, les tentatives de mise en place de cet identifiant ont échoué. La loi de modernisation de notre système de santé tente de résoudre ce problème en prévoyant l'utilisation généralisée du NIR comme identifiant patient unique. Il faut maintenant que les acteurs concernés s'adaptent pour mettre en place cet identifiant. Pour les établissements de santé, cette utilisation devrait être de toute manière accélérée par la mise en place des Groupements Hospitaliers de Territoire, qui devront organiser une mutualisation de la gestion des systèmes d'information et un système d'information convergent d'ici 2020. Le même problème se pose en termes d'authentification des professionnels de santé, par le biais du système de carte CPS notamment, dont nous avons déjà exposé les limites actuelles à plusieurs reprises.

543. L'autre obstacle technique majeur réside dans la multiplicité des opérateurs logiciels sur le marché. En effet, les industriels développent des solutions et des applications différentes afin de faire marcher le jeu de la concurrence. De ce fait, ces applications ne sont pas communicantes entre elles. Ainsi, en 2007, la Cour des comptes parlait même

[637] JÉGOU, Jean-Jacques. « Systèmes d'information de santé : le diagnostic est posé, le traitement s'impose », *op. cit.*

« *d'atomisation du parc de logiciels* », la seule exception étant les domaines de l'imagerie médicale et des laboratoires, dont les systèmes d'informations doivent être couplés avec des équipements techniques, dont le nombre de constructeurs est assez faible.

544. Enfin, un problème organisationnel vient également ralentir le développement pérenne de l'interopérabilité : celui de l'urbanisation des systèmes d'information. Ce terme, emprunté au domaine des travaux d'architecture des villes, a été repris par les professionnels de l'informatique pour désigner une démarche visant à structurer le système d'information d'une société afin de le rationaliser et d'améliorer ses performances et faciliter ses évolutions.

545. En matière de systèmes d'information de santé, pour reprendre les propos d'Yves ROBIN, « *dans une organisation du niveau de complexité de notre système de santé, c'est l'urbanisation ou le chaos* »[638]. Or, pour l'auteur, c'est bien à l'Etat qu'il appartient de poser les bases de cette urbanisation, afin d'harmoniser l'organisation des systèmes d'information de santé. Ainsi, pour l'ancien directeur de l'ASIP santé, plusieurs leviers permettraient de faire évoluer la situation actuelle en matière d'interopérabilité et d'urbanisation. Il serait question dans un premier temps de la mise en place par l'Etat d'un schéma global d'urbanisation, qui serait en soutien d'une politique globale de développement de l'e-santé. Ce schéma serait l'occasion d'organiser la répartition des missions et compétences respectives de l'ensemble des acteurs intervenants en la matière, que ce soit au niveau national ou régional. Il serait également nécessaire d'élaborer un référentiel « *univoque d'identités des personnes physiques et morales composants l'offre de soins* » afin de pouvoir établir ensuite une politique d'authentification des professionnels efficace et compatible avec les pratiques actuelles. Enfin, une de ses dernières préconisations majeures a été suivie puisqu'il conseillait d'adopter le NIR comme identifiant patient unique.

L'interopérabilité des SIS n'est pas le seul défi majeur à relever. En effet, afin d'être efficace, la gouvernance des SIS doit accorder une place importante aux acteurs régionaux.

---

[638] ROBIN, Jean-Yves. « L'urgence numérique. Faire de la France un leader de l'e-santé », *L'Harmattan*, 2015, p. 57.

§2. La place stratégique des acteurs régionaux dans la gouvernance des SIS

546. Au niveau national, l'Etat seul ne peut pas, d'une part, édicter la politique générale applicable en matière de SIS et, d'autre part, la mettre en place de manière uniforme sur l'ensemble du territoire. Il doit donc s'appuyer sur d'autres acteurs pour mettre en place et éventuellement adapter ces politiques. Au niveau régional, ce sont les Agences Régionales de Santé (ARS) qui ont ce rôle majeur (A) et qui servent notamment de lien avec les établissements de santé et professionnels concernés. Récemment, cette organisation régionale s'est étoffée avec l'apparition d'un nouvel acteur au rôle stratégique : le Groupement Hospitalier de Territoire (B).

A. L'ARS, acteur charnière dans la mise en œuvre des politiques relatives aux SIS.

547. Depuis plusieurs années, la France s'est engagée dans de nombreux chantiers de dessaisissement des services de l'Etat au profit d'autres organismes. En matière sociale, le Conseil National de modernisation des politiques publiques a entrepris, depuis 2007, une réorganisation des services centraux et déconcentrés de l'Etat en la matière[639]. Dans le domaine sanitaire, c'est la loi HPST qui a amorcé un changement important, par la création des Agences Régionales de Santé, services décentralisés de l'Etat en matière de santé publique[640].

---

[639] CRISTOL, Danièle, « La réorganisation des services de l'Etat en matière sociale », *RDSS*, 2011, p. 27.

[640] Article L1431-1 du Code de la santé publique : « *Dans chaque région et dans la collectivité territoriale de Corse, une agence régionale de santé a pour mission de définir et de mettre en œuvre un ensemble coordonné de programmes et d'actions concourant à la réalisation, à l'échelon régional et infrarégional :*
- des objectifs de la politique nationale de santé définie à l'article L. 1411-1 du présent Code ;
- des principes de l'action sociale et médico-sociale énoncés aux articles L. 116-1 et L. 116-2 du Code de l'action sociale et des familles ;
- des principes fondamentaux affirmés au I de l'article L. 111-2-1 du Code de la sécurité sociale.
Les agences régionales de santé contribuent au respect de l'objectif national de dépenses d'assurance maladie.
Leurs compétences s'exercent sans préjudice et dans le respect de celles des collectivités territoriales et des établissements et agences mentionnés aux articles L. 1222-1, L. 1313-1, L. 1413-2, L. 1418-1 et L. 5311-1 du présent Code ainsi qu'aux articles L. 312-8 du Code de l'action sociale et des familles et L. 161-37 du Code de la sécurité sociale. ».

548. Les ARS jouent ainsi un rôle majeur dans de nombreux projets relatifs aux systèmes d'information en santé, la DGOS s'appuyant sur elles pour la mise en œuvre de projets ou amorcer des phases de test au niveau régional. Cet acteur présente l'intérêt d'avoir les pouvoirs et l'organisation suffisante (1) pour aider l'Etat dans la mise en œuvre concrète de ses politiques. C'est pour cela qu'elles ont, pour les projets principaux, la délicate mission de les décliner ou parfois de les tester au niveau régional. C'est notamment le cas du programme hôpital numérique, projet phare de la DGOS en matière de SIS (2).

1) L'ARS, « bras armé » de l'Etat en matière de politiques de santé.

549. Les Agences Régionales de Santé, créées par la loi HPST, sont des établissements publics de l'Etat soumis à son contrôle. Contrairement aux Agences Régionales de l'Hospitalisation (ARH), qui étaient des GIP dont l'Etat était membre, les ARS sont donc une émanation directe de l'Etat. Leur création s'inscrit dans le cadre plus large de la révision générale des politiques publiques ainsi que de sa déclinaison territoriale[641]. Ainsi, comme l'a relevé la Cour des comptes, lors de son examen de la mise en place des ARS, « *la création des ARS confirme le niveau régional comme échelon pertinent de déclinaison et de gestion des politique de santé publique* »[642]. En effet, rappelons que jusqu'alors c'est l'échelon départemental qui était largement privilégié.

S'inscrivant dans une logique d'associations des compétences, les ARS regroupent à la fois des administrations déconcentrées de l'Etat (les anciennes Directions Départementales de l'Action Sanitaire et Sociale – DDASS - et Direction Régionales de l'Action Sanitaire et Sociale – DRASS -), des organismes d'assurance maladie (URCAM, CRAM et DRSM) ainsi que des structures mixtes qui associaient déjà Etat et assurance maladie (ARH). Ces agences se voient confiées de nombreuses délégations de pouvoir et bénéficient d'une autonomie et de pouvoirs renforcés par rapport notamment aux ARH. Enfin, au niveau national, les ARS sont pilotées par un Conseil National de Pilotage (CNP) des ARS, composé de représentants de l'Etat, de représentant de la Caisse Nationale de Solidarité pour l'Autonomie et de

[641] Cour des comptes, « La mise en place des Agences Régionales de Santé », rapport annuel relatif à la sécurité sociale, chapitre VIII, septembre 2012, p. 233.
[642] *Id.*, p. 234.

représentants des organismes d'assurance maladie[643]. Le CNP a pour rôle de délivrer, en amont, l'ensemble des directives nécessaires pour que les ARS puissent mettre en œuvre au niveau régional la politique de santé développée au niveau national. Par ailleurs, le CNP a pour rôle d'évaluer les actions des ARS ainsi que de leurs directeurs Généraux.

550. Le choix de faire des ARS des établissements publics de l'Etat n'est pas anodin et va dans le sens d'une réorganisation générale de la gouvernance du système de santé, qui induit un renforcement de l'emprise de l'Etat[644]. Les ARS sont les représentantes de l'Etat dans les régions, véritables "bras armés" de l'Etat, en charge de la mise en œuvre de la politique de santé sur les différents territoires. Ainsi, les ARS, de par leur organisation et leurs pouvoirs, apparaissent comme l'acteur majeur de la mise en œuvre de la politique développée par l'Etat en matière de SIS. Pour reprendre les termes employés par l'ASIP santé, « *acteur unique chargé de l'efficience des soins dans les territoires, les ARS sont en première ligne pour le déploiement des systèmes d'information partagés de santé* »[645]. Elles sont le relais indispensable à l'Etat au niveau des territoires de santé. Elles présentent également l'intérêt d'avoir une capacité à adapter la politique nationale aux particularités de leurs territoires. En effet, selon les régions et, au sein même des régions, selon les territoires de santé, les enjeux en matière de SIS ne seront pas les mêmes. Elles peuvent donc, selon les besoins des territoires, et les acteurs en place, instaurer les coopérations nécessaires, ou encore accompagner le développement et la modernisation des SIH de certains établissements. Pour autant, leur lien tutélaire avec l'Etat empêche des développements anarchiques de systèmes d'information de santé totalement régionalisés et donc cloisonnés.

551. Tout comme elle l'est pour les politiques de santé publique plus traditionnelles, l'ARS apparait parfaitement légitime non seulement pour appuyer et soutenir, en région, la politique nationale de développement de SIS mais également pour la déployer de manière concrète sur les territoires de soins. Elle apparait comme le lien entre l'Etat, concepteur de ces politiques, et établissements de santé, acteurs directs en charge de leur application. L'ARS, représentant de l'Etat et surtout de sa politique de santé dans les régions, va être le pivot sur lequel l'Etat

[643] Article L. 1433-1 du Code de la santé publique.
[644] VIOUJAS, Vincent. « De la loi HPST à la loi n° 2016-41 du 26 janvier 2016 : convergences et inflexions dans l'effort de modernisation de notre système de santé », *JCP-A*, n° 13, avril 2016, p. 2092.
[645] « L'ARS, acteur unique du système de santé en région », ASIP santé, disponible sur [http://esante.gouv.fr], consulté le 19 avril 2016.

va pouvoir se reposer afin de tester et de mettre en place sa politique en matière de systèmes d'information de santé. Cependant, les ARS bénéficiant d'une certaine autonomie, chacune d'entre elles peut développer une stratégie adaptée à sa région

2) L'ARS, acteur essentiel de la stratégie hôpital numérique

552. Piloté et mis en place par la DGOS, le programme hôpital numérique, destiné au développement et à la modernisation des systèmes d'information hospitaliers sur la période 2012-2017, a été lancé le 25 novembre 2011. Ce programme a pour buts principaux de coordonner l'ensemble des acteurs (établissements de santé, ARS, administration centrale, industriels) autour d'une feuille de route commune pour les SIH, soutenir les projets innovants et amener le système d'information de l'ensemble des établissements de santé au palier de maturité Hôpital numérique.

553. Les Agences Régionales de Santé ont pour mission la mise en œuvre, à l'échelon régional et infrarégional, des politiques nationales en matière de santé. A ce titre, elles déclinent, au sein de leur territoire, le programme Hôpital numérique. Les objectifs du programme doivent être pris en compte dans les politiques régionales de santé définies par les ARS, dans le cadre de documents stratégiques (programme régional SI, schéma directeur SI, programme de télésanté, …) mais également dans les contrats pluriannuels d'objectifs et de moyens (CPOM) qu'elles signent avec les établissements de santé de leur territoire. A titre d'exemple, les engagements réciproques de l'ARS et d'un établissement de santé sur les sujets relatifs aux systèmes d'information hospitaliers sont formalisés au sein du volet "système d'information", du CPOM, volet par ailleurs obligatoire.

554. Comme le précise le guide pratique à destination des agences régionales de santé pour la déclinaison du programme hôpital numérique[646], la DGOS attend de l'ARS qu'elle prenne « *une part active dans la mise en œuvre du programme Hôpital numérique, et être un réel promoteur du projet, sur toute sa durée* ». Ainsi, la mise en œuvre opérationnelle du programme repose sur trois axes, au sein desquels l'ARS aura un rôle à jouer.

[646] Publié par l'instruction DGOS/MSIOS n° 201-375 du 31 octobre 2012, BO santé, protection sociale solidarité, n° 2012-12 du 15 janvier 2013, p. 149.

555. Le premier axe est consacré à la gouvernance du projet. Les ARS participent à cette gouvernance par le biais de plusieurs outils. D'abord, elles intègrent le programme au sein de la politique régionale de santé, soit sous la forme d'une déclinaison du plan d'action national à l'échelle des territoires de santé, soit grâce à la contractualisation avec les établissements par le biais des CPOM. En ce qui concerne plus spécifiquement les CPOM, il est important de noter que le Code de la santé publique prévoit expressément que « *le contrat fixe […] les engagements du titulaire en termes de développement des systèmes d'information de transmission des données informatiques et le cas échéant, des activités de télémédecine* ». L'ARS a également la possibilité de mettre en place des structures de coopération visant à faciliter la mutualisation des moyens. A ce sujet, nous verrons que l'ARS dispose depuis peu d'un outil qui va, si sa mise en œuvre fonctionne, faciliter ces mutualisations : les Groupements Hospitaliers de Territoire (GHT).

556. Sur l'axe 2, consacré aux compétences SI, les ARS ont un rôle essentiellement pédagogique puisqu'elles devront assurer la coordination des formations initiales et continue. D'une manière concrète, l'ARS pourra s'assurer que la dimension SI est bien intégrée dans les programmes de formations, en s'appuyant notamment sur les délégations régionales de l'ANFH.

557. En ce qui concerne l'axe 3, consacré à l'offre de solution, les ARS n'interviennent pas. En revanche, leur rôle est stratégique sur l'axe 4 consacré au financement. En effet, c'est aux ARS qu'il appartient de sélectionner les dossiers qui seront retenus pour se voir octroyer un soutien financier au titre du programme. A noter que ce soutien n'est pas négligeable puisque, à titre d'exemple, en 2015, 154 millions d'euros ont été alloués à 600 établissements différents répartis au sein de 23 régions[647]. Les ARS sont donc au cœur de l'organisation du financement du projet. Cette mission très spécifique a d'ailleurs fait l'objet d'une instruction du ministère de la santé[648].

[647] Projet hôpital numérique, rapport d'activité 2015, p. 18.
[648] Instruction n°DGOS/PF/MSIOS/2013/225 du 04 juin 2013 relative au lancement opérationnel du volet financement du programme hôpital numérique, non publiée au *JORF*.

3) Les maîtrises d'ouvrage régionales, appuis stratégiques aux ARS

558. Autres acteurs régionaux incontournables et essentiels en matière de mise en œuvre de la politique des systèmes d'information de santé : les maîtrises d'ouvrages régionales ou MOAR.

La spécificité et la haute technicité des projets relatifs aux Systèmes d'information en santé ont nécessité de renforcer la maîtrise d'ouvrage régionale en charge de ces projets. Alors que de nombreux rapports, et notamment le rapport GAGNEUX, préconisaient de créer, dans chaque région, des structures de maîtrise d'ouvrage partenariales, chaque région devant se doter « *sous la responsabilité de l'agence régionale de santé, d'une structure de maîtrise d'ouvrage montée en partenariat avec l'ensemble des acteurs* », l'ASIP Santé a décidé de faciliter la création et le développement de ces MOAR dès 2010, en lançant le programme EMERGENCE. L'objectif de ce programme était d'accompagner les acteurs régionaux dans la mise en place d'une maîtrise d'ouvrage régionale, qui viendrait en appui de l'ARS pour les accompagner dans ses missions en matière de SIS. Ce programme s'inscrivait dans la continuité du programme de relance du DMP.

559. Alors que certaines régions, comme la région Midi-pyrénées, n'avaient pas attendu pour créer leur MOAR, d'autres ont de leur côté fortement bénéficié du programme EMERGENCE et de l'impulsion de l'ASIP Santé pour la mettre en place. Ainsi, un rapport relatif à l'état des lieux des maîtrises d'ouvrages régionales, réalisé par le cabinet KPMG sur commande de l'ASIP en novembre 2012[649], précisant qu'à cette date, 21 régions (sur 26 à l'époque) bénéficiaient d'une MOAR opérationnelle. Toutes ces structures de MOAR sans exception ont fait le choix du GCS de moyens, pour la grande majorité d'entre elles, GCS privé, même si trois MOAR conservaient, en 2012, le statut de GCS de moyens de droit public. Ce choix s'explique à la fois pour les avantages juridiques du GCS (structure dotée de la personnalité juridique, ayant une autonomie et un budget propre) mais également par le fait que cette formule se révèle parfaitement adaptée pour des coopérations entre plusieurs acteurs

[649] Cabinet KPMG, « Etat des lieux des maîtrises d'ouvrage régionales », rapport final, novembre 2012.

très différents (établissements publics, établissements privés, structures associatives, professionnels de santé).

560. Cependant, le choix du GCS présente un point négatif non négligeable : le fait que ce type de groupement soit, par définition, au service exclusif de ses adhérents. Or, il apparait difficile de faire des MOAR une structure d'appui aux ARS pour ses missions de santé publique, si cette même MOAR ne peut pas s'adresser à l'ensemble des acteurs concernés par l'ARS. Par ailleurs, comme le soulignait à juste titre le rapport de KPMG sur les MOAR, le statut de GCS peut perdre en agilité et en réactivité au fur et à mesure de l'augmentation de ses membres. Dès lors, le risque est que la MOAR devienne plutôt une structure de représentation qu'une structure opérationnelle. Cependant, les MOAR restent des acteurs régionaux indispensables au développement des SIS et de la mise en œuvre des politiques nationales en la matière.

B. Les GHT, nouveaux acteurs stratégiques pour le SIS.

561. Présentés, comme une « *[...] stratégie de prise en charge partagée autour d'un projet médical commun par les établissements publics de santé d'un même territoire [...]* » permettant la gestion mutualisée de *« certaines fonctions transversales (...)* »[650], les Groupements Hospitaliers de territoires, nouveaux venus dans le monde des coopérations hospitalières, sont des groupements présentant de nombreuses atypies (1). Parmi leurs nombreuses missions, les GHT doivent notamment veiller à la convergence des SI de leurs membres. Cette nouvelle "structure" devient donc un acteur incontournable de la gouvernance des SIS (2).

1) Les GHT une forme atypique de coopération

562. La loi de modernisation de notre système de santé, complétée par le décret n° 2016-524 du 27 avril 2016 relatif aux groupements hospitaliers de territoire[651], modifie profondément l'organisation des coopérations hospitalières, opérant un « *réel changement de*

[650] Ministre des Affaires sociales, de la Santé et des Droits des femmes, lettre de la mission d'accompagnement sur les groupements hospitaliers de territoire, 17 novembre 2014.
[651] Décret n° 2016-524 du 27 avril 2016 relatif aux groupements hospitaliers de territoire, *JORF* n°0101 du 29 avril 2016, texte n° 24.

paradigme »[652] en instaurant les Groupements Hospitaliers de Territoires (GHT). En effet, l'article 107 de la loi, codifié aux articles L. 6132-1 et suivants du Code de la santé publique prévoit que *« 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 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* ». Le GHT est présenté comme un outil de coopération qui vise « *à rationaliser les modes de gestion soit par une mise en commun de fonctions soit par des transferts d'activité entre établissements. Les modes de gestion s'entendent ainsi de plusieurs manières, la gestion de l'offre de soins d'une part (...) et la gestion des outils supports d'autre part, permettant une amélioration des modalités de travail* »[653]

Il est intéressant de se pencher sur cette nouvelle forme de "coopération" crée par la loi Touraine, originale en plusieurs points.

a) Spécificité des GHT

563. Le GHT présente la particularité de n'avoir de groupement que le nom. En effet, contrairement aux GCS ou aux GIE, les GHT ne donnent pas lieu à la naissance d'une nouvelle personne morale et reposent sur un dispositif conventionnel. En cela, les GHT sont les descendants directs des Communautés hospitalières de territoires, formule de coopération introduite par la loi HPST et qui disparait d'ailleurs avec la création des GHT[654]. En pratique, les GHT sont composés d'établissements publics, dont l'adhésion est encadrée par une convention constitutive, signée entre les différents établissements membres et validée par l'ARS. Notons qu'un établissement public de santé ne peut être partie qu'à un seul GHT et les

[652] VARNIER, Frédéric. « La coopération hospitalière au service de la modernisation de notre système de santé », *RDSS*, 2016, n° 4, p. 620.
[653] VÉRAN, Olivier. LACLAIS, Bernadette. TOURAINE, Jean-Louis et *ali*. Rapport fait au nom de la commission des affaires sociales sur le projet de loi relatif à la santé, n° 2673, mars 2015, p. 46.
[654] *V*. notamment en ce sens, l'article L. 6211-21 du Code de la santé publique.

coopérations de ce type ne peuvent donc pas être démultipliées. L'autre particularité de ces groupements est leur caractère obligatoire. En effet, les établissements de santé n'ont pas eu d'autre choix que d'adhérer à un GHT et ce, avant la date butoir du 1er juillet 2016 fixée par la loi. Ce caractère obligatoire constitue une rupture[655] avec ce qui existait précédemment en matière de coopération hospitalière. Par ailleurs, il est utile de préciser que le législateur, s'il a encadré et prévu l'ensemble des dispositions relatives à la constitution des GHT, il n'en a prévu aucune quant à leur dissolution ou encore au retrait des établissements. D'autres établissements peuvent cependant participer à un GHT par le biais d'une association ou d'un partenariat. En effet, la loi Touraine a ouvert la possibilité aux établissements déjà membres d'un GHT ou qui, au contraire, ne pourraient pas faire partie d'un GHT de par leur statut (hôpitaux des armées, établissements d'hospitalisation à domicile, établissements publics de santé autorisés en psychiatrie) d'être tout de même associé au projet médical. De même, tous les GHT doivent être associés à un CHU au titre des activités hospitalo-universitaires, cette association étant traduite à la fois dans le projet médical du groupement et dans une convention d'association, passée entre l'établissement support du GHT et le CHU concerné. Enfin, les établissements privés peuvent quant à eux être partenaires d'un GHT et ce, en signant une convention de coopération, encadrée par les dispositions de l'article L. 6134-1 du Code de la santé publique[656].

Ainsi, le GHT est fondé sur un dispositif strictement conventionnel. En effet, le GHT repose sur, *a minima*, deux conventions, la convention constitutive d'une part et la convention d'association avec un CHU d'autre part, même si celle-ci ne sera signée que par l'établissement support.

564. La convention constitutive présente un réel caractère stratégique, en ce qu'elle doit préciser des points majeurs du fonctionnement du GHT. Elle doit ainsi fixer le projet médical partagé, les délégations éventuelles d'activités, les transferts éventuels de soins ou

---

[655] VARNIER, Frédéric. « La coopération hospitalière au service de la modernisation de notre système de santé », *op. cit.*, p. 620.

[656] « *Dans le cadre des missions qui leur sont imparties et dans les conditions définies par voie réglementaire, les établissements de santé publics ou privés à but non lucratif peuvent participer à des actions de coopération, y compris internationales, avec des personnes de droit public et privé. Pour la poursuite de ces actions, ils peuvent signer des conventions, participer à des groupements d'intérêt public, des groupements d'intérêt économique ou des groupements de coopération sanitaire ou constituer entre eux des fédérations médicales interhospitalières. Pour les actions de coopération internationale, les établissements de santé publics ou privés à but non lucratif peuvent également signer des conventions avec des personnes de droit public et privé, dans le respect des engagements internationaux souscrits par l'Etat français* ».

d'équipement matériels lourds entre les établissements, l'organisation des activités et la répartition des emplois médicaux et pharmaceutiques, les modalités de constitution des équipes médicales communes et des éventuels pôles inter-établissements, et enfin les modalités pratiques d'organisation et de fonctionnement du GHT. Elle est également la base légale de la délégation de compétences entre les établissements et l'établissement support. Car en effet, l'autre particularité majeure des GHT est cet adossement à un établissement support, désigné au sein de la convention et qui aura en charge d'exercer certaines fonctions pour le compte des autres établissements et notamment la gestion commune d'un SIH convergent, la gestion du DIM, la fonction achat, la coordination des instituts et des écoles de formation. Cette convention est d'autant plus importante que le GHT ne dispose ni de la personnalité morale, ni d'un dispositif extrêmement encadré comme c'est par exemple le cas pour les GCS. La convention se doit donc d'être la plus précise possible, puisqu'elle a la lourde tâche, pour reprendre les propos de Catherine KELLER, de compenser « *l'absence d'incarnation juridique de la coopération qu'elle met en œuvre* »[657].

565. Plus qu'une simple mise en commun des moyens, telle que l'on peut la rencontrer dans les coopérations du type GIP ou GCS, les GHT induisent une délégation d'activité[658]. Ce que le texte prévoit relève en effet de la délégation de compétence puisque les établissements doivent déléguer *a minima* quatre compétences stratégiques - SIH, DIM, achats et formation - à l'établissement support qui agira alors pour leur compte. C'est avec une grande attention et une grande précaution que ces délégations d'activité devront être appréhendées par les différents établissements. En effet, l'établissement support devra mesurer l'impact de cette délégation sur sa responsabilité. Par ailleurs, la convention constitutive est la base juridique de cette délégation de compétence, ce qui ne fait que renforcer son importance.

b) Des questions en suspens.

566. La mise en place des GHT soulève plusieurs questions d'ordre juridique. D'abord, la pertinence du qualificatif de coopération attribué aux GHT. En effet, il est nécessaire de se demander si le terme de coopération est adapté pour désigner les GHT, à partir du moment où

[657] KELLER, Catherine. « De la communauté hospitalière de territoire au groupement hospitalier de territoire : continuité et rupture », *JCP –A*, 2015, p. 39.
[658] La délégation de compétence peut être définie comme le fait, pour une autorité administrative, de se dessaisir, dans les limites prévues par la loi, d'un ou plusieurs de ses pouvoirs en faveur d'un autre agent qui les exercera à sa place.

la mutualisation de moyens arrive en second plan. Pour certains auteurs, le GHT ne serait qu'une étape intermédiaire qui mènera irrémédiablement vers une fusion des établissements[659]. Il ne faut pourtant pas oublier le sens premier du terme coopération. Le dictionnaire donne la définition suivante de la notion de coopération : « *action de coopérer, de participer à une œuvre commune* ». En droit public, la coopération peut être définie comme la mise en commun de moyens par plusieurs partenaires afin de réaliser des missions communes. Elle suppose donc un partage des tâches, des moyens mais également des responsabilités. Or, le mécanisme de délégation d'activité est, pour sa part, totalement différent. En effet, un seul établissement dans ce cas sera responsable de l'exécution des missions et lui seul sera également responsable en cas d'échec. Cependant, le délégataire détiendra seul l'autorité décisionnaire, contrairement aux coopérations, où les établissements décident ensemble, dans le cadre d'instances.

567. Bien entendu, cette analyse doit être nuancée dans le cas des GHT. En effet, toutes les activités ne font pas l'objet d'une délégation de compétence. Pour certaines il y aura réelle mutualisation des moyens. L'existence d'un projet médical commun est d'ailleurs la preuve irréfutable de l'existence d'une forme de coopération. Par ailleurs, les textes prévoient l'existence d'une gouvernance commune. Ainsi, l'article L. 6132-2 du Code de la santé publique prévoit la mise en place d'un comité stratégique chargé de « *se prononcer sur la mise en œuvre de la convention et du projet médical partagé* », composé des directeurs des établissements membres, des Présidents de CME et des Présidents de CSIRMT des établissements membres.

Le GHT apparait donc à ce stade comme une formule hybride, à la lisière entre coopération fonctionnelle et coopération organique, et faisant appel à plusieurs mécanismes juridiques très distincts pour fonctionner.

568. Nous pouvons ensuite nous interroger sur la réelle simplicité attachée à l'absence de personnalité morale du GHT. En effet, le rapport intermédiaire de la mission Groupements Hospitaliers de Territoire, menée par Jacqueline HUBERT et Fréderic MARTINEAU et rendu en mai 2015, prônait une absence de personnalité morale, invoquant la lourdeur des

[659] HOUDART, Laurent. HOUDART, Stéphanie. CHAMPENOIS, Guillaume. «Tout ce que vous avez toujours voulu savoir sur les GHT », article disponible sur [http://www.houdart.org]. Consulté le 20 avril 2016.

coopérations donnant lieu à création d'une nouvelle personne morale et estimant que cette absence de personnalité morale pouvait au contraire se révéler être une condition de réussite de la coopération[660]. Or, cette simplicité présupposée n'existe pas en réalité[661]. En effet, le GHT existera par le biais de différents montages conventionnels, conventions qui pourraient se décliner sur trois niveaux différents (convention constitutive, convention(s) de partenariat et convention(s) d'association.). A ce sujet, Jacques HARDY parle d'un « *usage de la forme contractuelle […] poussée aux limites de la nécessité de créer une personne morale dédiée à la coopération* »[662]. Par ailleurs, l'absence de personnalité juridique peut laisser craindre une certaine fragilité du dispositif, même si, à ce sujet, les avis de la doctrine divergent[663].

569. Cette absence de personnalité juridique du GHT apporte, selon nous, une autre difficulté importante : celle de la répartition des responsabilités au sein d'une structure sans personnalité juridique. La réponse est simple pour les activités déléguées à l'établissement support. En effet, celui-ci en tant que délégataires devra en assumer l'ensemble des responsabilités, et ce poids ne sera pas anodin pour l'établissement qui aura la lourde charge d'être le support d'un GHT.

570. Cependant, pour ce qui est des activités mises en commun, et notamment la mise en place éventuelle de pôle inter-établissements, il sera nécessaire pour chacun des membres du GHT d'apporter une vigilance particulière à la traçabilité de l'ensemble de leurs actes. La répartition des responsabilités sera donc toujours possible, en appliquant les règles de droit commun. Force est de constater que l'existence d'une personne morale dûment identifiée

---

[660] HUBERT Jacqueline. MARTINEAU, Fréderic. « Mission Groupements Hospitaliers de Territoire » rapport intermédiaire, mai 2015, p. 25.

[661] KELLER, Catherine. « De la communauté hospitalière de territoire au groupement hospitalier de territoire : continuité et rupture », *op. cit.*

[662] HARDY, Jacques. « *Les catégories juridiques à l'épreuve de la réforme administrative. Le Cas des groupements hospitaliers de territoire* », *AJDA*, 2017, p. 919.

[663] *V.* notamment en ce sens VARNIER, Frédéric. « La coopération hospitalière au service de la modernisation de notre système de santé », *op. cit.*, p.620, qui estime que l'absence de personnalité juridique n'est pas synonyme de fragilité juridique, les activités étant simplement déplacées d'un établissement à un autre, conservant sa personnalité morale. *V.* également HARDY, Jacques. « Les catégories juridiques à l'épreuve de la réforme administrative. Le Cas des groupements hospitaliers de territoire », *op. cit.*. L'auteur estime pour sa part que « *l'absence de personnalité morale n'est pas surprenante dès lors qu'un GHT personnalisé aurait inévitablement été le moyen et, en même temps, le résultat d'une fusion des établissements concernés* ».

aurait permis d'éviter ce genre de difficultés. Quoi qu'il en soit, cette nouvelle organisation « *interroge les équilibres internes liés à la place respective de chaque établissement* »[664].

571. Enfin, dernière difficulté majeure, celle de l'articulation du GHT avec les coopérations déjà existantes. En effet, comme le souligne Catherine KELLER, l'absence de personnalité juridique rend plus compliquée l'articulation des coopérations déjà en place - peu importe leur forme - avec le GHT. Alors qu'une nouvelle personne morale aurait pu reprendre à son compte les coopérations existantes, le GHT, simple coopération fonctionnelle entre plusieurs établissements, devra cohabiter avec d'autres coopérations, la plupart existant sous la forme de GCS de moyens. Finalement cela amène à une autre question essentielle, celle de la pérennité des coopérations actuellement en place. Question d'autant plus importante pour les coopérations existantes en matière de compétences qui devront être déléguées à l'établissement support. Nous pensons ici par exemple aux ex-SIH devenus GIP dans le domaine de l'informatique ou encore aux groupements dont la mission est la mutualisation des achats hospitaliers. Par ailleurs, la question se pose également pour les domaines pour lesquels la délégation n'est pas aujourd'hui obligatoire au sein des GHT mais où une mutualisation est fortement préconisée telle que l'imagerie ou la biologie. Aujourd'hui, des GHT qui mutualiseraient leurs activités de biologie seraient amenés à coexister avec des GCS, parfois vieux de plusieurs années, au sein desquels des établissements coopèrent de manière efficace sur ces sujets. Catherine KELLER s'interroge à juste titre sur ce sujet : « *les établissements publics, adhérents, avec des établissements privés de santé, à des GCS de moyens […] vont-ils devoir renoncer à des années de dynamique coopérative […] ou s'impliquer dans une sédimentation coopérative complexe ?* ».[665]

2) La mutualisation des SIS entre établissements de santé

572. « *Vague de fond qui va modifier sur le long terme le marché de l'informatique et de l'e-santé en France* »[666]. Telle est la qualification donnée à l'obligation de mise en place d'un système d'information de santé convergent au sein des GHT, qui devra être opérationnel au

---

[664] SAISON-DEMARS, Johanne. « Modernisation du système de santé : une gouvernance hospitalière à géométrie variable ». *RDSS*, 2016, p. 633.
[665] KELLER, Catherine. « De la communauté hospitalière de territoire au groupement hospitalier de territoire : continuité et rupture », *JCP –A*, 2015, p. 41.
[666] Propos de Christophe Boutin, président de Maincare Solutions, lors d'un entretien à TICsanté le 16 février.

31 décembre 2020, étant entendu que la lourde tâche de gérer cela revient à l'établissement support de chaque GHT. Ce dispositif, à la fois innovant et parfaitement restructurant, nous amène à formuler plusieurs réflexions. Une première concernant le choix des mots, qui n'est pas anodin. En effet, la loi parle bien de convergence des SIS. Cependant cette convergence s'opérera au fil de l'eau et non, comme l'a signalé le rapport de fin de mission de jacqueline HUBERT et Frédéric MARTINEAU à l'occasion d'une opération « *Big Bang* »[667]. En effet, la loi Touraine instaure bien une convergence des SIS et non une fusion. Le choix des termes est important et le rapport se veut rassurant, précisant qu'il ne s'agit pas d'un "plan Marshall" de refonte des systèmes d'information mais plutôt la mise en place d'une gestion prévisionnelle cohérente des investissements futurs en la matière et des évolutions des SIS en place. La solution de l'implémentation d'une brique logicielle d'interopérabilité a donc été écartée, au profit d'une convergence certes plus lente, mais à terme plus efficace selon nous, puisqu'elle permettra de trouver, au sein de chaque GHT, un système d'information unifié, avec des logiciels identiques. La mutualisation de la fonction achats au sein du GHT devient ici un atout majeur et facilitateur en la matière.

573. D'un point de vue pratique, cette convergence a pour but principal d'uniformiser les outils de travail des professionnels qui pourront être amenés, à l'occasion de la mise en place des projets médicaux des GHT, à travailler au sein de plusieurs établissements différents. Ce sera aussi l'occasion d'uniformiser la gouvernance des systèmes d'information santé au niveau d'un territoire donné. Dès lors, le nombre d'acteurs en charge de la mise en œuvre des SIS et de la politique publique en la matière sera considérablement diminué, ce qui facilitera le dialogue et les échanges entre, d'une part, l'Etat, à l'origine des grandes orientations politiques en la matière et, d'autre part, l'ARS et les établissements de santé, principaux utilisateurs mais également exécuteurs de ces politiques. La convergence des SI au sein des GHT nous apparait constituer une opportunité intéressante pour permettre d'améliorer le développement et l'efficacité des SIH. Même si cette solution ne permettra pas de prendre en compte l'ensemble des spécificités de chaque membre d'un GHT, elle présente le grand avantage de diffuser de manière plus uniforme les politiques publiques. En termes d'organisation pratique, elle induit la mise en place d'une direction des systèmes d'information unique et centralisée. Elle nécessite également la mise en place d'un schéma

[667] HUBERT Jacqueline. MARTINEAU, Fréderic. « Mission Groupements Hospitaliers de Territoire », *op. cit.*, p. 22.

directeur des SIS unique. C'est d'ailleurs ce schéma directeur qui est, dans les deux années qui suivront la promulgation de la loi Touraine et des décrets d'application, la priorité.

La convergence des SI au sein du GHT présente toutefois, selon nous, quelques difficultés.

574. La première, que nous avons soulevée rapidement dans notre paragraphe précédent, concerne l'avenir des coopérations déjà en place en matière de système d'information et leur survie face aux GHT. En effet, nombreux sont les établissements qui se sont regroupés, sous forme de GCS, de GIP ou, avant cela, sous forme de SIH dans le but de mutualiser leurs moyens en matière de systèmes d'information hospitaliers. A ce sujet, le rapport intermédiaire de la mission GHT précise bien que « *les outils de coopération sont très largement utilisés* », étant précisé que 326 GCS (sur 621 existant à ce jour) sont constitués dans le seul but de mutualiser des fonctions informatiques. Certains de ces groupements sont par ailleurs devenus aujourd'hui des références en la matière. Citons par exemple le GIP SIB[668] ou encore le GIP e-sis. Mais finalement, ces groupements qui se sont, avec le temps, professionnalisés, au point de devenir éditeurs de logiciels, hébergeur à part entière, ne sont pas réellement menacés. Au contraire, l'avènement des GHT peut être synonyme de nouveaux clients. En revanche, certaines coopérations fonctionnelles, entre plusieurs établissements de petites tailles, seront certainement amenées à disparaitre ou tout du moins à se fondre dans les GHT ce, au nom de la convergence obligatoire des SIS.

575. La deuxième interrogation porte sur l'hébergement des données de santé de l'ensemble des établissements membres du GHT. Le rapport de la mission est assez clair sur ce sujet : il est préférable que l'établissement support ne soit pas hébergeur. En effet, cela, comme nous l'avons étudié auparavant, induirait de trop lourdes responsabilités mais également une trop lourde procédure pour se faire agréer. En effet, la convergence des SIS n'implique pas selon nous que l'établissement support endosse la responsabilité de l'archivage des données de santé, responsabilité par ailleurs lourde et complexe. Cependant, il devra peut-être, pour plus

[668] Le groupement d'intérêt public Santé Informatique de Bretagne (SIB) est un établissement public de coopération hospitalière spécialisé dans les prestations informatiques à destination des établissements de santé. Il est par ailleurs agréé hébergeur de données de santé.

de cohérence, orienter et coordonner le choix des établissements membres du GHT pour un hébergeur agréé unique.

Conclusion de la section

576. L'interopérabilité des SIS reste un défi technique majeur à relever dans le cadre de l'instauration d'une gouvernance unifiée et cohérente des SIS. Ce défi est de taille et aujourd'hui encore de nombreux obstacles empêchent son parfait développement. Pour autant, l'ASIP Santé y travaille depuis sa création et le législateur, encore très récemment, est venu débloquer en faisant du NIR l'identifiant de santé tant attendu.

L'Etat, chargé de donner une impulsion globale en matière de SIS, doit également veiller au bon développement des politiques qu'il élabore en la matière. Pour l'aider dans cette mission, il doit s'appuyer sur les acteurs présents à l'échelon régional. A ce titre, les ARS et les GHT se révèlent alors essentiels à la diffusion et la mise en œuvre concrète des politiques nationales développées en la matière. L'ARS, en tant que représentant de l'Etat dans la région en matière de politique de santé, va être en charge de l'application régionale des politiques développées en matière de SIS. Les ARS ont d'ailleurs joué un rôle majeur dans le programme Hôpital Numérique. Les GHT, nouveaux venus dans le paysage des coopérations hospitalières vont, quant à eux, permettre d'accélérer la convergence des SIS des différents établissements publics de santé.

Conclusion du chapitre

577. Instaurer une gouvernance efficace des SIS n'est pas chose aisée. Les interlocuteurs sont nombreux et éclectiques (Etat, Assurance maladie, établissements de santé, industriels du secteur, professionnels de santé.) les enjeux ne sont pas forcément les mêmes pour tous et les besoins différent souvent. A cela s'ajoute la technicité du sujet et, en conséquence, la nécessité d'un soutien d'experts. Dans ce contexte, l'Etat a tenté d'instaurer, dès 2009, une gouvernance intelligente et efficace, déléguant notamment la maîtrise d'ouvrage à une agence spécialisée en la matière et supprimant les organismes redondants et inefficaces. Cette gouvernance n'est bien entendu pas parfaite et se doit d'être améliorée. Pour ce faire, l'interopérabilité des SIS fait partie des pistes principales à explorer. Cette problématique assez technique, une fois résolue permettrait d'assurer une unicité et une cohérence nécessaires au sein des SIS, ce qui facilitera ainsi leur développement.

Par ailleurs, l'Etat ne peut pas ignorer l'importance des acteurs régionaux, qui jouent un rôle très important dans la gouvernance des SIS. En effet, l'Etat n'a pas d'autre choix que de s'appuyer sur les ARS pour diffuser et mettre en place ses politiques publiques relatives aux SIS. Mais l'échelon régional permet également d'adapter ces politiques, parfois trop généralistes et non adaptées aux spécificités des territoires de santé. Enfin, les GHT, nouveaux acteurs dans le paysage ont également un rôle majeur dans la gouvernance des SIS. Ils vont en effet permettre la convergence de plusieurs systèmes d'information hospitaliers, améliorant ainsi l'interopérabilité des systèmes et donc l'ensemble des projets qui pourront par la suite être mis en œuvre en matière de SIS par l'Etat.

Chapitre 2

La refonte du cadre juridique, un effort nécessaire

578. A ce stade de nos travaux, nous constatons que le cadre relatif aux TIC en santé est loin d'être abouti ni même adapté aux exigences ou aux besoins des professionnels. En effet, la spécificité même du sujet, à savoir l'utilisation d'outils d'information et de communication à distance, dans le contexte sensible, voir même intime, de la santé, rend son appréhension par le droit assez complexe.

D'un côté, le cadre en place doit être suffisamment souple pour accorder à la technologie la liberté dont elle a besoin afin d'évoluer constamment. D'un autre côté, le patient, son intimité et sa vie privée, doivent être protégés. Le législateur se retrouve donc face à un paradoxe : ne pas trop interdire, en veillant de ne pas trop en permettre non plus. En parallèle, il doit également jongler avec les différents intérêts en présence : les professionnels de santé, qui souhaitent voir leurs outils et leurs techniques évoluer en étant adaptés à leur pratique quotidienne ; les patients, dont la sécurité, et celle de leurs données personnelles doivent être assurées ; les industriels, qui souhaitant profiter, économiquement, de la commercialisation et de l'utilisation des nouvelles technologies. Ces contraintes liées aux exigences des matières et du secteur concernés se confrontent alors aux contraintes plus classiques du législateur. Il doit en conséquence construire un cadre juridique adapté à un domaine innovant, respectueux de la hiérarchie des normes et des cadres juridiques déjà en vigueur.

Cependant, le cadre juridique actuel, principalement construit au fil des évolutions technologiques, s'avère aujourd'hui incertain, fragilisant ainsi la sécurité juridique. (section I)

Il doit être repensé pour être adapté aux besoins actuels des professionnels de santé et ce, afin d'obtenir un juste équilibre entre respect des droits des patients et de ses données et efficacité des technologies disponibles (section II).

Section 1. Le cadre juridique actuel, source d'insécurité juridique

579. L'étude du cadre juridique des TIC en santé nous amène à identifier deux difficultés majeures : d'une part, le cadre semble aujourd'hui trop complexe, du fait notamment de sa forme, basé sur un empilement de références éparses, distinctes et parfois contradictoires ; d'autre part, il ne permet pas d'assurer la sécurité juridique nécessaire au bon développement et à une utilisation croissante des TIC en santé. Dès lors, ce cadre se révèle aujourd'hui être une source d'incertitudes et surtout, d'insécurité juridique pour l'ensemble des acteurs du domaine. Pour étayer nos propos, il nous est nécessaire dans un premier temps de revenir sur le concept même de sécurité juridique (Paragraphe I), avant de réfléchir aux origines de la complexité du cadre juridique actuel des TIC en santé, et donc de son insécurité (Paragraphe II).

§1. Retour sur la notion de sécurité juridique

« *Les lois inutiles affaiblissent les lois nécessaires* »[669]

580. Parfois qualifié de concept "clandestin", le principe de sécurité juridique est pourtant régulièrement associé au concept d'Etat de droit et considéré, comme une des finalités du droit. Ce principe est pourtant assez récent et demeure une création purement jurisprudentielle et doctrinale. Par ailleurs, le principe de sécurité juridique induit plusieurs applications concrètes et fondamentales dans notre droit et notamment la prévisibilité de la loi ainsi que la clarté et l'accessibilité de la norme. Afin d'appréhender ce concept, il nous est donc nécessaire de nous attarder sur les principes de clarté et d'intelligibilité de la norme (A), avant d'envisager les solutions avancées afin de garantir la sécurité juridique du droit (B).

[669] Montesquieu. « De l'esprit des lois », Partie 6, Livre XXIX « De la manière de composer les lois », 1758.

A. Portées des principes de clarté et d'intelligibilité de la norme

« *Quand le droit bavarde, le citoyen ne lui prête plus qu'une oreille distraite* ».[670]

581. Même si, selon le célèbre adage, « nul n'est censé ignoré la loi », il est évident qu'une loi qui ne serait pas appréhendable par le citoyen risquerait d'être, de ce fait, ignorée. La sécurité juridique induit donc une clarté et un caractère intelligible afin d'assurer son accessibilité par le citoyen. Ces concepts, composantes de la notion de sécurité juridique (2) se doivent d'être définis précisément (1).

1) Définition des principes

Quand on aborde la notion de sécurité juridique, d'autres principes sont régulièrement associés. Il s'agit des notions de clarté, d'intelligibilité et d'accessibilité de la loi.

582. C'est le Conseil constitutionnel qui, par plusieurs décisions, consacre le principe de clarté de la loi, avant de finalement l'abandonner. Bien que ces exigences de clarté et de précision dans la rédaction des dispositions législatives soient traditionnellement exigées par le Conseil constitutionnel en matière pénale[671], le principe de clarté de la norme est cependant apparu de manière explicite dans une décision portant sur une loi relative au travail. En effet, c'est dans sa décision n° 98-401 DC du 10 juin 1998, portant sur la loi d'orientation et d'incitation relative à la réduction du temps de travail que la Haute juridiction précise qu'une mesure définie de manière suffisamment claire et précise satisfaisait aux exigences posées par l'article 34 de la Constitution. Le Conseil constitutionnel exigeait désormais des lois qu'elles comportent des « *dispositions suffisamment précises et des formules non équivoques* »[672]. Puis, en 1999, les juges de la rue Montpensier ont dégagé un objectif à valeur constitutionnelle : celui d'accessibilité et d'intelligibilité de la loi[673].

583. Cependant, très vite, la doctrine a souligné la confusion possible entre ces deux notions relativement proches. Pour la doctrine, le Conseil constitutionnel lui-même était

---

[670] Rapport du Conseil d'Etat. « De la sécurité juridique », 1991, *La documentation française*.
[671] Les documents de travail du Sénat. « La qualité de la loi », série études juridiques, septembre 2007, p. 15.
[672] *Id.*, p. 16, à propos de la Décision n° 2001-455 DC du 12 janvier 2002.
[673] Décision n° 99-421 DC du 16 décembre 1999.

prompt à confondre le principe de clarté de la loi et l'objectif à valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi. Une étude de sa jurisprudence tend à démontrer la confusion réalisée par les Sages eux-mêmes[674]. Or, pour certains auteurs « *la volonté du Conseil de distinguer principe de clarté de la loi et objectif d'intelligibilité et d'accessibilité de la loi n'aurait été légitime qu'au prix d'une politique jurisprudentielle rigoureuse justifiant l'utilité respective de chacun des concepts* »[675]. De même, certains auteurs confondaient régulièrement les deux, allant parfois jusqu'à invoquer un objectif à valeur constitutionnelle de clarté et d'intelligibilité de la loi.[676] Il apparait effectivement assez complexe de mesurer la différence qui peut exister entre, d'une part, la clarté de la loi et, d'autre part, l'accessibilité et l'intelligibilité de la loi. La doctrine a donc très vite manifesté son intérêt pour l'objectif à valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, préconisant un abandon pur et simple du principe de clarté de la loi : « *la malléabilité de l'objectif de valeur constitutionnelle parait donc particulièrement adaptée à la recherche d'une plus grande qualité du droit […]. Au contraire le principe de clarté, parce qu'il semble vouloir recouvrir une dimension objective, induit une rigidité qui cadre mal avec la relativité de la notion de « qualité de droit » […] qui […] ne peut s'apprécier qu'au regard des circonstances de l'espèce* ».[677]

584. C'est ainsi que le Conseil constitutionnel, dans une décision du 27 juillet 2006, abandonna la référence au principe de clarté de la loi pour lui préférer l'objectif d'intelligibilité et d'accessibilité de la loi comme référence unique : « *considérant qu'il incombe au législateur d'exercer pleinement la compétence que lui confie la Constitution et, en particulier, son article 34 ; que le plein exercice de cet exercice, ainsi que l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, qui découle des articles 4, 5, 6 et 16 de la Déclaration des droits de l'homme et du citoyen de 1789, lui imposent d'adopter des dispositions suffisamment précises et des formules non équivoques […]* »[678]

---

[674] *V.* notamment en ce sens MILANO, Laure. « Contrôle de constitutionnalité et qualité de la loi », *Revue de droit public*, n° 3, 2006, p. 637.
[675] *Ibid.*
[676] *V.* notamment en ce sens LANDAIS, Claire. LE NICA, Frédéric. « Sécurité juridique : la consécration », *AJDA*, 2006, p. 1028
[677] GAY, Laurence, « Jurisprudence du Conseil constitutionnel », *Revue française de droit constitutionnel*, n° 50, avril-juin 2002, pp. 385-445.
[678] Décision n° 2006 - 540 DC du 27 juillet 2006.

Désormais, seul l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi doit être respecté par le législateur et peut fonder une déclaration de non-conformité à la Constitution.[679]

2) Des composantes d'un concept plus large : celui de sécurité juridique

585. La notion de sécurité juridique n'apparait pas au sein de notre corpus constitutionnel ou législatif et, bien qu'il la protège, le Conseil constitutionnel n'a pour autant jamais consacré la notion de sécurité juridique au sein de sa jurisprudence[680]. En revanche, le Conseil d'Etat a fait le choix de consacrer de manière solennelle ce principe jusqu'alors inexistant dans le droit administratif. Ainsi, par une décision en date du 24 mars 2006, le Conseil d'Etat, réuni en Assemblée[681], a pour la première fois, affirmer le principe de sécurité juridique. En l'espèce, les juges avaient dû se prononcer sur la légalité du décret du 16 novembre 2005 portant approbation du Code de déontologie des commissaires aux comptes. A cette occasion, la Haute juridiction précise que : *« considérant qu'indépendamment du respect de cette exigence, il incombe à l'autorité investie du pouvoir réglementaire d'édicter, pour des motifs de sécurité juridique, les mesures transitoires qu'implique, s'il y a lieu, une réglementation nouvelle […]* »[682] avant d'affirmer, pour le cas d'espèce qui lui était soumis que *« toutefois, à défaut de toute disposition transitoire dans le décret attaqué, les exigences et interdictions qui résultent du code apporteraient, dans les relations contractuelles légalement instituées avant son intervention, des perturbations qui, du fait de leur caractère excessif au regard de l'objectif poursuivi, sont contraires au principe de sécurité juridique* ». Il est intéressant de noter que cette décision symbolique fut par ailleurs rendue quelques semaines après la publication du rapport du Conseil d'Etat consacré à la sécurité juridique[683].

586. Tous les auteurs n'ont cependant pas accueilli de la même façon cette décision, certains considérant que cet arrêt « *constitue un signal fort quant à l'orientation de la*

---

[679] Les documents de travail du Sénat, série études juridiques, « La qualité de la loi », septembre 2007, p. 22.
[680] DUTHEILLET de LAMOTHE, Olivier. « La sécurité juridique : le point de vue du juge constitutionnel », rapport du Conseil d'Etat « Sécurité juridique et complexité du droit », mars 2006, p. 369.
[681] CE, Ass. 24 mars 2006, KPMG et autres, n° 288460 et s, Rec., p. 154 ; *AJDA*, 2006, p. 1028, chron. C. LANDAIS, Claire et LE NICA Frédéric ; *RFDA*, 2006, p. 463, concl. AGUILA, Yann ; *BJCP*, 2006, p. 173, concl. AGUILA, Yann.
[682] A noter que les dispositions de cette jurisprudence sont désormais codifiées au sein du Code des relations entre le public et l'administration, à l'article L. 221-5.
[683] Rapport public du Conseil d'Etat, « Sécurité juridique et complexité du droit », mars 2006.

jurisprudence administrative»[684], tandis que d'autres, plus frileux, se demandaient si l'évocation par le Conseil d'Etat dans ses considérants d'un motif de sécurité juridique, suffisait à lui seul pour en déduire que la Haute juridiction venait consacrer le principe[685]. Bien qu'enfin consacré, ce principe protéiforme pâtit toujours aujourd'hui d'un manque de définition précise de ses contours.

Finalement, le principe de sécurité juridique, ne serait qu'un « *un pavillon qui recouvre une multitude de principes plus spécifiques dont les caractéristiques - et notamment la valeur - peuvent être différentes* »[686]. Certains auteurs, comme le rapporte Fabrice MELLERAY, sont même allés jusqu'à parler « *d'instillation* » dans notre droit d'une perspective de sécurité plutôt que de la naissance d'un réel principe[687].

587. Pour le Conseil d'Etat, « *le principe de sécurité juridique implique que les citoyens soient, sans que cela appelle de leur part des efforts insurmontables, en mesure de déterminer ce qui est permis et ce qui est défendu par le droit applicable* »[688]Pour y parvenir, il est nécessaire que la norme réponde à certaines exigences matérielles et temporelles[689].

588. L'exigence matérielle réside principalement dans la qualité de la norme édictée. « *la loi permet, ordonne, édicte* »[690]. Cette exigence de qualité renvoie à l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi. En ce sens, l'accessibilité et l'intelligibilité de la loi sont deux des différentes caractéristiques qui composent le principe de sécurité juridique.[691] Pour autant, comme l'avait souligné le Sénat dans son étude consacrée au sujet, la loi peut être complexe, sans pour autant être contraire à la sécurité juridique. Le Conseil constitutionnel a eu l'occasion d'affirmer cette position à plusieurs reprises. Ce fut

---

[684] LANDAIS, Claire. LE NICA, Frédéric. « Sécurité juridique : la consécration », *AJDA*, 2006, p. 1028.
[685] MELLERAY, Fabrice. « L'arrêt KPMG consacre-t-il vraiment le principe de sécurité juridique ? », *AJDA*, 2006, p. 897.
[686] CASSIA, Paul. « La sécurité juridique, un « nouveau » principe général du droit aux multiples facettes », *Dalloz*, 2006, p. 1190.
[687] MELLERAY, Fabrice, « L'arrêt KPMG consacre-t-il vraiment le principe de sécurité juridique ? », *op. cit.*, en citant PACTEAU, Bernard, « La sécurité juridique, un principe qui nous manque ? », *AJDA*, numéro spécial 1995, p. 151.
[688] Rapport public du Conseil d'Etat « Sécurité juridique et complexité du droit », *op. cit*., p. 281.
[689] D'une manière différente, Paul CASSIA fait le choix de décomposer le principe de sécurité juridique en différenciant son volet objectif de son volet subjectif.
[690] PORTALIS, « Discours préliminaire du Code civil », 1804.
[691] MATHIEU, Bertrand. « Les lois de finances au crible de la sécurité juridique», *LPA*, n° 10, 2006, p. 4.

notamment le cas dans sa décision n° 2000-437 DC du 19 décembre 2000. En l'espèce, la loi de financement de la sécurité sociale pour 2001 avait été soumise à son appréciation. Les juges de la Haute juridiction avaient alors précisé que « *si la loi déférée accroit encore la complexité des circuits financiers […] elle énonce de façon précise les nouvelles règles de financement qu'elle instaure* ». Ainsi, une loi pourra être intelligible, mais complexifier les règles en place, sans que cela ne porte atteinte, aux yeux du Conseil constitutionnel, à la sécurité juridique[692].

589. L'exigence temporelle quant à elle réside dans l'impératif de prévisibilité du droit, dont découle le principe de non-rétroactivité de la norme mais également l'obligation d'instaurer des mesures transitoires. Le principe fondamental de non rétroactivité de la norme est posé par l'article 2 du Code civil, selon lequel « *la loi ne dispose que pour l'avenir ; elle n'a point d'effet rétroactif* ». S'il était encore nécessaire d'insister sur le caractère quasi sacré de ce principe dans notre droit, rappelons que cette disposition du Code civil existe et, est restée inchangée, depuis 1803. En ce qui concerne les actes administratifs, le principe développé par la jurisprudence du Conseil d'Etat est le même[693]. Enfin, la nécessité, pour le législateur, d'instaurer des mesures transitoires lors de la mise en place d'une nouvelle réglementation a été posé par le même arrêt venant reconnaitre l'existence du principe de sécurité juridique, l'arrêt dit "KPMG".

La sécurité juridique constitue donc un principe vaste, aux contours non réellement définis de manière stricte à l'heure actuelle. Il est toutefois possible d'améliorer cette sécurité juridique, grâce à plusieurs outils.

B. Les outils de lutte contre l'insécurité juridique

590. Aujourd'hui, nombreux sont les articles de doctrine portant sur la notion de sécurité juridique. Le Conseil d'Etat ainsi que les sages du Conseil constitutionnel se sont également saisis du sujet. C'est d'ailleurs en grande partie à cette occasion que des pistes de lutte contre

---

[692] Conseil constitutionnel, décision n° 2000-437 DC du 19 décembre 2000, *JORF* n°298 du 24 décembre 2000, p. 20576.

[693] CE, Ass, 25 juin 1948, Société du journal l'Aurore, Rec. p. 289 ; *Gaz. Pal*, 1948, 2, p. 7, concl. LETOURNEUR ; *JCP G* 1948, II, 4427, note MESTRE ; *GAJA* 1999, p. 408.

l'insécurité juridique ont été avancées (2). Mais avant d'envisager celles-ci, il est intéressant de s'attarder sur les causes de la fragilisation actuelle de la sécurité juridique (1).

1) Les origines variées de l'insécurité juridique

591. « *Ce mal, on le sait, est protéiforme. L'insécurité juridique se nourrit de l'inflation normative comme de l'instabilité des règles ou encore du déclin de l'art de légiférer* »[694]. Nicolas MOLFESSIS nous apporte, par ce constat, les principales causes de l'insécurité juridique. En effet, l'insécurité juridique, ou plutôt, la mise en danger de la sécurité juridique, résulte principalement d'une multiplication croissante des normes et de leur révision régulière. Cet accroissement des normes trouve plusieurs sources diverses.

592. La première est l'apparition, ces dernières années, de nouveaux domaines de législation, portant sur des spécialités parfois complexes. C'est par exemple le cas des biotechnologies, ou du secteur du numérique qui, comme nous l'évoquons tout au long de nos recherches, a des répercussions dans de nombreux domaines, et notamment celui de la santé.
Ces secteurs liés à la technologie de pointe évoluent rapidement, et le législateur a parfois des difficultés à suivre cette évolution, le temps du débat parlementaire n'étant clairement pas le même que celui du progrès scientifique. Au final, nous nous retrouvons avec un corpus de textes épars, parfois contradictoires et souvent inadaptés.

De même, le foisonnement des normes est accentué par l'augmentation des sources de droit externes. Si nous restons sur l'exemple des Technologies de l'Information et de la Communication, le Conseil d'Etat, dans son rapport annuel de 2006, a constaté que pas moins de 6 directives avaient été adoptées à ce sujet par l'Union européenne depuis le milieu des années 1990[695]. Par ailleurs, comme nous l'étudierons plus en détails ultérieurement, le règlement européen relatif à la protection des données personnelles, publié le 4 mai 2016[696], et transposable directement d'ici 2018 bouleverse notre droit interne, modifiant certaines

---

[694] MOLFESSIS, Nicolas. « Combattre l'insécurité juridique ou la lutte contre du système juridique contre lui-même », rapport du Conseil d'Etat « Sécurité juridique et complexité du droit », mars 2006, p. 391.
[695] Rapport du Conseil d'Etat « Sécurité juridique et complexité du droit », mars 2006, p 240.
[696] 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, 4 mai 2016, L 119/1.

dispositions de la loi Informatique et Libertés de 1978, déjà pourtant modifiée à plusieurs reprises.

593. Le rapport du Conseil d'Etat insiste également sur une nouvelle source possible du droit, qui est apparue avec la naissance des autorités administratives indépendantes En effet, certaines d'entre elles disposent d'un pouvoir normatif et toutes contribuent à l'élaboration de règles applicables au travers de leurs décisions. C'est ainsi le cas de la CNIL, dont les décisions font loi dans le domaine spécifique de la protection des données à caractère personnel.

594. Autre source d'insécurité juridique régulièrement relevée, le contournement de la procédure parlementaire, voire sa dénaturation, visant notamment l'utilisation abusive des ordonnances de l'article 38 de la Constitution ou encore à la procédure d'urgence. Par ce biais sont régulièrement adoptées des ordonnances dite de "simplification", dont les conséquences sur notre droit ne sont finalement pas celles attendues, certains auteurs allant même jusqu'à parler de "cynisme" du pouvoir exécutif.

L'atteinte à la sécurité juridique passe également par une atteinte directe à la qualité de la norme. Une norme fragile ou une norme incomplète ne permettra pas d'assurer la sécurité juridique que tout citoyen est en droit d'attendre. Or, la loi est parfois paralysée par l'absence de publication des textes d'application[697].

595. Enfin, face à ces sources du foisonnement de la norme, que nous pouvons qualifier d'objectives, nous trouvons des causes plus subjectives, présentant plutôt un caractère politique et sociologique. Comme le résume très bien Guy Carcassonne, « *tout sujet d'un vingt heures est virtuellement une loi* »[698]. La force très symbolique de la loi en France pousse parfois les gouvernants à abuser de cet outil[699]. Or, communication politique et droit ne font pas forcement bon ménage et il en résulte parfois des lois inutiles et un corpus juridique complexifié. Le médiateur de la République a également réalisé ce constat, rappelant, à

[697] MORVAN, Patrick. « Le principe de sécurité juridique : l'antidote au poison de l'insécurité juridique ? », *Droit social*, 2006, p. 707.
[698] CARCASSONNE, Guy. « Penser la loi », *Pouvoirs*, septembre 2005, p. 39.
[699] De CLAUSSADE, Jocelyne. « Sécurité juridique et complexité du droit : considérations générales du Conseil d'Etat », *Recueil Dalloz*, 2006, p. 737.

l'occasion de son rapport annuel de 2005, « *l'empilement des textes souvent votés trop rapidement et dans le souci, illusoire, de répondre par la précipitation législative à des emballements médiatiques et d'opinion* »[700].

Cette insécurité juridique, issue de sources variées, peut toutefois être contrée.

2) Les pistes de sécurisation du droit

596. « *La lutte contre l'insécurité juridique est devenue en soi un objet de réglementation* »[701]. Depuis plusieurs années, les textes relatifs à la simplification du droit ont tendance à se développer. Nous pouvons citer à titre d'exemple la loi n° 2014-1545 du 20 décembre 2014 relative à la simplification de la vie des entreprises et portant diverses dispositions de simplification et de clarification du droit et des procédures administratives[702], ou l'ordonnance n° 2015-1288 du 15 octobre 2015 portant simplification et modernisation du droit de la famille[703]. Mais ces textes sont loin d'être isolés et le législateur a entendu s'emparer des difficultés posées par la multiplication croissante des normes et les difficultés de lisibilité pour le citoyen que cela engendre. Malheureusement parfois, les solutions deviennent elles-mêmes sources de dysfonctionnements. Ainsi, comme le soulignait Nicolas MOLFESSIS dans son analyse, le choix des ordonnances de simplification, sensées désencombrer le parlement et simplifier rapidement et efficacement les normes en place, a abouti à l'effet inverse : le nombre croissant de ces ordonnances participant à l'inflation normative est régulièrement dénoncé et critiqué[704].

597. Finalement, il est avant tout nécessaire de réfléchir au but recherché avant de mettre en place certaines actions. La sécurité juridique, principe désormais consacré par le Conseil d'Etat, s'obtient par la mise en place de solutions concrètes et non pas par la seule édiction d'un principe. Ainsi, plusieurs solutions ont pu être avancées. En étudiant les solutions

---

[700] Médiateur de la République, rapport annuel pour 2005, p. 16.
[701] MOLFESSIS, Nicolas. « Combattre l'insécurité juridique ou la lutte contre du système juridique contre lui-même », *op. cit.* p. 391.
[702] Loi n° 2014-1545 du 20 décembre 2014 relative à la simplification de la vie des entreprises et portant diverses dispositions de simplification et de clarification du droit et des procédures administratives, *JORF* n°0295 du 21 décembre 2014, p. 21647.
[703] Ordonnance n° 2015-1288 du 15 octobre 2015 portant simplification et modernisation du droit de la famille, *JORF* n°0240 du 16 octobre 2015, p. 19304
[704] MOLFESSIS, Nicolas. « Combattre l'insécurité juridique ou la lutte contre du système juridique contre lui-même », *op. cit.* p. 394.

adoptées par nos voisins, le Conseil d'Etat avait notamment proposé, dans son rapport de 2006, de mettre en place des procédures d'élaboration des textes plus rigoureuses[705]. Cette nécessité de rigueur, avancée par la Haute juridiction dans son rapport de 2006[706] a conduit à une réforme introduite en 2009 par une loi organique[707]. Celle-ci, restée discrète[708], a pourtant introduit à l'obligation, pour les auteurs d'un projet de loi, d'en exposer les motifs, au regard notamment du droit applicable, et d'en évaluer les impacts qu'ils soient sociaux, financiers, économiques ou environnementaux. Cette réforme n'a pourtant pas forcément été appliquée correctement, le Conseil d'Etat lui-même estimant que « *même si des progrès notables sont à mettre au crédit des administrations, la qualité des études d'impact ou s'agissant des lois de finances, des évaluations préalables, doit encore être sensiblement améliorés* »[709].

Par ailleurs, signalons que ce dispositif ne vaut que pour les projets de lois. Ainsi, l'ensemble des textes émanant des parlementaires eux-mêmes ne sont pas soumis à ces études préalables. Or, comme le relève Yves JEGOUZO, l'évaluation *a priori* des lois joue un rôle mineur dans le processus de création de la norme, étant donné que ces dernières années, le gouvernement a plutôt privilégié la voie parlementaire, et donc les propositions de lois, pour faire passer ses textes[710].

598. Au niveau réglementaire, des dispositions similaires ont également été mises en place. Ainsi, comme le rappelle par exemple la circulaire n° 5817/SG du 1er ministre en date du 12 octobre 2015, « *l'évaluation préalable des projets de textes réglementaires et le gel de la réglementation défini par la circulaire du 17 juillet 2013 contribuent à l'amélioration de la qualité du droit* ». En effet, la circulaire du 17 juillet 2013[711] prévoit que tout nouveau projet de texte réglementaire créant des charges nouvelles pour les collectivités, les entreprises ou le public ne peut être adopté sans qu'il soit, en contrepartie, accompagné d'une simplification équivalente. Il est par ailleurs prévu une évaluation préalable de l'ensemble des projets de

[705] Rapport du Conseil d'Etat « sécurité juridique et complexité du droit », *op. cit.*, p. 300.
[706] Rapport du Conseil d'Etat « sécurité juridique et complexité du droit », *op. cit.*, p. 313. Le Conseil d'Etat préconisait de recourir à une loi organique afin de fixer les obligations en termes de procédure et notamment de subordonner tout dépôt de loi d'une évaluation préalable des impacts de la réforme.
[707] Loi organique n° 2009-403 du 15 avril 2009 relative à l'application des articles 34-1, 39 et 44 de la Constitution, *JORF* n°0089 du 16 avril 2009, p. 6528.
[708] JEGOUZO, Yves. « L'étude d'impact : formalité ou garantie de la qualité de la loi ? », *AJDA*, 2012, p. 1425.
[709] Rapport annuel du Conseil d'Etat, 2012, p. 135.
[710] JEGOUZO, Yves. « L'étude d'impact : formalité ou garantie de la qualité de la loi ? », *op. cit.*, p. 135.
[711] Circulaire du 17 juillet 2013 relative à la mise en œuvre du gel de la réglementation, *JORF* n°0165 du 18 juillet 2013, p. 11993.

textes réglementaires applicables aux collectivités locales, aux entreprises ou au public, par le biais de fiches d'impact. Enfin, une information systématique du public sur ces évaluations, par le biais des publications des fiches d'impact, doit être mise en place. Ce dispositif des fiches d'impact a par ailleurs été étendu à l'évaluation préalable des projets de normes ayant des conséquences sur les missions ou l'organisation des services déconcentrés de l'Etat, textes initialement exclus du dispositif.

599. Il nous faut également signaler le travail de "débroussaillage" des circulaires qui avait été effectué ces dernières années, notamment grâce au décret n° 2008-1281 du 8 décembre 2008 relatif aux conditions de publication des instructions et circulaires[712]. En effet, comme le soulignait le législateur dans son rapport relatif au décret n° 2008-1281 du 8 décembre 2008, « *la prolifération des circulaires fait l'objet de critiques répétées de la part de membres du Parlement mais aussi des collectivités territoriales, des entreprises et plus largement de l'opinion*. » Ainsi, afin d'éviter une stratification des circulaires, et pour permettre au citoyen d'en prendre connaissance, le décret du 8 décembre 2008 oblige les administrations à publier leurs circulaires sur un site unique, celui du Premier ministre[713]. Les circulaires qui ne figurent pas sur ce site ne sont pas opposables aux administrés. A noter que l'ensemble des dispositions issues du décret de 2008 a été codifié depuis le 1er janvier 2016 au sein du Code des relations entre le public et l'administration, aux articles R. 312-8 et R. 312-9.

Le législateur travaille donc à instaurer les conditions nécessaires à une amélioration de la sécurité juridique.

[712] Décret n° 2008-1281 du 8 décembre 2008 relatif aux conditions de publication des instructions et circulaires, *JORF* n°0287 du 10 décembre 2008, p. 18777.

[713] L'article 1 du décret prévoit que « *les circulaires et instructions adressées par les ministres aux services et établissements de l'État sont tenues à la disposition du public sur un site internet relevant du Premier ministre. Elles sont classées et répertoriées de manière à faciliter leur consultation.* ».

§2. La complexité du cadre juridique s'appliquant aux TIC en santé

« *La loi protège-t-elle encore le faible lorsqu'elle est aussi complexe, foisonnante et instable ?* ».

600. Cet extrait d'un entretien accordé par Mme Josseline de CLAUSADE, Conseiller d'Etat[714], illustre bien les difficultés que posent une loi et, plus généralement, un cadre juridique trop complexe pour ses utilisateurs. En effet, un cadre juridique qui serait trop flou, trop complexe et trop diversifié, n'offre pas la sécurité juridique à laquelle le citoyen est en droit de s'attendre. Finalement, quand le droit devient complétement hermétique au profane et n'est plus accessible qu'aux plus aguerris des experts juridiques, il est légitime de se demander s'il remplit encore son rôle fondamental.

C'est, à l'échelle des TIC en santé, la question que nous pouvons légitimement nous poser. Car force est de constater que le cadre juridique général dans lequel évoluent les TIC en santé n'est pas des plus simples à appréhender (A), causant alors un sentiment global d'insécurité juridique pour les professionnels qui y sont confrontées (B).

A. L'utilisation des TIC à l'hôpital, une pratique évoluant dans des environnements normatifs distincts

601. Règlementer l'utilisation des TIC en santé induit de prendre en compte un certain nombre de paramètres n'ayant, a priori, rien à voir ni avec les technologies de communication, ni la santé à proprement parler. Cependant, l'obtention d'un cadre juridique adapté et donc facilement applicable passe par cet exercice complexe (1). Toutefois, à l'heure actuelle, le cadre existant ne fait qu'empiler différents textes, parfois généraux, parfois hyper spécialisés, sans réelle cohérence entre eux (2).

[714] Les documents de travail du Sénat, série études juridiques, « La qualité de la loi », *op. cit.*, p. 7.

1) Multiplicité des matières à prendre en compte

602. Au-delà du droit, l'introduction des TIC dans la pratique médicale « *se situe au carrefour de plusieurs approches scientifiques et de plusieurs champs sectoriels (médecine, éthique, droit, économie, psychologie,...)* »[715]. Cette multiplicité des matières à prendre en considération est une des sources de difficulté à l'élaboration d'un cadre unifié.

603. D'une manière générale, le développement des TIC touche toute la société, il modifie l'ensemble des secteurs industriels et de service mais également la vie au travail, la vie quotidienne, et plus récemment, la façon dont les personnes gèrent leur santé. Ainsi, les enjeux du développement des TIC en santé sont multiples et les considérations qui entourent son encadrement juridique sont nombreuses.

604. Un des enjeux majeurs est bien entendu l'enjeu économique. Il est clair que les industriels du secteur ne vont pas s'aventurer à développer une solution coûteuse sans retour sur investissement prévisible. Dès lors, le cadre juridique peut devenir un frein s'il s'avère trop contraignant pour les industriels, ou au contraire un élément moteur s'il s'avère être favorable, en imposant, par exemple, certaines solutions techniques ou en allouant des crédits pour le développement des TIC en santé.

605. Au-delà de l'aspect juridique se pose évidemment la question du débat éthique fortement présent dans des domaines où l'innovation scientifique touche de très près à l'humain. A titre d'exemple, les débats éthiques sont nombreux en bioéthique, autour notamment de l'encadrement de l'étude du génome et du développement de la médecine prédictive. En ce sens, l'éthique n'est pas absente des débats relatifs aux TIC en santé. Il porte particulièrement sur la confidentialité de l'information médicale, son partage et donc sur la protection de la vie privée. En effet, les TIC permettent, nous l'avons vu[716], de collecter, stocker, partager et exploiter des quantités importantes de données. Ces données, qui sont extrêmement sensibles car touchant à l'intimité des personnes qu'elles concernent, peuvent être un bien précieux pour de nombreuses personnes, que ce soient les professionnels de

---

[715] BERANGER, Jérôme. Le COZ, Pierre. « Réflexion éthique sur la pluridisciplinarité et la confidentialité de l'information en imagerie médicale via les nouvelles technologies de l'information et de la communication », *Cancer/radiothérapie*, 2012, n° 16, pp. 215-218.
[716] *V. Supra*. n° 37.

santé, les chercheurs, mais aussi les assureurs ou les organismes bancaires par exemple. La question est donc de savoir jusqu'où protéger les données de santé et avec qui les partager. Quel équilibre peut être trouvé entre bonne utilisation des données de santé et protection de la vie privée ? Cette question rejoint celle relative à la possible reconnaissance d'un droit de propriété des personnes sur leurs données personnelles[717]. Finalement, doit-on envisager un régime de dispositions des données de santé similaire à celui qui s'applique aux éléments du corps humain, interdisant de manière stricte toute possibilité de commercialisation de celles-ci ? Ou au contraire, doit-on adhérer à la théorie de l'« *Empowerment* » qui pourrait permettre aux personnes, selon certains partisans du concept, de devenir de véritables acteurs de la protection de leurs données, renforçant ainsi celle-ci ? Toutes ces questions sont aujourd'hui encore discutées dans le cadre notamment du débat relatif à l'ouverture élargie de l'accès à certaines données de santé, l'ensemble s'inscrivant dans le cadre plus large de l'open-data en santé.

606. De fait, suite au rapport rendu en 2014 à la Ministre de la santé, Madame Marisol TOURAINE, par la Commission open-data, constituée en novembre 2013, la Ministre a très vite affirmé sa volonté de développer l'open-data en santé. Le rapport de la Commission définit l'open-data comme « *l'ouverture et le partage de données par leur mise en ligne dans des formats ouverts, en autorisant la réutilisation libre et gratuite par toute personne*.»[718]. Derrière ce terme anglophone se cache donc l'ouverture au public des données de santé et ce, dans le but de promouvoir la démocratie sanitaire, favoriser l'autonomisation du patient mais aussi, et surtout, développer la recherche et l'innovation en santé. C'est ainsi que, sur la base de cette étude, la loi de modernisation de notre système de santé[719] vient, dans son chapitre V intitulé « créer les conditions d'un accès ouvert aux données de santé », prévoir les conditions du développement de l'open data en santé. La volonté du législateur est de *« réformer l'accès aux données de santé afin que leurs potentialités soient utilisées au mieux dans l'intérêt de la collectivité, et du principe de valeur constitutionnelle de protection de la santé, tout en assurant la confidentialité des données personnelles, qui procède du droit au respect de la vie privée, autre exigence de rang constitutionnel, d'autant plus forte qu'il s'agit de données*

[717] *V. Supra*. n° 111 et s.
[718] Rapport de la Commission Open Data en santé, p. 9.
[719] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte n° 1.

sensibles »[720]. Ces nouvelles dispositions sont la preuve de l'extrême importance des questions éthiques relatives aux limites de l'utilisation des données de santé face à la nécessité de protéger la vie privée.

607. Enfin, le développement des TIC en santé pousse, de manière indirecte, à se pencher sur la question de la place et de l'utilisation des réseaux sociaux. En effet, ces derniers, directement liés au développement de l'utilisation des TIC dans la société, sont aujourd'hui très présents. Qu'ils soient professionnels (VIADEO, LinKedin) ou personnels (Facebook, Twitter), leur existence, leur importance et leur force ne peuvent être ignorées. Le secteur hospitalier n'y échappe pas et nombreux sont les établissements qui ont fait le choix d'ouvrir et développer un compte Facebook ou un compte Twitter. De même, les personnels de ces établissements détenant un ou plusieurs comptes sur les réseaux sociaux sont également nombreux. Aussi, l'utilisation de ces réseaux nous amène à nous poser des questions majeures à la fois en termes de respect de la vie privée (vie privée des personnels mais également des patients) et de respect de la liberté d'expression. L'erreur majeure est de considérer les réseaux sociaux comme étant des lieux clos, où les informations échangées restent privées. En effet, selon les paramètres de confidentialité sélectionnés, les informations pourront être considérées comme publiques ou privées. Il est donc nécessaire de se reporter aux conditions générales d'utilisation du réseau social, trop souvent ignorées par les utilisateurs. A titre d'exemple, les conditions générales d'utilisation de Facebook, et plus spécifiquement leur politique d'utilisation des données, prévoient la chose suivante : *« le terme informations publiques fait référence aux informations que vous partagez avec tout le monde, dans votre profil public, ou encore aux contenus que vous partagez sur une Page Facebook ou sur un autre forum public. Les informations publiques sont accessibles à tout le monde, au sein comme en dehors de nos Services, et peuvent être vues ou retrouvées à l'aide de moteurs de recherche en ligne, d'API et de médias hors ligne, tels que la télévision.*»[721]

Ainsi, un utilisateur qui fait le choix, dans ses paramètres de sécurité, d'un profil public, doit savoir que toutes ses informations seront publiques et donc accessibles à tous, y compris par le biais de moteurs de recherche. Par ailleurs, une personne commentant un profil public ou partageant des informations (photos, commentaires ou autres) sur un profil, une

[720] Exposé des motifs loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, disponible sur : [https://www.legifrance.gouv.fr], consulté le 1er septembre 2016.
[721] Politique d'utilisation des données, Facebook, disponible sur [https://www.facebook.com]. Consultée le 29 août 2016.

page ou un groupe public, doit avoir à l'esprit que ces informations seront publiques, peu importe si son profil personnel est par ailleurs privé. Il est donc important de s'intéresser aux conditions générales d'utilisation ainsi qu'à la politique d'utilisation des données du réseau social et ce, à chaque fois qu'elles sont mises à jour, afin de paramétrer au mieux son profil et protéger ses données.

608. Toute la difficulté de l'encadrement de l'utilisation des réseaux sociaux par les professionnels des établissements de santé réside dans la juste adéquation entre le respect de la liberté d'expression des professionnels, d'une part, et le respect par ces derniers de leurs obligations professionnelles, d'autre part. En effet, rappelons que les professionnels travaillant à l'hôpital, et plus spécifiquement les professionnels de santé, sont débiteurs d'une obligation de respect du secret professionnel[722]. De même, ces professionnels, en tant qu'agents publics, doivent respecter une obligation de confidentialité, de neutralité et de réserve[723]. Ces obligations sont bien entendu valables sur les réseaux sociaux également. La liberté d'expression sur les réseaux sociaux est donc permise, mais celle-ci doit s'exercer dans le respect du patient, de l'institution, de ses collègues et de sa profession. Ainsi la diffamation, l'injure ou encore le dénigrement vont venir limiter cette liberté d'expression. Dans ce contexte, le caractère public d'une information diffusée sur les réseaux sociaux va avoir son importance. En effet, alors que la diffamation publique est considérée comme un délit, punissable d'une amende de 12 000 euros, la diffamation privée est, quant à elle, une contravention punie d'une amende de 38 euros. Même chose pour l'injure qui sera plus durement réprimée si elle est publique (amende de 12 000 euros – article 33 de la loi du 29 juillet 1881[724]) que si elle est privée (contravention de première classe – article R. 621-2 du Code pénal). Dès lors, il est légitime de se demander ce qui peut bien être considéré comme "public" sur un réseau social. La jurisprudence nous apporte quelques réponses à ce sujet.

Ainsi, la Cour d'Appel de Lyon[725] a par exemple considéré qu'un licenciement était fondé sur une cause réelle et sérieuse pour un salarié qui, « *en n'activant pas les critères de confidentialité de son compte Facebook a pris le risque que ses propos, qu'il pensait privés soient accessibles à d'autres salariés de la société eux même titulaires d'un compte*

[722] Article L. 1110-4 du Code de la santé publique.
[723] *V.* notamment en ce sens, les dispositions de l'article L. 1110-4 du Code de la santé publique, mais également les dispositions de l'article 25 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires. Loi dite loi Le Pors. *JORF* du 14 juillet 1983, p 2174.
[724] Loi du 29 juillet 1881 sur la liberté de la presse, *JORF* du 30 juillet 1881, p. 4201.
[725] CA Lyon, ch. soc., sect. A, 24 mars 2014, n° 13/03463.

Facebook». Selon les juges, les propos, peu flatteurs, auraient excédé le droit à la liberté d'expression de leur auteur. En revanche, comme le précise la Cour administrative d'appel de Rouen, « *la seule existence de propos injurieux et calomnieux sur le réseau social ne suffit pas, en elle-même, à justifier du licenciement d'un salarié, il incombe à l'employeur de démontrer le caractère public des correspondances litigieuses* » [726]. Ainsi, l'employeur, qui souhaiterait sanctionner un agent pour des propos tenus sur un réseau social, devra d'abord établir le caractère public des propos.

La notion de liberté d'expression, confrontée aux obligations des professionnels de santé, et plus généralement, des fonctionnaires, doit donc également être prise en compte dans le cadre de la réflexion relative à l'encadrement des TIC en santé.

2) L'empilement législatif et règlementaire relatif aux TIC en santé

609. L'encadrement de l'innovation et, d'une manière générale des sciences et techniques par le droit, résulte de l'agrégation de plusieurs disciplines préexistantes (droit de la santé, de la propriété intellectuelle, de l'environnement) [727] et c'est là que réside toute la difficulté de ce type de matière. Les TIC en santé n'échappent pas à la règle.

610. Lors du congrès annuel de l'Association pour la promotion de la sécurité des SI en santé (Apssis), plusieurs participants ont pointé du doigt ce qu'ils ont qualifié de « *maquis réglementaire* »[728] des SI en santé. Si nous reprenons cette expression anecdotique, c'est parce qu'elle reflète bien, selon nous, l'état du cadre juridique actuel des SIS. En effet, la difficulté majeure résulte aujourd'hui du fait que l'utilisation des TIC en santé évolue dans deux cadres normatifs bien distincts : celui de l'informatique et des outils de communication, d'une part, et celui de la santé, d'autre part[729], ces deux domaines répondant à des contraintes spécifiques et très strictes. D'ailleurs Caroline ZORN-MACREZ déplorait au sujet de ces différents textes « *leur méthode d'élaboration au coup par coup conduisant à multiplier les antinomies*

[726] CA Rouen, 15 novembre 2011, n°11/01827.
[727] VERGES, Etienne. « L'évolution scientifique et technologique au prisme du droit : aperçu d'une relation à plusieurs facettes », *In* « Variations évolutions métamorphose », *PU St Etienne*, Institut universitaire de France, 2012, p. 371.
[728] Dépêche TIC Santé, « Le "maquis réglementaire" de la sécurité des SI en santé pointé du doigt », 7 avril 2016, disponible sur [http://www.ticsante.com]. Consultée le 1er septembre 2016.
[729] DEBOST, Claire. « L'appréhension juridique de la relation de soin au prisme des nouvelles technologies », *Jurisdoctoria*, n° 8, 2012, p. 104.

textuelles »[730]. Cependant, si l'on pousse la réflexion un peu plus loin, et au vu de notre étude, nous comprenons très vite que ces deux environnements normatifs sont, eux-mêmes, assez compliqués à appréhender, faisant parfois appel à d'autres branches du droit ou devant, tout du moins, tenir compte d'autres cadres juridiques.

611. Cet « *empilement législatif et réglementaire* », pour reprendre l'expression de Philippe BICLET[731], est aggravé par l'absence de perméabilité entre les différentes couches. Certains textes sont en effet adoptés sans prendre en considération ce qui aurait pu être prévu par ailleurs. De cela résulte à la fois des difficultés majeures d'interprétation mais également des difficultés dans la mise en place concrète des TIC en santé. La cartographie du cadre juridique actuel donne l'impression que le sujet n'a pas été traité réellement dans sa globalité mais bout par bout, selon les besoins des acteurs. Cette façon de procéder ne peut malheureusement que donner lieu à de nombreuses incohérences. Le constat sans appel qui avait été fait par Nicolas MOLFESSIS peut être repris ici et appliqué aux TIC en santé : « *une même situation juridique se trouve […] placée sous l'empire de diverses règles spéciales qui s'additionnent pour déterminer par agglutination […] le droit applicable* »[732].

612. Aujourd'hui, même si un corpus juridique relatif à l'utilisation des TIC en santé commence à se développer, « *cette réglementation éparse manque de cohérence et nuit à sa juste application par les professionnels de santé* »[733]. Par ailleurs, ce corpus n'est pas toujours en cohérence avec les différents textes généralistes applicables. Enfin, l'ensemble de cet encadrement juridique se construit sans concertation avec les principaux intéressés, à savoir les professionnels de santé. Ceux-ci se voient opposer de nouvelles contraintes, à la fois techniques et juridiques, qui parfois même ne répondent pas à leur besoin[734]. La difficulté actuelle est "l'entre-deux" dans lequel se situe le corpus juridique relatif aux TIC en santé. Il n'est pas encore abouti, puisque certaines situations sont encore peu ou pas encadrées, mais certaines mesures qui le composent sont suffisamment contraignantes pour freiner les évolutions technologiques ou les projets qui pourraient y être liés.

---

[730] ZORN-MACREZ, Caroline. « Chroniques martiennes des données de santé numérisées. Brèves observations sur une réglementation surréaliste », *RDS*, n° 36, juillet 2010, pp. 331-342.
[731] BICLET, Philippe. « Hébergement et échange des données de santé », *Médecine et droit*, 2010, p. 159.
[732] MOLFESSIS, Nicolas. « Combattre l'insécurité juridique ou la lutte contre du système juridique contre lui-même », *op. cit*., p 392.
[733] DEBOST Claire. « L'appréhension juridique de la relation de soin au prisme des nouvelles technologies », *op. cit*., p. 113.
[734] *Ibid.*

613. Finalement, nous pouvons légitimement nous poser la question de l'opportunité d'une intervention renforcée du législateur sur ce sujet. L'innovation et l'évolution constante qu'induit ce type de technologie nécessitent une certaine souplesse qu'un cadre juridique trop contraignant risquerait de freiner. De même, une superposition de textes épars conduit à une absence de lisibilité et d'efficacité de l'encadrement juridique.

Au-delà de cette problématique de lisibilité des textes, se pose également parfois la question des limites de leur applicabilité, certains d'entre eux prévoyant parfois des conditions strictes d'application, sans pour autant apporter les outils nécessaires à leur mise en œuvre.

B. Un cadre juridique source d'incertitudes

614. L'empilement des textes applicables s'avère souvent source de difficultés pour les acteurs et utilisateurs des TIC en santé. En effet, la question du texte applicable à l'espèce va se poser à plusieurs reprises, donnant parfois lieu à interprétations diverses et éventuelles prises de risques, notamment de la part des établissements dans la mise en œuvre de leurs projets. Mais l'insécurité juridique résulte également du fait que certains textes soient inaboutis, causant là encore des problèmes d'interprétation et de mise en œuvre. Tout cela concourt à créer une insécurité juridique dans le développement des TIC à l'hôpital.

615. En la matière, dispositions de droit commun et dispositions particulières cohabitent. Ainsi, le législateur a, nous l'avons vu, fait le choix d'encadrer de manière spécifique les modalités de conservation et d'échange de données de santé par voie informatique. Cependant, pendant longtemps, le législateur n'est pas allé au bout des choses, créant ainsi des situations intermédiaires au sein desquelles les règles étaient inabouties et donc difficilement applicables et opposables.

616. Cette affirmation est particulièrement vraie dans le cas des modalités d'application du décret dit "confidentialité". Comme nous avons pu le voir précédemment dans nos recherches[735] ce décret renvoyait, pour son application concrète, à des référentiels qui auraient

[735] *V. Supra.* n° 242 à 243.

dû être publiés par voie d'arrêtés, les établissements devant alors se mettre en conformité avec les dits arrêtés dans le délai d'un an suivant leurs publications. Or, ces arrêtés n'ont jamais été publiés. Face à la lenteur du pouvoir réglementaire, la question de la valeur de ce texte s'est rapidement posée. En effet, dans quelle mesure le décret confidentialité pouvait-il être considéré comme étant réellement applicable et donc opposable aux établissements de santé, à partir du moment où l'un des éléments essentiels à sa mise en œuvre n'a jamais été publié? Pour répondre à cette question, il nous semble intéressant de nous arrêter sur la notion de délai raisonnable, développé en droit administratif, et sur les actions qui auraient pu être menées à l'encontre de ce décret.

617. Très tôt, le Conseil d'Etat a reconnu que la responsabilité de l'État pouvait être engagée du fait de la non-intervention des décrets d'application dans un délai raisonnable[736]. Cependant, le juge étudie chaque cas où le non-respect d'un délai raisonnable serait invoqué auprès de lui, et il est nécessaire qu'un préjudice résultant du retard soit établi, « *le retard [n'étant] pas, en soi, un préjudice* »[737]. Ce principe ne s'applique pas seulement aux décrets qui devraient être pris en application d'une loi mais également aux arrêtés prévus par des décrets. Le Conseil d'Etat, dans une décision rendue le 29 juin 2011[738], a ainsi considéré que : « *l'exercice du pouvoir réglementaire comporte non seulement le droit mais aussi l'obligation de prendre dans un délai raisonnable les mesures qu'implique nécessairement l'application de la loi, hors le cas où le respect d'engagements internationaux de la France y ferait obstacle ; que lorsqu'un décret pris pour l'application d'une loi renvoie lui-même à un arrêté la détermination de certaines mesures nécessaires à cette application, cet arrêté doit également intervenir dans un délai raisonnable* ». La Haute juridiction peut d'ailleurs se montrer parfois très stricte, n'hésitant pas à enjoindre l'Etat, défaillant, de prendre les textes d'application attendus en assortissant sa décision d'une astreinte[739].

618. Il est vrai que cette notion de délai raisonnable ne repose sur aucun texte. Cependant, au fil des années, la notion a été développée et affinée, à la fois par le juge européen et par le Conseil d'Etat. Dans le cas du décret "confidentialité", les arrêtés nécessaires à la bonne

---

[736] CE, Ass. 27 novembre 1964, Veuve Renard, Rec. p. 590.
[737] ABIKHZER, Franck. « Le délai raisonnable dans le contentieux administratif : un fruit parvenu à maturité ? », *AJDA*, 2005, p. 985.
[738] CE, 29 juin 2011, Sté Cryo-Save France, n° 343188.
[739] *V*. notamment en ce sens : CE, 28 juillet 2000, Assoc. France Nature Environnement, n° 204024, Rec. 2000, p. 322 ; CE, 28 mars 1997, UNAF, n° 180943, Rec. 1997, p. 124.

application du texte n'avaient toujours pas été adoptés à la veille de la promulgation de la loi de modernisation de notre système de santé, soit presque 9 années après l'entrée en vigueur du texte. Bien que la jurisprudence étudie chaque cas de manière indépendante, il nous apparaît cependant qu'une durée de 9 ans aurait difficilement pu être considérée comme étant un délai raisonnable. Les établissements auraient d'ailleurs pu saisir le Ministre en charge de la santé d'une demande tendant à l'adoption de ces référentiels. Dans l'hypothèse d'une réponse négative, ou sans réponse de sa part dans un délai de deux mois, il leur aurait alors été possible de lui adresser ensuite un recours gracieux et, le cas échéant, déposer un recours pour excès de pouvoir auprès du Conseil d'Etat afin d'obtenir l'annulation du décret confidentialité. Pour autant, cela n'aurait pas été, selon nous, dans l'intérêt des établissements de santé. En effet, ceux-ci souhaitaient avant tout sécuriser leurs pratiques par l'adoption des référentiels.

619. Pendant longtemps, l'abrogation du texte a été envisagée, un nouveau texte étant supposément en cours d'élaboration[740]. Dans l'entre-temps, les professionnels n'avaient pas d'autre choix que de s'en référer aux référentiels de l'ASIP santé. Aujourd'hui, toutefois, la loi de modernisation de notre système de santé[741] a tenté de résoudre cette difficulté. Comme le précisaient les motifs de la loi, le but du législateur était d'harmoniser « *des règles de droit dans un domaine où l'évolution rapide de la législation a pu conduire à des écarts* ». Pour autant, il nous semble que les mêmes erreurs ont été commises.

En effet, l'article 96 de cette loi vient créer un article L. 1110-4-1 au Code de la santé publique qui dispose : « *afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces*

[740] SAMARCQ, Nicolas. BRIOIS, Sébastien. « Données de santé à caractère personnel : les enjeux de la diffusion des TIC », *Expertises*, 2010, p. 386.
[741] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte n° 1.

référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. »

620. L'obligation de se référer à des référentiels approuvés par arrêté ministériel n'est plus simplement règlementaire mais bien légale. Cette obligation acquiert donc un poids supplémentaire. Même s'il est vrai que les travaux de l'ASIP relatifs aux référentiels de sécurité et d'interopérabilité sont bien avancés, le risque que ces référentiels ne soient jamais opposables aux acteurs concernés reste le même. En effet, nous sommes, aujourd'hui encore, dans l'attente de publication d'un arrêté. Le législateur a gagné du temps, mais il va bien devoir agir dans un délai raisonnable.

Par ailleurs, il nous semble important d'attirer l'attention sur un décret pris en application de l'article 96 de la loi de modernisation de notre système de santé, et ses conséquences sur le décret confidentialité. En effet, le décret n° 2016-994 du 20 juillet 2016[742] vient modifier les articles R. 1110-1 à R. 1110-3 du Code de la santé publique, initialement issus du décret confidentialité. L'ancienne section I de la première partie, du livre 1er du titre premier du chapitre préliminaire de la partie règlementaire du Code de santé publique, précédemment intitulée « *confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique* » devient désormais « *Conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social* ».

Ainsi, l'ensemble des dispositions introduites par le décret confidentialité disparaissent purement et simplement. Ce décret, qui avait causé de nombreuses interrogations quant à ses modalités d'application, disparait donc de manière assez discrète.

.

[742] Décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel, *JORF* n°0169 du 22 juillet 2016, texte n° 21.

Conclusion de la section

621. L'appréhension du principe de sécurité juridique et de l'ensemble de ses corollaires nous permet d'effectuer une analyse critique sur le cadre actuel des TIC en santé, et de constater qu'il se révèle finalement vecteur d'insécurité juridique. Il est vrai que la construction de ce cadre est un défi de taille. Non seulement cela nécessite de faire appel à plusieurs branches du droit (droit civil, droit pénal, droit de la santé, droit de l'Internet), mais cela induit également de tenir compte des enjeux éthiques et économiques du domaine. Le législateur doit donc appréhender l'ensemble de ces contraintes dans leur globalité et prendre le recul nécessaire afin de construire un cadre cohérent, compréhensible et donc sécurisé.

Or, le cadre actuel n'est qu'une succession de textes épars, parfois contradictoires, ce qui rend complexe sa compréhension par les acteurs concernés. Par ailleurs, le cadre semble parfois inabouti, certains arrêtés pourtant essentiels n'ayant jamais été adoptés. Bien que la loi de modernisation de notre système de santé tente de corriger certaines de ces lacunes, le chemin vers un cadre plus lisible nous semble encore long.

Tout cela conduit à un cadre créateur d'incertitude et vecteur d'insécurités. Il nous semble donc aujourd'hui essentiel de le repenser.

Section 2. Un cadre juridique à repenser

622. Actuellement, le cadre juridique relatif aux TIC en santé peut paraitre difficilement accessible aux personnes qui y sont confrontées. Nous pensons ici plus particulièrement aux personnels de santé, mais également aux établissements de santé, parfois dépourvus face à la complexité des règles existantes. Il est donc nécessaire de repenser, si ce n'est entièrement, tout du moins en partie, le cadre des TIC en santé. En effet, il nous apparait clairement à ce stade de nos recherches que le cadre juridique actuellement en place constitue un réel frein au bon développement des TIC en santé (Paragraphe I). Le législateur doit donc réfléchir à un cadre innovant qui serait à la fois moteur et protecteur (Paragraphe II).

§1. Le cadre actuel, frein au développement pérenne des TIC à l'hôpital

« *La science avance plus vite que le droit et lui soumet de plus en plus souvent des situations inédites et embarrassantes* ».[743]

623. Souvent, l'innovation va plus vite que le droit, qui se contente de suivre et d'encadrer *a posteriori*. C'est le constat qui est régulièrement réalisé quand on aborde la question des liens entre droit, sciences, technique et innovation. Toutefois, quand on y regarde de plus près, cela n'est finalement pas aussi simple qu'il y parait. L'innovation scientifique et technique et le droit sont en réalité engagés dans une relation complexe, dont l'équilibre est souvent difficile à atteindre (A). C'est pourquoi il nous faut peut-être aujourd'hui nous éloigner de nos outils juridiques classiques, souvent contraignant, pour nous orienter vers les solutions plus originales et surtout plus flexibles, proposées par le droit souple (B).

A. L'encadrement juridique de l'innovation, un équilibre délicat

624. Comme le souligne Anne LAUDE, « *le dispositif juridique ne saurait être un frein à l'impérieuse nécessité d'innovation. Bien au contraire, il se doit d'être un outil*

[743] MATTEI, Jean-François. « Rapport au premier ministre sur l'éthique médicale », 1993.

d'encadrement au progrès scientifique »[744]. L'étude du lien entre sciences, technologies et droit n'est pas récente et déjà en 1966, David F. CAVERS[745] tentait de démontrer que le droit n'était pas qu'un « *instrument de prohibition et obstacle au développement de la connaissance et des innovations* »[746].

625. Médecine et Technologies de l'Information et de la Communication sont deux domaines où l'innovation est essentielle. Parfois, cependant, l'innovation n'est possible que par la transgression. Il est donc nécessaire de trouver un équilibre entre progrès et encadrement afin de maintenir une sécurité nécessaire pour les patients. Il est nécessaire de rechercher des « *compromis précaires entre les exigences juridiques et les nouvelles réalités techniques* »[747]. Car le développement des TIC ne fait pas que modifier les conditions dans lesquelles le droit va s'appliquer, elle crée de nouvelles situations, jamais appréhendées jusqu'alors par le droit, et auxquelles les règles existantes ne peuvent s'appliquer. Pour illustrer cela, Bertrand WARUSFEL cite, à juste titre, l'exemple du développement des bases de données et des droits qui peuvent y être afférents. Ainsi, il est rapidement apparu que l'application ou non de la protection issue du droit d'auteur à ces bases n'était pas une question qui pouvait se trancher aussi facilement. De là est né, au niveau européen, des règles propres à la structure et au contenu des bases de données, règles que nous avons par ailleurs exposées précédemment dans nos recherches et pris en exemple afin de tenter de qualifier le droit d'un établissement de santé sur le dossier patient[748].

626. Dans ses travaux consacrés au sujet, Etienne VERGES affirmait que « *d'une part, le droit est un outil de contrainte qui limite la liberté des chercheurs et qui fait obstacle au progrès scientifique. D'autre part l'évolution du droit est trop lente et ne parvient pas à suivre le rythme imposé par le progrès scientifique* »[749]. Bien que le législateur ait pu parfois

---

[744] LAUDE, Anne. « L'encadrement juridique de l'innovation », *Les tribunes de la santé*, 1/2004 (n°2), pp. 37-46.
[745] CAVERS, David. « Law and science, some points of confrontation », *in* « Law and the social role of science», *Rockefeller University Press*, 1966, p. 5.
[746] VERGES, Etienne. «L'évolution scientifique et technologique au prisme du droit : aperçu d'une relation à plusieurs facettes », *in* « Variation, évolutions, métamorphoses », *PU St Etienne*, Institut universitaire de France, 2012, p. 371.
[747] WARUSFEL, Bertrand. « Le droit des nouvelles technologies : entre technique et civilisation », La lettre de la rue Saint Guillaume, *Revue des Anciens élèves de Sciences-Po*, n° 127, juin 2002, pp. 52-59.
[748] *V. Supra*. n° 111 et s.
[749] VERGES, Etienne. «L'évolution scientifique et technologique au prisme du droit : aperçu d'une relation à plusieurs facettes », *op. cit.*, p. 371

intervenir tardivement dans certains domaines innovant - ce qui a d'ailleurs pu lui être reproché - pour autant, il a fait preuve d'une grande réactivité dans d'autres domaines. C'est notamment le cas d'Internet, domaine où le législateur a pris soin de rapidement adapter le droit commun à ce nouvel outil et, plus généralement, au développement des technologies du numérique.

Dans son étude, Etienne VERGES tente de démontrer les différents rôles du droit vis-à-vis de l'innovation scientifique et technologique. Ainsi, il apparait que le droit peut à la fois avoir un rôle d'encadrement mais également d'incitation, par le biais de politiques publiques allant en ce sens. Nous ajouterons à cela le rôle protecteur du droit vis-à-vis de l'innovation, rôle majeur qui ne doit pas être oublié.

627. Le cadre contraignant comporte plusieurs niveaux. En effet, il peut tout d'abord s'agir de l'interdiction pure et simple des activités (c'est le cas, par exemple, du clonage humain, interdit par les lois bioéthiques). Il existe également des régimes d'autorisation préalable ; ainsi, les protocoles de recherche impliquant la personne humaine ne peuvent être mis en œuvre sans l'avis préalable du comité de protection des personnes[750], qui va avoir pour rôle d'étudier les conditions dans lesquelles la sécurité des participants à l'essai sera assurée, mais également la pertinence du projet et de sa méthodologie. Il s'agit dans les deux cas d'une contrainte *a priori*, dans le but de sécuriser en amont les innovations scientifiques et technologiques. Mais le droit intervient aussi *a posteriori*, dans une optique de réparer les conséquences négatives du fait du développement des innovations. Il s'agit alors de mettre en œuvre la responsabilité des commettants afin de réparer les dommages qui seraient survenus. Pour Etienne VERGES, cette mise en œuvre de la responsabilité « *est essentielle dans une société technoscientifique dans laquelle le développement des innovations s'accompagne d'un risque incompressible. La responsabilité du fait d'une activité à risque, constitue le corollaire de la liberté d'exercice de l'activité scientifique et technologique.* »[751].

628. Cependant, il arrive que le cadre contraignant soit pointé du doigt par les industriels. Dans le cas de l'encadrement des TIC en santé, le Conseil National du Numérique (CNNum),

[750] Articles L. 1121-1 à L. 1126-11 du Code de la santé publique.
[751] VERGES, Etienne. «L'évolution scientifique et technologique au prisme du droit : aperçu d'une relation à plusieurs facettes », *op. cit.*, p. 371.

dans son étude de 2015 consacré au numérique en santé[752], préconise d'ailleurs d'adopter des *« procédures pragmatiques de régulation du marché de la santé connectée en phase avec les cycles courts de l'innovation »*[753]. Pour le CNNum, cela passe par un assouplissement du contrôle *a priori*, au bénéfice d'un renforcement du contrôle *a posteriori* et de la veille sanitaire. La flexibilité mais également un traitement rapide des dossiers (par le biais de « fast tracks » - guichets rapides) sont également essentiels. Effectivement, nous ne pouvons qu'adhérer à cette solution impliquant un droit plus pragmatique et plus réactif face aux cycles de l'innovation, particulièrement courts. Par ailleurs, actuellement, certaines procédures, par exemple en matière de protection des données de santé, peuvent être particulièrement longues et coûteuses, ce qui, comme le souligne l'étude du CNNum, peut s'avérer extrêmement pesant sur le modèle économique développée par les acteurs des TIC en santé. A terme, cela présente indubitablement des conséquences dommageables pour les petits industriels, moins compétitifs, et donc d'une manière générale pour les acteurs concernés, qu'ils s'agissent des professionnels ou des patients, se retrouvant face à un marché au choix restreint et peut être moins bien développé qu'il ne pourrait l'être par ailleurs.

629. A côté de ce cadre qualifié de contraignant, il existe également un cadre incitatif. En effet, le droit se révèle être parfois un outil au service de l'innovation. Certaines politiques publiques sont même très incitatives puisqu'elles participent directement au développement de la recherche et de l'innovation. Dans le domaine de la santé, nous pouvons citer à titre d'exemple les MERRI – Missions d'Enseignement, de Recherche, de Référence et d'Innovation – financements accordés dans le cadre de la tarification à l'activité et des Missions d'Intérêt Général d'Aide à la contractualisation (MIGAC) aux établissements de santé en fonction de leurs activités de recherche[754].

630. Plus généralement, le droit permet de créer les outils institutionnels nécessaires au bon développement de la recherche. C'est ainsi qu'est née en 2005 l'agence Nationale de la Recherche (ANR), agence dont la mission est de financer les projets de recherche. C'est elle qui pilote le plan d'Investissements d'avenir, et qui a par ailleurs géré l'appel à projets RHU

[752] CNNum, « La santé, bien commun de la société numérique », rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes, 2015.
[753] VERGES, Etienne. «L'évolution scientifique et technologique au prisme du droit : aperçu d'une relation à plusieurs facettes », *op. cit.* p 14.
[754] Article L. 162-22-13 du Code de la sécurité sociale.

(recherche hospitalo-universitaire) ayant abouti au soutien financier, à hauteur de 32,5 millions d'euros, de projets de recherche en santé présentant un fort potentiel de transfert rapide vers l'industrie ou vers la société[755].

631. Enfin, le droit est également un outil de protection de l'innovation, et plus particulièrement de ses résultats. En effet, une innovation, pour vivre et se développer, doit être protégée et valorisée. Le droit, au travers du droit de la propriété intellectuelle apporte une palette complète d'outils, destinés à protéger (brevet, droit d'auteur) et valoriser (contrats de cession ou de licence) les créations issues de l'innovation. Finalement, le droit permet de « *garantir la valeur économique des résultats scientifiques* »[756]

Innovation, sciences et droit sont au cœur d'une relation complexe, aux enjeux nombreux et parfois opposés. Cependant, loin d'être un ennemi de l'innovation, le droit l'accompagne, l'encadre et la facilite même parfois. Mais il faut pour cela réussir à trouver le juste équilibre, parfois précaire. Cet équilibre passe peut-être par une solution alternative aux outils normatifs tels qu'on les connait : le droit souple.

B. Le recours au droit souple, une solution à envisager

632. Souvent qualifié de droit mou (sans sanction), voire parfois de droit flou (sans précision) ou droit doux (sans obligation)[757], le droit souple a longtemps été déconsidéré par la grande majorité des juristes. En 2013 pourtant, le Conseil d'Etat a choisi d'en faire l'objet de son étude annuelle, vantant alors les mérites d'un droit qu'il avait vivement critiqué dans des études antérieures. Cette notion très actuelle n'est pourtant pas récente et il nous faut nous y attarder (1) avant de démontrer l'intérêt que le droit souple présente en matière d'encadrement des TIC en santé (2).

---

[755] Sur l'appel à projets RHU, *V*. notamment [http://www.agence-nationale-recherche.fr].
[756] VERGES, Etienne. «L'évolution scientifique et technologique au prisme du droit : aperçu d'une relation à plusieurs facettes », *op. cit.* p. 14.
[757] THIBIERGE Catherine. « Réflexion sur les textures du droit », *RDT Civ*, 2003, p. 599.

1) La notion de droit souple.

633. Depuis plusieurs années, nous assistons, que ce soit au niveau international, européen ou en droit interne, à un développement des instruments alternatifs à la loi et au règlement, qui, même s'ils n'ont pas de force contraignante vis-à-vis des personnes à qui ils s'adressent, leur permettent « *d'orienter leur comportement* ».

634. Utilisée de plus en plus couramment, la notion de droit souple pouvait faire référence à toute une panoplie de documents tels que les avis et recommandations d'AAI, les normes (du type norme ISO), les certifications, les labels ou encore les guides de bonne pratique. Cette notion a très vite attiré l'attention du Conseil d'Etat qui, alors qu'il l'avait critiqué dans ses rapports de 1991 et de 2006, a adopté dans son étude de 2013, une position quelque peu différente quant au droit souple, invoquant alors la complémentarité du droit souple avec les sources traditionnelles du droit, permettant ainsi de renforcer la qualité de ce dernier. Finalement, pour la Haute juridiction, « *parler de droit souple, c'est admettre qu'il s'agit de droit* »[758]. A cette occasion, la Haute juridiction a tenté de définir ce concept afin d'en délimiter les contours, proposant ainsi « *une échelle de normativité graduée, qui va du droit souple au droit dur* ».[759]. Pour le Conseil d'Etat, le droit souple serait donc composé de l'ensemble des instruments répondant à trois conditions cumulatives : ils ont pour objet de modifier ou orienter le comportement de leurs destinataires, ils ne créent pas, par eux-mêmes, des obligations et ils présentent par leur contenu ou leur mode d'élaboration un degré de formalisation et de structuration qui les apparentent aux règles de droit[760].

635. Dans leur étude, les magistrats du Conseil d'Etat relèvent quatre utilités au droit souple : la première concerne sa substitution au droit dur quand le recours à ce dernier n'est pas envisageable. La deuxième concerne l'appréhension des phénomènes émergents et notamment des évolutions technologiques : dans ce contexte, le droit souple constitue une étape préalable à l'utilisation du droit "dur" face à des phénomènes encore en mutation et qui nécessitent donc un cadre facilement évolutif. La troisième porte sur l'accompagnement de la mise en œuvre du droit dur par le droit souple, aux travers des chartes ou encore des

[758] Etude annuelle du Conseil d'Etat, « Le Droit souple », questions/réponses, 2013.
[759] RICHARD, Jacky. « Droit souple : pour une doctrine de recours et d'emploi », *Recueil Dalloz*, 2013, p. 2512.
[760] Etude annuelle du Conseil d'Etat, « Le Droit souple », 2013, p. 9.

démarches de conformité. Enfin, le dernier avantage réside dans l'alternative que constitue le droit souple au droit dur dans certains domaines où cette solution permet de concilier les besoins de régulation et les nécessités d'une certaine liberté.

636. Droit souple et droit dur sont séparés par une frontière finalement assez perméable, le droit souple pouvant être une étape avant d'arriver au droit dur ou pouvant même parfois être pris en compte par le juge[761]. Par ailleurs, le Conseil d'Etat parle même d'échelle de normativité graduée, s'affranchissant des théories de Kelsen pour affirmer qu'il existerait une continuité, sous forme de gradation, entre le droit dur et le droit souple. Cependant, le droit souple ne sera efficace que si son effectivité est assurée, c'est-à-dire s'il emporte l'adhésion des personnes auxquelles il s'adresse. C'est le cas s'il en vient à être considéré comme un standard, ou si sa violation emporte des conséquences négatives pour la personne qui ne le respecterait pas. Enfin, la légitimité de ces règles de droit souple repose en grande partie sur l'implication des acteurs dans son élaboration. L'étude du Conseil d'Etat sur le sujet a donc permis de répondre au besoin qui existait de « *mieux saisir une notion déjà fuyante, bien que d'apparition récente* »[762].

637. Depuis cette étude, le développement du droit souple et son utilisation n'ont cessé de croitre. Par ailleurs, le Conseil d'Etat admet même désormais[763] la possibilité de former un recours en excès de pouvoir contre des actes qui ne répondent pas aux critères classiques de la décision faisant grief, et qui s'apparentent plutôt à du droit souple[764]. Ainsi, à l'occasion de ses décisions *Société Fairvesta International GMBH* et *Société Numéricable*, l'Assemblée, après avoir rappelé que « *les avis, recommandations, mises en garde et prises de position adoptées par les autorités de régulation dans l'exercice des missions dont elles sont investies, peuvent être déférés au juge de l'excès de pouvoir lorsqu'ils revêtent le caractère de dispositions générales et impératives ou lorsqu'elles énoncent des prescriptions individuelles dont ces autorités pourraient ultérieurement censurer la méconnaissance* », est venue préciser que « *ces actes peuvent également faire l'objet d'un tel recours […] lorsqu'ils sont de nature*

[761] CE, 11 décembre 1970, n° 78880, *Crédit foncier de France*, Rec, p. 750 ; *DP*, 1971, 1224, note WALINE ; *JCP G* 1972, II, 17132, note FROMONT ; *AJDA* 1971, p. 196 ; *D*. 1971, p. 674, note LOSCHAK.
[762] DEUMIER, Pascale. « Saisir le droit souple par sa définition ou par ses effets », étude annuelle du Conseil d'Etat, 2013, p. 247.
[763] CE, Ass. 31 mars 2016, Société Fairvesta International GMBH, n° 368082, *AJDA*, 2016, p. 717 com. DUTHEILLET de LAMOTHE, Louis. ODINET, Guillaume.
[764] DUTHEILLET de LAMOTHE, Louis. ODINET, Guillaume. « Un recours souple pour le droit souple », *AJDA*, 2016, p. 717.

à produire des effets notables […] ou ont pour objet d'influer de manière significative sur les comportements des personnes auxquels ils s'adressent ». Le juge doit alors contrôler ces actes au même titre qu'il contrôle les décisions faisant grief. La Haute juridiction ne s'arrête pas là puisqu'elle est venue très récemment préciser le point de départ du délai de recours contre les actes de droit souple des autorités de régulation en le fixant à deux mois à compter de la mise en ligne de l'acte incriminé[765].

Le Conseil d'Etat poursuit donc la construction prétorienne relative à l'utilisation et à la place du droit souple, en faisant ainsi de ce droit un outil juridique à part entière, qui peut être une bonne alternative dans certains cas spécifiques, et notamment, selon nous, dans le cas de l'encadrement de l'utilisation des TIC en santé.

2) Le développement du droit souple pour encadrer les TIC en santé.

638. La médecine et les nouvelles technologies sont deux domaines en mutation permanente. Ainsi, leur encadrement, même s'il est indéniablement nécessaire, se doit d'être suffisamment souple et flexible pour s'adapter aux évolutions permanentes. Cependant, ces matières sont paradoxalement des matières où le droit applicable peut se révéler dans certains cas complexes et dans d'autres presque inexistants. Il est donc légitime de se demander si le droit souple, tel que défini par le Conseil d'Etat dans son étude de 2013, ne constituerait pas une alternative pertinente, permettant d'assurer un cadre juridique à l'utilisation des TIC en santé suffisamment souple pour un développement efficace et pérenne.

Plusieurs exemples viennent argumenter en ce sens. En effet, le législateur, qui s'était attelé à l'encadrement strict de l'hébergement des données de santé, quel qu'en soit leur support, semble aujourd'hui faire machine arrière face à l'ampleur de la tâche[766]. De même, l'encadrement très strict de la communication et de l'échange des données de santé informatisées, mise en place par le décret "confidentialité", est aujourd'hui inabouti, les différents arrêtés nécessaires à la mise en œuvre du décret n'ayant jamais été publiés[767]. Finalement, il apparaît que des outils plus souples que les textes juridiques "classiques"

[765] CE, 13 juillet 2016, Société GDF Suez, n° 388150; *JCP A*, 2016, 2252, note Olivier Le BOT.
[766] Article 204 de la loi n° n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, à propos de la mise en place d'une certification des hébergeurs de données de santé, à la place de leur agrément actuel.
[767] *V. Supra*. n° 242 à 243.

seraient peut-être plus adaptés à l'encadrement des TIC en santé. Le recours au droit souple doit donc être envisagé de manière sérieuse dans ce cas.

639. Argument fort en faveur d'une utilisation plus présente du droit souple dans le cas des TIC en santé : celui-ci est déjà très présent en droit médical comme en droit des nouvelles technologies. Ainsi, en matière médicale, les recommandations de bonnes pratiques (RBP), développées dans les années 1990, sont aujourd'hui très ancrées. A titre d'exemple, la Haute Autorité de Santé, créée en 2004, est en charge de l'élaboration de RBP dans le domaine sanitaire. Il en est de même pour l'Autorité Nationale de Sécurité du Médicament (ANSM), dans son domaine spécifique d'action. De leur côté, les sociétés savantes médicales produisent régulièrement de "guidelines", qui recueillent une très forte adhésion de la part des professionnels concernés.

640. Les RBP présentent l'avantage « *par leur normativité souple, de préserver à la fois la liberté de prescriptions des médecins et le droit pour le patient d'être soigné selon les données acquises de la science* »[768]. Pourtant, la question de la nature juridique de ces RBP s'est posée très rapidement et le juge a apporté certaines précisions à leur sujet. La Haute juridiction avait déjà eu l'occasion de préciser que les RBP en matière médicale constituaient des instruments d'aide à la décision pour les praticiens, mais également pour le juge[769]. Dans le cadre de son arrêt *Conseil National de l'Ordre des Médecins*[770], le juge administratif va plus loin et considère que certaines RBP sont susceptibles de recours pour excès de pouvoir à partir du moment où elles sont rédigées sur le mode impératif. En l'espèce, le Ministre de la santé avait refusé de retirer un arrêté portant homologation de RBP émises par l'ancienne agence nationale d'accréditation et d'évaluation en santé (aujourd'hui la Haute Autorité de Santé). Ces RBP avaient été prises sur la base de l'article L. 1111-9 du Code de la santé publique, qui précisait alors que « *un décret en Conseil d'Etat fixe les conditions d'application du présent chapitre. Les modalités d'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès, font l'objet de recommandations de bonnes pratiques établies par l'Agence nationale d'accréditation et d'évaluation en santé et homologuées par arrêté du ministre chargé de la santé.* »

---

[768] KRZICH, Delphine. « Force normative et efficacité des recommandations de bonne pratique en matière médicale », *RDSS*, 2014, p. 1087.
[769] *V*. en ce sens, CE, 12 janvier 2005, n° 25600.
[770] CE, 26 septembre 2005, n° 270234, *Conseil National de l'Ordre des Médecins*, Rec, 2005, p. 395.

Pour le Conseil d'Etat, ces RBP, «*qui visent normalement à donner aux professionnels et établissements de santé des indications et orientations pour l'application des dispositions législatives et réglementaires relatives à l'accès des patients aux informations médicales, n'ont pas en principe, même après leur homologation par le ministre chargé de la santé, le caractère de décision faisant grief, elles doivent toutefois être regardées comme ayant un tel caractère, tout comme le refus de les retirer, lorsqu'elles sont rédigées de façon impérative* »[771]. Ainsi, ces RPB qui, par leur caractère impératif, viennent modifier l'ordonnancement juridique, constituent des actes faisant grief susceptibles de recours en excès de pouvoir. Il nous est possible de faire un parallèle ici avec la jurisprudence *Duvignères*[772] du Conseil d'Etat, qui venait faire la distinction entre circulaires impératives et circulaires interprétatives[773]

641. Le Conseil d'Etat a par la suite confirmé sa jurisprudence à plusieurs reprises. En 2011 d'abord, à l'occasion de l'arrêt *Formindep*[774] où il vient préciser que les recommandations de bonnes pratiques élaborées par la Haute Autorité de Santé sur la base de dispositions légales, « *ont pour objet de guider les professionnels de santé dans la définition et la mise en œuvre des stratégies de soins à visée préventive, diagnostique ou thérapeutique les plus appropriées, sur la base des connaissances médicales avérées à la date de leur édiction* » ; il poursuit en en précisant « *qu'eu égard à l'obligation déontologique, incombant aux professionnels de santé […] d'assurer au patient des soins fondés sur les données acquises de la science, telles qu'elles ressortent notamment de ces recommandations de bonnes pratiques, ces dernières doivent être regardées comme des décisions faisant grief susceptibles de faire l'objet d'un recours pour excès de pouvoir* ». De même, en 2013, le Conseil d'Etat adopte une position similaire vis-à-vis des RBP adressées par l'AFSSAPS (aujourd'hui ANSM)[775]. Il apparaît donc clairement que, progressivement, les RPB, prennent une place majeure dans le domaine du droit médical.

---

[771] CE, 26 septembre 2005, *op. cit.*
[772] CE, 18 décembre 2002, Mme Duvignères, n° 233618, Rec., 2002, p. 463, concl. P. FOMBEUR ; *Dr. adm.*, 2003, comm. 73 et repère 3 ; *Procédures*, 2003, n° 154, note S. DEYGAS ; *AJDA*, 2003, p. 487, chron. F. DONNAT et D. CASAS.
[773] MARKUS, Jean-Paul. « Nature juridique des recommandations de bonnes pratiques médicales », *AJDA*, 2006, p 308.
[774] CE, 27 avril 2011, Association pour une formation médicale indépendante, n°334396, JurisData n° 2011-007009.
[775] CE, 4 octobre 2013, Sté Laboratoires Servier, n° 356700.

642. Du côté des TIC, le droit souple est également très prisé. En effet, il s'avère être un outil particulièrement adapté à un domaine où les évolutions sont constantes. Ainsi, les acteurs privés de ce domaine s'engagent dans la conception de normes afin de gérer leurs relations. Ces normes « *se distinguent également par leur origine extra étatique et la négociation qui conduit à leur élaboration* »[776]. Le domaine des TIC voit alors se développer les chartes et les autres guides de bonnes pratiques.

Aujourd'hui, nous pouvons donc facilement imaginer que ces outils puissent également être utilisés en matière de TIC en santé. D'ailleurs, les établissements de santé, face aux lacunes du cadre actuel, et afin de sécuriser leurs pratiques, construisent leurs propres chartes et règlements intérieurs en matière de systèmes d'information hospitaliers. Le but de ces textes est d'organiser le bon usage des TIC dans le cadre notamment du traitement des données de santé mais également de la prise en charge des patients.

[776] SARR, Minata. « Droit souple et commerce électronique », Jurisdoctoria, 2012, n°8, p. 52.

§2. Le législateur sur la voie de la modernisation du cadre juridique

643. Que ce soit au niveau national ou au niveau européen, le législateur cherche à adapter les règles en place afin de sécuriser les pratiques liées à l'utilisation des TIC en santé. Il a en effet eu l'occasion de constater à de multiples reprises la nécessité de rénover le cadre en place, aujourd'hui devenu trop complexe et inadapté aux nouvelles pratiques et technologies qui se développent rapidement.

Alors que le législateur français a souhaité corriger certains dysfonctionnements qui pouvaient devenir pesant (B), le législateur européen, pour sa part, s'est concentré sur un sujet qui lui est cher depuis de nombreuses années : celui de la protection des données à caractère personnel (A).

A. Une volonté européenne d'unifier la protection des données personnelles

644. A l'issue d'une procédure législative particulièrement fastidieuse (1), le Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données[777] a enfin été adopté. Il apporte de nombreuses modifications, notamment en terme de droits des personnes concernées par un traitement de données à caractère personnel, mais aussi au sujet des procédures et obligations préalables à la mise en œuvre d'un traitement automatisé de données à caractère personnel (2).

1) Une procédure législative longue et délicate.

645. Adopté le 27 avril 2016, à l'issue d'un trilogue entre le Conseil de l'Union européenne, la Commission européenne et le Parlement européen, le règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, entrera en vigueur le 25 mai 2018. Ce règlement voit enfin le jour après quatre longues années de discussions et de négociations.

[777] 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* n° L 119 du 4 mai 2016, p. 1.

Initialement en effet, le projet de règlement avait été adopté en Commission européenne le 25 janvier 2012, dans le but de rénover le cadre juridique applicable, issu de la directive 95/46/CE du 24 octobre 1995, texte devenu quelque peu obsolète face à l'augmentation de l'utilisation de l'outil informatique et plus spécifiquement de l'Internet. En effet, selon plusieurs études du Groupe de l'article 29[778], la directive de 1995 soulevait certaines difficultés d'interprétation.

Alors que l'outil utilisé en 1995 était la directive, nécessitant ainsi une transposition par chacun des Etats membres dans son droit interne, la réforme est, quant, à elle, basée sur un autre outil juridique : le règlement. Celui-ci présente en effet l'avantage de créer les mêmes règles applicables dans tous les Etats membres et donc en ce sens de diminuer les différences qui peuvent exister entre les Etats. Cela a pour conséquence de réduire la marge de manœuvre que pourraient avoir les Etats avec une directive, et qui permettrait d'adapter certains éléments à leur droit interne.

646. Le processus législatif s'est avéré long et laborieux[779]. Bien évidemment les enjeux économiques ont été une des causes majeures de la longueur de la procédure, dont l'issue était initialement annoncée pour 2014. Comme le précise le règlement dans ses considérants, « *le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité* ». Le texte s'est donc attaché à trouver le juste équilibre entre protection des données et de la vie privée, liberté d'expression et enjeux économiques. Pour certains auteurs, l'objectif prioritaire de ce texte est bien de construire un marché unique numérique[780].

Par ailleurs, comme le souligne à juste titre Céline CASTETS-RENARD dans son analyse du Règlement[781], une autre difficulté majeure rencontrée par le législateur européen a été de trouver l'équilibre entre la volonté d'uniformiser le cadre relatif à la protection des données personnelles en Europe, en choisissant l'outil du règlement et d'autre part, la possibilité pour chaque Etat d'articuler ces nouvelles normes avec celles déjà existantes dans

---

[778] *V*. Notamment en ce sens avis n° 8/2010, 16 déc. 2010, WP 179 ; avis n° 5/2009, 12 juin 2009, WP 163.

[779] Alors que le projet adopté en janvier 2012 a été soumis à discussions au sein du Conseil de l'Union européenne le 7 décembre 2012, celles-ci se sont terminées en mars 2014 et le Parlement n'a été saisi du projet que le 12 mars 2014, le trilogue entre le Conseil, le Parlement et la Commission ne débutant qu'en avril 2016.

[780] CASTETS-RENARD, Céline. « Brève analyse du règlement général relatif à la protection des données personnes », *Dalloz IP/IT*, 2016, p. 331.

[781] *Ibid.*

sa législation interne. Ainsi, il est important de souligner que le Règlement, initialement outil contraignant, laisse ici une marge de manœuvre importante aux Etats membres puisqu'il prévoit que certains points du texte pourront donc être précisés par chaque Etat membre.

2) La mise en place d'un cadre rénové

647. Sans revenir sur l'intégralité du texte, il est important d'en souligner les points principaux, qui représentent, selon nous, les avancées majeures dans la protection des données à caractère personnel. Le Règlement s'attache, en premier lieu, à définir deux notions essentielles : d'une part, celle de données personnelles en son article 4.1 et, d'autre part, celle de consentement. Ainsi, les données personnelles sont *« toute information se rapportant à une personne physique identifiée ou identifiable […] est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

648. Le consentement quant à lui est défini comme étant « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Passé cet exercice de définition, il s'attache ensuite à instaurer un cadre rénové de la protection des données à caractère personnel au sein de l'Union européenne.

a) Le renforcement du droit des personnes

Avec ce nouveau Règlement, les droits des personnes dont les données à caractère personnel font l'objet d'un traitement sont renforcés.

649. Il nous semble intéressant de nous attarder d'abord sur le droit au consentement. De manière assez classique, le règlement reprend l'obligation, pour la personne concernée par un traitement de données à caractère personnel, d'y consentir de manière libre et explicite (article 7 du Règlement), à défaut, le traitement ne sera pas, en principe, licite (article 6 du

Règlement). Mais la nouveauté apportée par le Règlement réside dans la possibilité pour la personne, de retirer son consentement. En effet à tout moment, il est possible de revenir sur le consentement accordé en vue d'un traitement de données à caractère personnel. Bien entendu, et en cela, le texte est bien fait, le règlement prévoit expressément que le retrait n'est valable que pour l'avenir et ne remet aucunement en question la licéité du traitement, initialement fondé sur le consentement préalable. Cependant, le législateur européen ajoute une mention quelque peu surprenante puisqu'il conclut cette disposition par la phrase suivante : « *il est aussi simple de retirer que de donner son consentement* ». Peut-être qu'avec cette formulation le législateur européen a entendu appuyer sur la facilité qui doit être accordée à la personne de revenir sur son accord. Notons que la formule, bien qu'elle nous surprenne, a le mérite d'avoir évolué par rapport celle de la proposition de règlement dans sa version de 2014 puisqu'il était initialement prévu qu' « *il devrait être aussi simple de retirer son consentement que de le donner* ». Cette formulation, qui relevait plus du vœu pieu que d'une réelle obligation légale, aurait pu être source de difficultés[782], puisqu'elle n'aurait fait peser qu'une simple obligation de moyens sur le responsable du traitement. Pour conclure sur le consentement, notons que le Règlement maintient une série d'exceptions à son recueil. Ces exceptions[783] sont les mêmes que celles prévues par la loi Informatique et Libertés.

De plus, le Règlement laisse une marche de manœuvre aux Etats membres sur ce point puisqu'ils pourraient « *maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement* ». En d'autres termes, cette liste d'exception n'est pas limitative et elle pourra être augmentée par chacun des Etats membres, selon ses besoins.

---

[782] BOIZARD, Maryline. « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », *Communication commerce électronique*, n° 3, mars 2016, étude 6.

[783] L'article 6 du Règlement européen prévoit que « *le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:*
a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;
d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ».

650. Le Règlement consacre son chapitre III aux droits des personnes concernées par un traitement. De manière assez classique par rapport à la législation actuelle, le règlement débute par le rappel de l'obligation d'informer la personne préalablement à la mise en œuvre du traitement de manière claire, intelligible et facilement accessible. Finalement, le texte fait du responsable du traitement le débiteur d'une obligation de transparence renforcée vis-à-vis des personnes concernées. A noter que les droits d'accès et de rectification sont maintenus.

651. Mais le texte innove également puisqu'il vient créer de nouveaux droits. Ainsi, les personnes concernées par un traitement de données à caractère personnel pourront désormais obtenir la limitation de leur traitement. Ce droit, assez original, suspend l'utilisation des données collectées par le responsable du traitement (le temps d'obtenir la rectification de données inexactes ou encore si le responsable n'a plus besoin des données mais qu'elles sont nécessaires à la personne concernées pour faire valoir ses droits par exemple), qui continue néanmoins à en assurer la conservation.

De même, le droit à l'oubli (appelé droit à l'effacement), qui était déjà en partie consacré par la loi Informatique et Liberté en son article 40, est rappelé par le règlement, qui prévoit de nouveaux cas d'applicabilité. Désormais, la personne pourra obtenir l'effacement de ses données si celles-ci ne sont plus nécessaires à la finalité du traitement ou, comme nous l'avons vu, si elle décide de retirer son consentement. La personne concernée par un traitement de données à caractère personnel bénéficie également d'un droit à la portabilité de ses données, c'est-à-dire le droit d'obtenir du responsable du traitement l'ensemble des données qui la concerne dans un format structuré.

Corollaire direct des droits, la possibilité d'obtenir réparation du fait de la violation de ceux-ci est également prévue par le Règlement, en son chapitre VIII. Ainsi, « *toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable de traitement ou du sous-traitant réparation du préjudice subi* » (article 82 du règlement). Par ailleurs, une réclamation à l'encontre d'un responsable de traitement défaillant peut être formulée par voie de recours administratif juridictionnel ou auprès de l'autorité de contrôle. Une action juridictionnelle peut être par ailleurs déposée à l'encontre d'une autorité de contrôle.

b) Un nouveau cadre de contrôle et de sanction

«Réorganisation et documentation : ce sont les maîtres mots qu'il faut retenir du Règlement général sur la protection des données n° 2016/679 »[784]

652. Point majeur de ce règlement, celui-ci vient créer le délégué à la protection des données (Data Protection Officer – DPO). Ainsi, sa désignation est obligatoire pour toutes les entreprises du secteur public quelle que soit la nature des traitements réalisés. Les établissements de santé qui ne s'étaient pas encore dotés d'un correspondant informatique et libertés (CIL) vont donc devoir d'ici mai 2018, se mettre à la recherche d'un DPO. Le Règlement fixe une liste de ce que devront être, *a minima*, les missions de ce nouvel acteur. Si certaines sont similaires à celle de notre actuel CIL, de nouvelles missions apparaissent cependant. Il s'agit du contrôle des règles internes de l'entreprise en matière de protection des données à caractère personnel, une mission de conseil et de vérification de l'exécution des analyses d'impact devant être réalisées par l'entreprise et, enfin, une mission de coopération et de contact avec l'autorité de contact (ce qui , même si la loi Informatique et Libertés ne le prévoit pas, était déjà le cas des CIL en grande majorité).

Le DPO dispose, bien entendu, d'une indépendance dans l'exercice de ses missions et ne rend des comptes qu'au niveau le plus élevé de la hiérarchie de l'entreprise. En cela, rien de nouveau par rapport au CIL.

653. Dans chaque Etat membre, une autorité de contrôle indépendante doit être mise en place afin de contrôler la bonne application du Règlement, mais également protéger les droits des personnes[785]. Finalement sur ce point, la France est en avance puisque la CNIL est en place depuis de nombreuses années. Ses missions, et peut-être ses moyens, devront cependant être adaptés au nouveau Règlement. Nous ne nous attarderons donc pas sur ces dispositions. En termes de sanctions, un nouveau régime d'amende, plus dur, est mis en place. L'article 83 de Règlement vient poser le cadre général permettant aux autorités de contrôle de sanctionner les responsables de traitement défaillants. Les amendes pourront s'élever jusqu'à 10 000 000 euros ou 2% du chiffre d'affaires annuel mondial dans certains cas (en cas de violation des conditions relatives au consentement des enfants par exemple) ou dans d'autres cas jusqu'à

---

[784] BOURGEOIS, Matthieu. BOUNEDJOUM, Amira. « Réforme européenne des données personnelles : registres internes et DPO, la nécessaire réorganisation des entreprises », *JCP Entreprises et Affaires*, n° 22, juin 2016, p. 1326.
[785] Chapitre VI du Règlement.

20 000 000 euros ou 4% du chiffre d'affaires annuel mondial, en cas d'illicéité du traitement notamment. Par ailleurs, pour tous les cas qui ne seraient pas réglés par l'article 83 du Règlement, l'article 84 prévoit la possibilité, pour chaque Etat membre, de prévoir d'autres mesures d'amendes.

654. Malgré ce durcissement, nous nous interrogeons sur la pertinence de ces amendes. Bien sûr, le texte prévoit une amende maximale, modulable par l'autorité de contrôle compétente. Malheureusement, comme nous avions déjà pu le constater[786], les amendes excessives ne sont jamais prononcées et finissent par ne plus être dissuasives.

C) Des nouvelles formalités

655. Autre point essentiel de ce Règlement, la modification des formalités préalables à la mise en œuvre d'un traitement de données. Le responsable du traitement doit désormais mettre en place un registre des activités du traitement. Ce registre s'impose à toutes les entreprises avec un aménagement pour les entreprises de moins de 250 employés. Le responsable de traitement et son sous-traitant sont tous deux en charge de la tenue de ce registre. Autre nouveauté non négligeable : la nécessité dans certains cas de réaliser une analyse d'impact relative à la protection des données. C'est en effet le cas lorsqu'un traitement est susceptible d'engendrer un risque trop élevé pour les droits et libertés des personnes physiques. Cela concerne notamment les traitements de profilage sur la base duquel des décisions juridiques peuvent être prises ; la surveillance systématique à grande échelle d'une zone accessible au public ou les traitements à grande échelle de données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ainsi que les données génétiques et biométriques. Cependant, le Règlement n'apporte pas plus de précisions et laisse aux autorités de contrôle de chaque Etat membre le soin de publier une liste des types d'opération de traitement pour lesquelles une analyse d'impact sera nécessaire. Dans l'hypothèse où l'analyse d'impact réalisée démontre que le traitement envisagé présente un risque élevé pour le respect du droit des personnes, le responsable du traitement doit se rapprocher de l'autorité de contrôle.

[786] *V. Supra*. n° 91.

Ainsi, le législateur européen a travaillé à la rénovation du cadre relatif à la protection des données à caractère personnel. En France, le législateur s'est attelé quant à lui, à différents chantiers.

B. Une volonté française de moderniser le cadre applicable

656. Le législateur français tente de moderniser le cadre juridique de l'utilisation des TIC en santé. Cela passe, sur le long terme, par un important travail d'encadrement du numérique d'une manière générale (2), et à plus court terme, par un chantier de correction de certains dysfonctionnements (1).

1) La loi de modernisation de notre système de santé, patch correctif de certains dysfonctionnements

657. La loi de modernisation de notre système de santé[787] adoptée, le 26 janvier 2016, contient plusieurs dispositions relatives à l'utilisation des TIC en santé. Certaines font partie intégrante de la loi et d'autres ont été adoptées par voie d'ordonnance[788]. Pourtant, force est de constater que certaines de ces mesures, pourtant réellement impactantes, sont passées presque inaperçues. Elles n'ont fait l'objet d'aucun commentaire de la part de la doctrine, celle-ci préférant se focaliser sur les mesures phares de la loi telles que les GHT ou la refonte du service public hospitalier.

Pourtant, le législateur a entendu, à travers cette loi, simplifier ou uniformiser certaines dispositions applicables aux TIC en santé devenues trop complexes.

658. Bien entendu, la refonte du DMP est une des mesures principales relatives aux TIC en santé et présente dans ce texte. Plus qu'un simple "patch correctif"[789], les mesures prévues par

[787] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n°0022 du 27 janvier 2016, texte 1.
[788] Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, *JORF* n°0011 du 13 janvier 2017, texte n° 17 ; 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, *JORF* n°0011 du 13 janvier 2017, texte n° 21.
[789] Nous utilisons volontairement cette expressément tirée de l'informatique. Dans ce cadre, un patch désigne un morceau de Code apportant un correctif à un programme.

l'article 96 de la loi de modernisation de notre système de santé et son décret d'application[790] représentent, selon nous, l'ultime tentative du législateur de sauver ce projet ambitieux dont on ne compte plus les échecs depuis plus de 10 ans. Mais l'article 96 vient également transformer le consentement du patient, nécessaire préalablement à tout hébergement externalisé de données de santé auprès d'un hébergeur agréé, en simple non opposition. Il résout ainsi certaines difficultés pratiques régulièrement rencontrées par les professionnels.

659. Les mesures les plus discrètes, mais pour autant importantes, se situent au sein du titre V de la loi, consacré aux mesures de simplification. Ainsi, l'article 204 de la loi prévoit la possibilité pour le Gouvernement de venir, « *dans les conditions prévues à l'article 38 de la Constitution et dans un délai de douze mois à compter de la promulgation de la présente loi […] prendre par ordonnances les mesures d'amélioration et de simplification du système de santé relevant du domaine de la loi* ». Par ce biais, le Gouvernement a pu poser, par voie d'ordonnance, certaines règles en matière d'hébergement de données de santé[791]. Les dispositions en matière d'agrément des hébergeurs de données de santé prévues au Code de la santé publique ont été harmonisées avec celles relatives à l'agrément des personnes dépositaires d'archives publiques, telles que prévues à l'article L. 212-4 du Code du patrimoine. Cette disposition démontre bien la volonté du législateur d'appréhender ce type de problématique dans sa globalité. Par ailleurs, et nous l'avons étudié en détail précédemment, la procédure d'agrément est largement simplifiée et la certification remplacera la procédure du comité d'agrément des hébergeurs.

Enfin, par voie d'ordonnance[792], le Gouvernement a apporté une solution à la problématique concrète que rencontrent tous les établissements de santé aujourd'hui, à savoir créer les modalités de destruction des dossier médicaux papiers qui ont été numérisés.

2) La loi pour une République numérique

a) Les travaux préalables du Conseil d'Etat

[790] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, *JORF* n°0155 du 5 juillet 2016
[791] *Ibid.*
[792] 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, *JORF* n°0011 du 13 janvier 2017, texte n° 21.

660. En 2014, le Conseil d'Etat avait consacré son étude annuelle[793] au numérique et aux droits fondamentaux. Ce choix qui constituait, selon le Conseil d'Etat, une audace de sa part, était pourtant apparu comme évident, notamment car l'essor du numérique dans notre société avait forcément des conséquences sur les droits fondamentaux des personnes. Le Conseil d'Etat se devait donc de revêtir son rôle de gardien des droits et libertés fondamentaux. A l'occasion de cette étude, la Haute juridiction a donc constaté que non seulement le numérique a permis d'obtenir la reconnaissance de nouveaux droits fondamentaux autonomes tels que le droit à la protection des données personnelles et le droit d'accès à Internet, mais il a également bouleversé le régime juridique de certaines libertés fondamentales. En effet, à l'heure de l'Internet les moyens classiques de protection de la liberté d'expression et de la vie privée ont pu être mis à mal. La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[794] a permis de stabiliser le régime relatif à la liberté d'expression[795], mais les questions relatives aux limites de la liberté d'expression restent vives. En soi, ce n'est pas tant la question des limites à apporter à la liberté d'expression qui se pose mais plutôt les moyens pour lutter contre les contenus illicites, normalement interdits. Pour le Conseil d'Etat, il était donc nécessaire de repenser la protection des droits fondamentaux face à l'essor du numérique.

661. Cette protection n'est possible que par une responsabilisation accrue des utilisateurs. Cette notion revient, comme nous avons pu le constater, très régulièrement. En accordant plus de moyens d'actions en cas de violation de leurs droits, mais également, en leur accordant une plus grande maîtrise de leurs données personnelles, les utilisateurs des outils numériques pourraient se protéger plus facilement. D'ailleurs, à l'occasion de cette étude, le Conseil d'Etat a avancé la possibilité de consacrer un droit à l'autodétermination informelle de l'individu, plutôt que celui d'un droit à la propriété, estimant qu'il convenait d'écarter ce qu'il a qualifié de logique patrimoniale dans la protection des données.

662. Face à ces différents constats, le Conseil d'Etat avait formulé cinquante propositions, tendant notamment à l'amélioration de la définition des droits fondamentaux à l'ère du

---

[793] Conseil d'Etat, étude annuelle, « Le numérique et les droits fondamentaux », 2014, *La documentation française*.
[794] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, *JORF* n°0143 du 22 juin 2004, p. 11168.
[795] Conseil d'Etat, étude annuelle « Le numérique et les droits fondamentaux », dossier de presse, 2014, p. 5.

numérique, au renforcement des pouvoirs des individus vis-à-vis de leurs données, à la redéfinition des moyens de protection des droits fondamentaux et du rôle des autorités publiques et à l'organisation de la coopération européenne et internationale.

663. En parallèle de cette étude très instructive sur l'impact du numérique sur les droits fondamentaux, le Conseil national du numérique a mené, entre octobre 2014 et février 2015, une concertation qui a permis au Gouvernement d'élaborer sa stratégie numérique. Le 9 décembre 2015, le projet de loi pour une République Numérique a été adopté en conseil des Ministres. Enfin, la loi pour une République Numérique a été adoptée le 7 octobre 2016[796].

b) Les enjeux de la loi

664. La loi, issue d'une vaste concertation nationale en ligne[797], se décompose en trois axes : "la circulation des données et du savoir", "la protection des droits dans la société numérique" et "l'accès au numérique". Les motifs du projet de loi précisent bien que l'objectif du Gouvernement, avec ce projet est double : *« d'une part, donner une longueur d'avance à la France dans le domaine du numérique en favorisant une politique d'ouverture des données et des connaissances ; d'autre part, adopter une approche progressiste du numérique, qui s'appuie sur les individus, pour renforcer leur pouvoir d'agir et leurs droits dans le monde numérique* »[798].

665. A travers ce texte, le législateur entend, d'une part, favoriser l'innovation liée au numérique, par des leviers incitatifs, et, d'autre part, encadrer en amont cette innovation et assurer la protection des individus. Cette loi présente l'ambition d'encadrer, dans sa globalité, le développement du numérique en France. Il est vrai que la loi pour une République Numérique tente de toucher toutes les sphères du droit concernées par le numérique. Qualifiée de "polymorphe"[799], la République numérique touche effectivement au droit public, au droit

---

[796] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n°0235 du 8 octobre 2016, texte n°1.

[797] Selon le communiqué de presse du Conseil des Ministres en date du 9 décembre 2015, « *En seulement trois semaines, près de 21 000 participants ont publié 8 500 contributions. A l'issue de cet exercice, le Gouvernement a retenu cinq nouveaux articles d'inspiration citoyenne dans son projet et a intégré près de 90 modifications du projet* », disponible sur [http://www.gouvernement.fr]. Consulté le 31 août 2016. Cependant, cette notion de « co-écriture citoyenne » avancée par le Gouvernement est parfois critiquée. *V.* notamment en ce sens PASTOR, Jean-Marc. « Les politiques publiques dans la république numérique », *Dalloz actualités*, 19 décembre 2015.

[798] Exposé des motifs de la loi, disponible sur [https://www.legifrance.gouv.fr]. Consulté le 19 mars 2017.

[799] DALEAU, Jeanne. « République numérique : après la consultation publique, la discussion parlementaire », *Dalloz actualités*, 28 janvier 2016

des affaires mais également au droit de la consommation, au droit de la propriété intellectuelle et au droit pénal. Certaines des dispositions prévues par le texte méritent d'ailleurs que nous nous y attardions.

666. Dans le cadre de l'axe relatif à l'incitation à la circulation des données, le gouvernement propose, bien évidemment, d'élargir l'ouverture des données publiques en France. L'Open Data est effectivement un enjeu primordial à l'heure du développement du numérique. Le premier titre prévoit ainsi la mise en ligne obligatoire sur le site Internet des administrations, des documents administratifs librement communicables. Mais le point qui attire le plus notre attention est l'introduction de la notion de données d'intérêt général afin de permettre, notamment, un accès simplifié aux statistiques publiques.

667. En ce qui concerne le renforcement de la protection dans la société numérique, nous pouvons constater que certaines propositions issues de l'étude annuelle du Conseil d'Etat ont été reprises. En effet, de nouveaux droits sont créés et notamment le droit à la libre disposition de ses données par un individu (l'autodétermination informelle). L'exposé des motifs de la loi précise d'ailleurs que la piste de la création d'un droit de propriété sur les données personnelles n'est pas retenue, notamment car « *la valeur des données personnelles d'un individu est très limitée, de l'ordre de quelques centimes d'euros* »[800]. Cet argument très pragmatique finira certainement de convaincre les personnes qui militaient encore pour ce droit et qui n'avaient peut-être pas encore intégrés pleinement les risques qui existent à reconnaitre un droit de propriété des personnes sur leurs données personnelles.

668. Par ailleurs, la loi introduit également le droit à la portabilité des données, en totale redondance avec le Règlement européen relatif à la protection des données adopté en avril 2016, tout comme l'est l'ensemble de dispositions venant modifier la loi Informatique et Libertés. Il aurait été préférable que le législateur ne crée pas un doublon avec le Règlement européen. Même si celui-ci n'entrera en vigueur, au plus tard, qu'en mai 2018, il aurait été souhaitable d'éviter de créer, encore une fois, une superposition de textes portant sur le même sujet, au risque de créer des dispositions divergentes.

---

[800] Exposé des motifs du projet de loi pour une République numérique, à propos de l'article 26, disponible sur [https://www.legifrance.gouv.fr]. Consulté le 31 août 2016.

Si cette loi a le mérite de s'emparer d'un sujet complexe à encadrer, quelques erreurs sont déjà présentes et il aurait été préférable d'inscrire ce texte dans la ligne directe des mesures prises au niveau européen, et notamment celles contenues dans le Règlement européen, afin d'éviter de rendre illisible le cadre juridique.

Conclusion de la section

669. Le cadre juridique des TIC en santé doit être rénové, cela est incontestable. Il est vrai qu'il peut parfois être compliqué de trouver le bon équilibre entre le droit, souvent vu comme un outil contraignant, et l'innovation technologique, rapide et nécessitant une grande liberté. Pourtant, quand cet équilibre est atteint, droit et innovation sont alors des alliés de taille, le droit permettant à l'innovation de se développer au sein d'un cadre à la fois protecteur pour les usagers mais aussi incitatif et valorisant pour les chercheurs. Cependant, la flexibilité nécessaire doit être recherchée dans des outils juridiques un peu moins classiques. Le droit souple apparait alors comme constituant une solution adaptée. En matière de TIC en santé, cela est d'autant plus vrai que les deux domaines concernés, à savoir la médecine et les technologies de communication, utilisent déjà depuis longtemps les outils issus du droit souple.

670. Bien qu'ils ne semblent pas explorer cette piste pour l'instant, le législateur européen et le législateur français se sont toutefois tous deux attelés à la modernisation du cadre juridique des TIC en santé, chacun dans des domaines différents. Le législateur européen rénove ainsi le travail qu'il avait réalisé en 1995 en matière de protection des données à caractère personnel, tandis que le législateur français tente de réparer certains dysfonctionnements présents depuis longtemps. Il fait aussi preuve d'initiative à travers la loi relative à la République Numérique. Il marque ainsi sa volonté d'accompagner le développement des TIC, dans leur globalité, en remplissant à la fois un rôle protecteur (en édictant de nouveaux droits fondamentaux) mais également incitateur (en tentant de rendre accessible à tous les outils du numérique).

Il faut toutefois qu'il veille à garder un rythme soutenu en la matière s'il ne veut pas être très vite dépassé. De même, il doit apprendre de ses erreurs, et veiller à ne pas être de nouveau redondant avec d'autres textes, au risque de complexifier encore plus le cadre juridique.

Conclusion du chapitre

671. Le cadre juridique de l'utilisation des TIC à l'hôpital, construit au fur et à mesure, n'est qu'une succession de textes épars et parfois inaboutis qui, mis bout à bout, ne forment absolument pas un ensemble cohérent. A l'heure actuelle, ce cadre juridique ne remplit pas correctement son rôle, en étant source d'une certaine insécurité juridique. Pour lutter efficacement contre cela, il est nécessaire de limiter l'inflation législative. Le législateur doit se montrer plus rigoureux dans l'élaboration des normes, en tâchant de privilégier la qualité de celles-ci, plutôt que leur quantité. La rénovation de ce cadre semble donc inéluctable.

Pour cela, il nous apparait indispensable que le droit s'adapte aux exigences des innovations technologiques. Réactivité, inventivité et souplesse doivent donc être les maîtres-mots de ce nouveau cadre juridique. Le législateur devra peut-être s'orienter vers les solutions proposées par le droit souple qui, longtemps critiqué, apparait aujourd'hui pour beaucoup (et notamment par le Conseil d'Etat) comme une alternative efficace pour encadrer certains domaines nécessitant une forte flexibilité. En cela, cette solution semble être adaptée pour venir, en partie, constituer le cadre juridique des TIC en santé. Enfin, soulignons que le législateur européen et le législateur français se préoccupent d'ores et déjà de moderniser le cadre juridique des TIC en santé. Le règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données propose un encadrement global rénové du traitement des données à caractère personnel. Les TIC en santé, nécessitant la collecte et le traitement de données de santé seront donc directement impactées par cette réforme. Le législateur français, quant à lui, a profité de la loi de modernisation de notre système de santé pour glisser quelques nouveautés et surtout quelques simplifications en ce qui concerne la conservation et l'échange de données de santé. Par ailleurs, la loi pour une République numérique ambitionne de venir reconnaitre de nouveaux droits fondamentaux, issus directement du développement des TIC. Pour autant, ceci n'est que le début d'un chantier bien plus grand. De nombreuses incohérences subsistent et de nouvelles technologies développées dans le secteur de la santé doivent être appréhendées par le droit. Le chemin est donc encore long.

Dans l'attente, les établissements de santé ne restent pas sans réagir. Ils sont en effet venus compenser les lacunes du législateur, en tentant de se réguler eux-mêmes afin de

proposer des solutions technologiques innovantes à leurs professionnels et leurs patients, tout en s'assurant que les droits de ces derniers seront respectés.

Conclusion du titre

672. Le bon développement des SIS en France a besoin d'une gouvernance efficace. Pour que des projets d'ampleur, nécessitant une ligne de conduite nationale unifiée (tel que le DMP par exemple) puissent aboutir, il est en effet nécessaire que l'Etat prennent les choses en main et instaure le cadre de conduite propice à leur bon développement. Les pouvoirs publics s'y attèlent et la gouvernance rénovée, en place depuis 2009, a le mérite d'être plus lisible pour les différents acteurs. La gouvernance et la conduite des projets de SIS ne peuvent reposer seulement sur l'échelon national et, ainsi, au niveau régional, les ARS et les GHT représentent les appuis essentiels pour les établissements de santé.

Pour réussir à sécuriser l'utilisation des TIC dans la pratique médicale, les pouvoirs publics doivent également réfléchir à la refonte du cadre juridique actuel. En effet, l'influence de sources de droit extérieure, l'apparition de nouveaux domaines complexes et protéiformes (tel que les TIC en santé) ou encore la propension du gouvernement à légiférer de manière médiatique, dégradent de plus en plus la qualité de nos normes. Aujourd'hui, la complexité entourant les TIC en santé posent une difficulté majeure pour établir un cadre lisible et compréhensible par tous les acteurs. A la décharge du législateur, il est vrai que les enjeux entourant les TIC en santé sont nombreux et variés. Il faut adopter une vision globale de la matière, en prenant en compte les contraintes juridiques, bien évidemment, mais également les contraintes éthiques, économiques et techniques. Une réforme s'impose donc afin de pouvoir apporter aux établissements l'environnement juridique clair dont ils ont besoin.

Néanmoins, la sécurisation de l'utilisation des TIC dans la pratique médicale peut être amorcée par les établissements eux-mêmes, plus à même d'identifier leurs besoins en la matière. En accompagnant l'informatisation de leurs pratiques par une réflexion portant sur la sécurisation de ces dernières, les établissements sont ainsi assuré d'un développement serein et sûr de l'utilisation des TIC.

TITRE 2

LES ETABLISSEMENTS DE SANTE, ACTEURS CLES DE LA SECURISATION DE L'UTILISATION DES TIC A L'HÔPITAL

673. Comme le pointait à juste titre la Cour des Comptes dans son étude de 2016 consacrée à la modernisation des systèmes d'information hospitaliers, « *loin de s'atténuer, la complexité des processus d'informatisation des hôpitaux a plutôt tendance à s'accroitre* »[801]. Les établissements de santé, pour relever le défi de l'informatisation, doivent faire face à une problématique multiple : non seulement ils doivent s'assurer d'installer un système d'information hospitalier qui soit à la fois efficient et adapté aux besoins des professionnels pour leur pratique quotidienne, mais ils doivent également veiller à ce que ce système d'information respecte la législation en vigueur en matière d'utilisation des TIC, de traitement des données à caractère sensible et de droits des usagers. Trouver ce juste équilibre n'est pas toujours aisé pour les établissements de santé qui doivent agir dans un cadre financier et juridique contraint, ce dernier étant parfois, comme nous le constatons depuis le début de nos recherches, fluctuant et difficile à appréhender. Dans ce contexte particulier, les établissements de santé vont pouvoir jouer un rôle essentiel dans la sécurisation de leurs pratiques, compensant ainsi les lacunes du législateur et des pouvoirs publics en la matière.

Ainsi, les établissements disposent de plusieurs outils permettant d'encadrer au mieux leur démarche d'informatisation, les plaçant ainsi au cœur de la sécurisation de leurs pratiques (chapitre premier). Le CHRU de Lille est d'ailleurs un exemple de sécurisation réussie, qui mérite que nous nous y attardions (chapitre second).

[801] Cour des Comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, septembre 2016, p. 330.

Chapitre 1

Les établissements de santé, au cœur de la sécurisation de leurs pratiques

674. Le développement des systèmes d'information hospitaliers se révèle être un chantier long et jonché d'embuches. A titre d'exemple, le CHU de ROUEN, suite à un incident lors du déploiement de la prescription informatisée au sein de son système d'information, a dû revenir de manière transitoire au papier[802]. Aujourd'hui, force est de constater que les établissements de santé ne sont pas tous égaux en termes de développement de leur système d'information hospitalier. Alors que certains peinent à déployer leur dossier patient informatisé (AP-HP, CHU de Rouen)[803], d'autres ont eu l'occasion de développer, avec succès, une solution interne, qu'ils peuvent désormais diffuser au sein d'autres établissements (Hospices civils de Lyon)[804].

675. Ces différences en termes d'avancée ont des sources multiples. Ainsi, il arrive parfois, comme le souligne la Cour des Comptes que « *des dérives de délais, de coûts et de qualité se cumulent* »[805]. Cependant, les établissements de santé ne sont pas totalement démunis face à ce défi de taille qu'est le développement de leur système d'information hospitalier. Ainsi, ils vont pouvoir être les acteurs directs de la sécurisation de leurs pratiques.

En amont d'abord, puisqu'ils vont pouvoir inscrire le développement et la mise en place de leur système d'information hospitalier dans une démarche stratégique, leur permettant ainsi d'anticiper le mieux possible les difficultés et les risques liés à l'informatisation des pratiques médicales (Section I). Puis, en aval, une fois le système d'information hospitalier mis en place, les établissements vont pouvoir user d'outils juridiques et managériaux afin d'anticiper certains risques et sanctionner des pratiques incorrectes (Section II). Dans la pratique, bien évidemment, ces différentes solutions se superposent et devront être mises en œuvre simultanément.

---

[802] *Id.*, p. 337.
[803] *Id.*, p. 353.
[804] *Id.*, p. 353.
[805] *Id.*, p. 339.

Section 1. Les pistes de sécurisation a priori

676. La mise en œuvre et le développement des TIC dans la pratique médicale doit être réfléchie en amont par les établissements de santé. Les risques liés à l'utilisation des TIC, qu'ils soient d'ordre juridique ou technique, peuvent être anticipés et les pratiques peuvent, dès leur origine, être sécurisées. Ainsi, la mise en place d'une stratégie d'établissement autour du développement du système d'information hospitalier est une condition essentielle à une utilisation sereine des TIC (Paragraphe I). Par ailleurs, les établissements de santé peuvent également faire appel à des experts dans le domaine, qui sauront les guider et les accompagner dans la mise en place de leur système d'information hospitalier (Paragraphe II).

§1. La gestion stratégique de l'informatisation à l'hôpital

677. L'ensemble des applications informatiques utilisées à l'hôpital, qu'il s'agisse des logiciels médicaux ou des simples logiciels administratifs (gestion de la paie par exemple, ou de la facturation), s'organise dans le cadre précis du Système d'Information Hospitalier (SIH). Il nous est nécessaire de définir ce concept de SIH (A), avant de réfléchir aux modalités permettant de gérer de manière stratégique son développement (B).

A. Le Système d'information hospitalier

1) Bref rappel historique

678. Le système d'information hospitalier tel qu'il existe aujourd'hui au sein des établissements de santé a mis du temps à se développer. Ce sont les fonctions purement administratives qui, dans un premier temps, ont été informatisées. Ainsi, certaines fonctions ayant trait à la gestion des ressources humaines (la paie notamment) mais également les fonctions financières (la facturation ou encore la comptabilité) ont été informatisées, par le biais notamment d'application développées au niveau national[806].

[806] ANAP, « Audit des systèmes d'information hospitaliers auprès d'établissements représentatifs », rapport final, mars 2014, p. 13.

679. En 1972, le statut des syndicats inter-hospitaliers est créé[807]. Ce type de coopération se développe alors afin de mutualiser les efforts et les moyens en matière d'informatique hospitalière. Les centres Régionaux de l'Informatique Hospitalière (CRIH) apparaissent à la même époque. Il s'agit de structures publiques qui *« sont en charge d'assurer le développement, la maintenance et l'exploitation de l'informatique hospitalière »*[808]. Ce sont les CRIH qui, dans un premier temps, vont développer et proposer des solutions logicielles aux établissements de santé. Cependant, à partir de 1989, le marché va s'ouvrir aux industriels du secteur privé.

680. Par ailleurs, en 1982, la création du Programme de Médicalisation des Systèmes d'Information (PMSI) va renforcer la nécessité pour les établissements, de s'informatiser de manière fiable afin de recueillir les données relatives à l'activité médicale et les transmettre aux autorités compétentes. En effet, le nouveau mode de financement de l'activité, à savoir le budget global, introduit par Jean de KERVASDOUE (alors Directeur des Hôpitaux)[809], impose aux établissements de santé de valoriser au mieux leur activité, en tenant un relevé le plus précis possible de celle-ci. Ce ne sont toutefois que les prémisses du PMSI, qui sera généralisé en 1995[810].

681. Puis, après le développement de l'offre informatique relative au secteur médico-technique (biologie et imagerie) entre 1990 et 2000, c'est la production de soins qui va commencer à être informatisée à partir de 2000. Cette informatisation ne trouve cependant pas sa source dans une volonté d'améliorer la prise en charge ou d'informatiser de manière intensive la pratique médicale. La justification est purement médico-économique. En effet avec la loi de financement pour 2004 apparait la tarification à l'activité[811] : désormais, les ressources des établissements de santé dépendent de leur activité. Le développement de l'informatique et notamment de l'informatique médicale devient alors, aux yeux des

---

[807] Décret n°72-353 du 2 mai 1972 relatif à la création des syndicats inter-hospitaliers et à leurs conseils d'administration, *JORF* du 4 mai 1972, p. 4605.
[808] ANAP, « Audit des systèmes d'information hospitaliers auprès d'établissements représentatifs », *op. cit.*, p. 13.
[809] Ancien nom de l'actuelle Direction Générale de l'Offre de Soins (DGOS).
[810] Arrêté du 20 septembre 1994 relatif au recueil et au traitement des données d'activité médicale et de coût, visées à l'article L. 710-5 du Code de la santé publique, par les établissements de santé publics et privés visés aux articles L. 714-1, L. 715-5 du Code de la santé publique et aux articles L. 162-23, L. 162-23-1 et L. 162-25 du Code de la Sécurité Sociale et à la transmission aux services de l'État et aux organismes d'assurance maladie d'informations issues de ces traitements, *JORF* n° 242, 18 octobre 1994, p. 14761.
[811] Loi n° 2003-1199 du 18 décembre 2003 de financement de la sécurité sociale pour 2004, *JORF* n°293, 19 décembre 2003, p. 21641.

établissements de santé, un véritable enjeu stratégique. Les établissements de santé, aidés et motivés par le plan hôpital 2007, vont donc se lancer dans l'informatisation de la production de soins de manière accélérée.

Par ailleurs, et comme nous l'avons vu précédemment, les politiques nationales incitatives vont se développer, poussant les établissements de santé à développer leur système d'information hospitalier.

2) Tentative de définition de la notion de système d'information hospitalier

La notion de "système d'information hospitalier" peut, à première vue, paraître assez vague. Pour comprendre les enjeux mais également les difficultés liées à sa mise en place ainsi qu'à sa sécurisation, il est donc nécessaire de tenter d'en définir les contours.

682. La circulaire du 6 janvier 1989 relative à l'informatisation des hôpitaux publics[812] précise que le système d'information hospitalier peut être défini comme « *l'ensemble des informations, de leurs règles de circulation et de traitement nécessaires à son fonctionnement quotidien, à ses modes de gestion et d'évaluation ainsi qu'à son processus de décision stratégique* ». Dans son audit des systèmes d'information hospitaliers, publié en mars 2014[813], l'ANAP revient sur la définition d'un système d'information hospitalier. Ainsi, le rapport précise que le système d'information hospitalier, qui ne peut se réduire au seul système informatique, « *est la combinaison d'organisations avec les Technologies de l'Information et de la Communication* »[814]. A l'appui de cette définition, le rapport cite l'auteur R. De COURCY, pour lequel « *un système d'information (SI) est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de collecter, regrouper classifier, traiter et diffuser de l'information dans un environnement donné* »[815].

683. D'un point de vue strictement technique, un SIH va se construire à partir de briques fonctionnelles: les pro-logiciels. Ces briques sont ensuite assemblées les unes aux autres,

[812] Circulaire n° 275 du 6 janvier 1989 relative à l'informatisation des hôpitaux publics, non parue au *JORF*.
[813] ANAP, « Audit des systèmes d'information hospitaliers auprès d'établissements représentatifs », rapport final, mars 2014.
[814] *Id.*, p. 11.
[815] *Ibid.*, citant DE COURCY (R.), Les systèmes d'information en réadaptation, Québec, Réseau international CIDIH et facteurs environnementaux, 1992, n° 5, vol. 1-2, p. 7-10.

chacune étant classée au sein d'un domaine fonctionnel. Le rapport de l'ANAP tente, avec succès selon nous, de schématiser l'organisation en briques fonctionnelles d'un SIH type[816]. Ainsi, au sein d'un SIH, nous pouvons retrouver, en termes de domaines fonctionnels le pilotage médico-économique, la production de soins cliniques, la production de soins medico-technique et les fonctions support. Au sein même de ces domaines seront développées des briques fonctionnelles. Toute la difficulté réside dans l'assemblage de ces briques fonctionnelles entre elles. En effet, le système d'information hospitalier, comme on peut le constater, va être composé de plusieurs centaines de logiciels différents. Or, ces briques, associées les unes aux autres ne forment que rarement un ensemble cohérent. L'interopérabilité encore inexistante des différentes solutions logicielles est une cause de cette difficulté. Toutefois, cette difficulté résulte également de la considération portée aux SIH par les directeurs d'établissement. En effet, leur vision actuelle des SIH est encore trop peu stratégique.

B. Une gestion stratégique indispensable

Progressivement, les directions d'établissement ont pris conscience des enjeux qui entouraient le système d'information hospitalier. D'abord considéré comme un simple sujet technique, le SIH devient, peu à peu, un sujet stratégique. Malgré tout, tous les établissements de santé n'ont pas à ce jour, développé une réelle stratégie autour de leur système d'information.

684. Dans son étude de 2014, l'ANAP observe que « *si des progrès sont notables, du chemin reste encore à parcourir pour que le SIH trouve définitivement sa place au sein de la stratégie de l'établissement* »[817]. Pour illustrer ses propos, l'ANAP avance le fait qu'aujourd'hui encore, le fonctionnement du SIH et ses possibles évolutions ne sont pas pris en compte dans l'élaboration du projet médical d'établissement. Or, à une époque où la pratique médicale s'informatise, il est évident que les projets médicaux doivent s'appuyer, en partie, sur l'expertise des directions des systèmes d'information (DSI).

[816] Ce schéma est repris en annexe de nos travaux, annexe I.
[817] ANAP, « Audit des systèmes d'information hospitaliers auprès d'établissements représentatifs », *op. cit.*, p. 23.

685. Le constat réalisé par la Cour des Comptes à l'occasion de son étude nationale de 2016 consacrée aux systèmes d'information hospitaliers[818] est un peu plus nuancé. En effet, pour la Cour des Comptes, « *les 41 établissements de l'enquête se sont dotés d'une stratégie informatique* »[819]. La Cour souligne toutefois que « *ce pilotage stratégique associe encore insuffisamment l'utilisateur* »[820]. Autrement dit, les outils développés dans le cadre du SIH ne sont pas toujours présentés en amont aux principaux utilisateurs, ce qui peut se révéler parfois très bloquant à l'issue d'un projet.

Il apparaît alors essentiel pour les établissements de « *penser les systèmes d'information comme un outil au service de la stratégie de l'établissement, assurer la stabilité des stratégies informatiques dans la durée, capitaliser sur une première expérience d'informatisation, maîtriser la conduite de projet, associer en continu les utilisateurs, anticiper les risques et intégrer dès la conception du projet les gains d'efficience recherchés* »[821]

Dans son rapport, l'ANAP identifie quatre déterminants au bon développement des SIH au sein des établissements de santé.

686. En premier lieu, l'ANAP considère que « *la maturité de la stratégie doit se traduire par une intégration systématique du sujet SIH dans l'ensemble des projets de l'établissement* »[822]. En effet, le SIH ne doit plus être un simple outil servant la mise en œuvre de projets internes, mais bien un projet à part entière. Une culture du SIH doit être distillée au sein de l'établissement, et auprès de l'ensemble des personnels. Pour cela, l'établissement de santé doit donc d'abord élaborer une stratégie autour du développement de son SIH,

---

[818] Cour des Comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », Rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, *op. cit.*

[819] *Id.*, p. 333.

[820] *Ibid.*

[821] Rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », Cour des Comptes, septembre 2016, p. 360.

[822] ANAP, « Audit des systèmes d'information hospitaliers auprès d'établissements représentatifs », *op. cit.*, p. 35.

composée d'un schéma directeur des systèmes d'information (SDSI)[823], dont la mise en œuvre sera supervisée par un comité stratégique.

687. Mais la stratégie n'est pas le seul déterminant au succès du développement d'un SIH. Il faut également que les professionnels soient associés à ce développement de manière active. Par exemple, les groupes de travail doivent être composés de professionnels de terrain, bien évidemment intéressés par l'informatique. Ce sont ces professionnels qui feront le lien entre la Direction des Systèmes d'Information et les utilisateurs.

688. La maturité des logiciels et de l'interopérabilité est le troisième déterminant au bon développement des SIH, selon l'ANAP. En effet, le SIH est composé de nombreuses briques fonctionnelles et de plusieurs centaines de logiciels. Il est donc plus que nécessaire de réfléchir en termes d'urbanisation du SIH afin que le système construit soit cohérent, fonctionnel et surtout communiquant.

689. Enfin, le dernier déterminant concerne la méthode développée pour mettre en place le SIH. Il est nécessaire que la gestion de projet soit rigoureuse et prenne notamment le temps d'identifier les impacts de l'informatisation, cadrer et prioriser les projets, donner un rythme au déploiement et ne pas oublier de mettre en place une démarche de conduite du changement. En effet, trop souvent les établissements de santé ont considéré que c'était à l'informatique de s'adapter aux pratiques. Or, aujourd'hui, il est nécessaire que les pratiques évoluent grâce à l'informatique. Il est donc essentiel pour cela que les organisations actuelles s'adaptent et intègrent pleinement l'informatique. L'établissement de santé devra donc veiller à l'accompagnement managérial de l'informatisation.

[823] Le rapport de la Cour des Comptes précise, à ce propos, que la plupart des établissements de son enquête disposaient d'un tel schéma.

§ 2. L'appui sur des ressources qualifiées

690. Le développement d'un SIH nécessite de hautes connaissances techniques. Les directeurs des établissements de santé doivent donc s'entourer des compétences nécessaires afin de mener à bien l'informatisation des fonctions administratives et médicales de leurs établissements.

Les établissements peuvent alors faire le choix de recruter des experts informatiques afin de les intégrer directement à leurs équipes (A). Ils peuvent également faire appel, sous certaines conditions, à de sociétés extérieures, qui pourront alors les accompagner dans leur démarche de développement du SIH (B). D'une manière générale, les établissements s'appuient sur ces deux possibilités afin de renforcer l'expertise relative aux SIH en leur sein.

A. Le recrutement de compétences spécialisées

691. Les établissements de santé, dans le cadre de la mise en place de leur stratégie informatique, doivent s'entourer d'experts. Cependant, le recrutement de compétences spécialisées, et notamment d'ingénieurs informatiques, reste un défi de taille pour les établissements de santé. A ce sujet, la Cour des Comptes observe, dans son rapport de septembre 2016[824], que certains établissements tels que l'AP-HP, le CHU de Saint Etienne, ou encore le Groupe hospitalier public du sud de l'Oise ont rencontré de réelles difficultés à assurer de tels recrutements, les amenant à se détacher des statuts de la fonction publique hospitalière[825].

692. Il est vrai que les statuts de la fonction publique hospitalière peuvent parfois être un obstacle au recrutement de personnel hautement spécialisé. Pour comprendre les raisons de ces difficultés, il nous faut nous pencher sur les règles applicables au sein de la fonction publique hospitalière en matière de recrutement du personnel.

---

[824] Cour des Comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », Rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, *op. cit.*
[825] *Id.*, p. 334.

Le principe, qui est par ailleurs le même au sein de toutes les fonctions publiques, est celui du recrutement de personnel titulaire de la fonction publique. En effet, l'article 3 de la loi Le Pors[826] dispose que : « *sauf dérogation prévue par une disposition législative, les emplois civils permanents de l'Etat, des régions, des départements, des communes et de leurs établissements publics à caractère administratif sont, à l'exception de ceux réservés aux magistrats de l'ordre judiciaire et aux fonctionnaires des assemblées parlementaires, occupés soit par des fonctionnaires régis par le présent titre, soit par des fonctionnaires des assemblées parlementaires, des magistrats de l'ordre judiciaire ou des militaires dans les conditions prévues par leur statut* ».

693. Le législateur a cependant prévu quelques exceptions permettant, dans certains cas, aux établissements publics de santé de faire appel à des agents recrutés par voie contractuelle. Ainsi, l'article 9-1 de la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière[827] prévoit que : « *les établissements peuvent recruter des agents contractuels pour assurer le remplacement momentané de fonctionnaires ou d'agents contractuels autorisés à exercer leurs fonctions à temps partiel ou indisponibles […] Le contrat est conclu pour une durée déterminée. Il est renouvelable, par décision expresse, dans la limite de la durée de l'absence de l'agent à remplacer*. ». L'article poursuit en précisant que : « *pour les besoins de continuité du service, des agents contractuels peuvent être recrutés pour faire face à une vacance temporaire d'emploi dans l'attente du recrutement d'un fonctionnaire* ». Enfin, « *les établissements peuvent recruter des agents contractuels pour faire face à un accroissement temporaire d'activité, lorsque celui-ci ne peut être assuré par des fonctionnaires* ». L'article 9 de cette même loi dispose quant à lui que : « *par dérogation à l'article 3 du titre Ier du statut général, les emplois permanents mentionnés au premier alinéa de l'article 2 peuvent être occupés par des agents contractuels lorsque la nature des fonctions ou les besoins du service le justifient, notamment lorsqu'il n'existe pas de corps de fonctionnaires hospitaliers susceptibles d'assurer ces fonctions ou lorsqu'il s'agit de fonctions nouvellement prises en charge par l'administration ou nécessitant des connaissances techniques hautement spécialisées* ». Ainsi, les établissements de santé peuvent recruter par voie contractuelle des ingénieurs informatiques qualifiés, à partir du moment où

[826] Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires. Loi dite loi Le Pors. *JORF* du 14 juillet 1983, p. 2174.
[827] Loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière, *JORF* du 11 janvier 1986, p. 535.

ils justifient que la nature des fonctions qui seront exercées nécessite des connaissances techniques hautement spécialisées.

694. Cependant, l'autre difficulté rencontrée par les établissements de santé dans le cadre du recrutement concerne la rémunération des agents. En effet, par principe, les agents titulaires de la fonction publique ont droit à « *une rémunération comprenant le traitement, l'indemnité de résidence, le supplément familial de traitement ainsi que les indemnités instituées par un texte législatif ou réglementaire. Les indemnités peuvent tenir compte des fonctions et des résultats professionnels des agents ainsi que des résultats collectifs des services. S'y ajoutent les prestations familiales obligatoires* »[828]. Ainsi, en ce qui concerne les agents qui seraient titulaires de la fonction publique, l'établissement de santé n'a pas de marge de manœuvre et devra, en termes de rémunération, s'en tenir aux dispositions statutaires.

695. Pour les contractuels en revanche, les établissements vont pouvoir se permettre d'accorder des rémunérations supérieures à celles prévues par les grilles statutaires. En effet, l'article 1-2 du décret n° 91-155 du 6 février 1991[829] prévoit la chose suivante : *« Le montant de la rémunération est fixé par l'autorité administrative, en prenant en compte, notamment, les fonctions occupées, la qualification requise pour leur exercice, la qualification détenue par l'agent ainsi que son expérience* ». La rémunération peut donc, pour les agents contractuels, être fixée contractuellement, et elle est laissée, en théorie, à la libre appréciation de l'autorité administrative. Toutefois, la jurisprudence est venue apporter un bémol à ce principe. Ainsi, pour rémunérer un agent contractuel, un employeur public se doit de prendre en compte la rémunération des agents titulaires exerçant des fonctions équivalentes, ainsi que le niveau de diplôme et l'expérience professionnelle des autres agents contractuels qui exercent des fonctions équivalentes[830].

696. Par ailleurs, la liberté d'action de l'employeur public en matière d'octroi d'une prime à un agent contractuel a été soumise à questionnement. Le Conseil d'Etat, dans une décision en date du 23 mars 2009, précise que les agents contractuels de la fonction publique hospitalière

---

[828] Article 20 de la loi Le Pors.
[829] Décret n° 91-155 du 6 février 1991 relatif aux dispositions générales applicables aux agents contractuels des établissements mentionnés à l'article 2 de la loi n° 86-33 du 9 janvier 1986 modifiée portant dispositions statutaires relatives à la fonction publique hospitalière, *JORF* n° 35, 9 février 1991, p. 2058.
[830] CAA Marseille, 9 avril 2013, n°11MA00840.

ne pouvaient se voir octroyer le bénéfice de la prime de service.[831] S'est alors posée la question de l'attribution d'autres primes à des agents contractuels. Une réponse claire a été apportée à cette question par l'instruction n° DGOS/RH4/2015/108 du 2 avril 2015 relative au régime indemnitaire applicable aux agents contractuels des établissements relevant de la fonction publique hospitalière[832]. Ce texte faisait suite aux nombreuses sollicitations du Ministre de la santé à ce sujet, tant par les organisations syndicales, que par les établissements de santé ayant fait l'objet d'un contrôle de la Cour des Comptes au sujet des modalités de rémunération des agents contractuels, et plus particulièrement le versement des primes et indemnités. Le raisonnement tenu par la DGOS dans cette instruction est le suivant : selon les dispositions du décret n° 91-155 du 6 février 1991[833], les modalités de rémunération de l'agent contractuel sont fixées par leur contrat. L'article 20 de la loi Le Pors quant à lui pose le principe selon lequel il n'y a pas de prime ou d'indemnité sans texte législatif ou réglementaire. Or, selon la DGOS, « *aucune disposition de la loi du 9 janvier 1986 susmentionnée n'instaure que les agents contractuels de la FPH sont soumis aux dispositions de cet article. Par ailleurs, l'article 54 du décret du 6 février 1991 rend applicables à ces agents les règles fixées par le décret du 24 octobre 1985 susmentionné qui se borne à définir chacun des éléments de la rémunération principale mentionnée à l'article 20 du titre Ier du statut général et à préciser leurs modalités de calcul. Ainsi, l'absence de renvoi à cet article 20 ne signifie pas une interdiction mais une possibilité de verser des primes et indemnités aux agents contractuels de la FPH sans que celles-ci soient nécessairement instituées par un texte législatif ou réglementaire* »[834]. Ainsi, et comme l'a fixé la jurisprudence, sans texte réglementaire, certains éléments de la situation des agents contractuels peuvent être fixés par le biais du contrat[835]. En revanche, seule l'autorité détentrice du pouvoir de nomination, sous laquelle sont placés les agents contractuels, pourra instaurer une prime en leur faveur[836].

697. Sous réserve de respecter l'ensemble de ces dispositions, un établissement de santé pourra donc embaucher des agents contractuels et leur accorder une prime. Cette souplesse

---

[831] CE, 23 mars 2009, n°312446.
[832] Instruction n° DGOS/RH4/2015/108 du 2 avril 2015 relative au régime indemnitaire applicable aux agents contractuels des établissements relevant de la fonction publique hospitalière, non parue au *JORF*.
[833] Décret n° 91-155 du 6 février 1991 relatif aux dispositions générales applicables aux agents contractuels des établissements mentionnés à l'article 2 de la loi n° 86-33 du 9 janvier 1986 modifiée portant dispositions statutaires relatives à la fonction publique hospitalière, *JORF* n°35 du 9 février 1991, p. 2058
[834] *Id.*, p. 2.
[835] CE, *Ass*. 30 janvier 1997, avis n° 359964.
[836] CE, 23 mars 2009, n° 312446.

accordée aux établissements de santé va leur permettre, dans une certaine mesure, d'accroitre leur attractivité vis-à-vis d'employeurs privés. Ils pourront donc envisager de recruter des compétences hautement spécialisées, dans le cadre de la mise en place de leur SIH.

B. L'appel aux ressources extérieures

698. Pour développer leur SIH de manière sécurisée et pérenne, les établissements de santé peuvent également faire le choix de faire appel à des ressources extérieures. Ce choix peut se traduire par l'achat de prestations ou d'outils informatiques auprès de sociétés extérieures, ou par la mutualisation des ressources informatiques entre établissements de santé. Cette possibilité ayant déjà fait l'objet d'une étude précédemment[837], nous nous focaliserons ici sur les modalités d'appui sur des sociétés extérieures.

699. Les établissements de santé n'ont pas pour mission principale de développer des solutions informatiques, ni de les mettre en œuvre dans le cadre d'un SIH cohérent. Cependant, ils sont porteurs d'un besoin bien défini et parfois même d'un projet précis. A ce titre, ils sont les maîtres d'ouvrage (ou maîtrise d'ouvrage) du projet. C'est à eux qu'il revient de définir l'objectif du projet, son calendrier et le budget qui lui sera consacré. Cependant, le maître d'ouvrage n'a pas toujours les compétences techniques nécessaires pour mener à bien son projet. C'est pourquoi il doit faire appel aux compétences d'un maître d'œuvre. Celui-ci aura pour responsabilité de réaliser le projet dans les délais et les coûts fixés. Par ailleurs, l'établissement de santé, en tant que maitre d'ouvrage, pourra s'entourer d'une assistance à la maîtrise d'ouvrage, ayant pour mission de l'accompagner dans la gestion et le pilotage du projet.

Ainsi, la conception du SIH, et notamment la conception de nouveaux logiciels qui vont venir l'alimenter, peut être confiée à des sociétés prestataires (1). L'établissement peut également être accompagné dans sa gestion stratégique du SIH par une société de conseil (2).

[837] *V. supra*. n° 222 à 224.

1) L'aide à la conception du SIH

700. La conception de logiciels informatiques est un secteur industriel en plein essor, qui nécessite par ailleurs une expertise technique et scientifique de haut niveau. A l'heure actuelle, rares sont les établissements qui ont fait le choix de développer en interne une solution logicielle permettant de répondre à leurs besoins. Le rapport de la Cour des Comptes publié en septembre 2016 cite cependant l'exemple réussi des Hospices Civils de Lyon (HCL) qui ont fait le choix d'être leur propre éditeur en ce qui concerne le dossier médical informatisé. Ainsi, à partir de 2012, les HCL ont développé leur propre dossier patient informatisé, nommé "*Easily*". Le déploiement de cette solution s'est fait par ailleurs sans retard et la solution convient aux utilisateurs[838]. Mais ce cas reste une exception et, en grande majorité, les établissements de santé font le choix de faire appel à des éditeurs pour leur fournir les solutions logicielles dont ils ont besoin.

701. A l'heure actuelle, le choix en la matière est assez vaste. En effet, plusieurs centaines d'éditeurs[839] de solutions logicielles sont actuellement présents sur le marché français. Cependant, ces acteurs présentent la particularité d'être principalement de petites entreprises, certains se spécialisant par ailleurs dans des marchés dits de "niche". Cette surspécialisation pose une difficulté importante aux établissements de santé, qui n'auront aucune visibilité sur la pérennité de ce type de structure et donc sur la solution mise en place. A titre d'exemple, le CHU de Nîmes avait choisi son éditeur pour le dossier patient informatisé en 2009. Cet éditeur a été racheté en 2011 et a proposé de nouvelles solutions logicielles, alors que le marché passé par le CHU de Nîmes était encore en cours et la solution initiale en cours de déploiement. Cette opposition entre le titulaire du marché et le CHU de Nîmes a mené à un contentieux entre les parties, réglé en 2014, mais entraînant de fortes pertes financières pour le CHU de Nîmes[840].

---

[838] Cour des Comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, *op. cit.*, p. 353.
[839] Plus de 300 selon le rapport de l'ANAP contre 277 selon le rapport de la Cour des Comptes.
[840] Cour des Comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », Rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, *op. cit.*, p 352.

Face à la technicité du sujet et à l'ampleur de l'offre sur le marché, parfois peu visible, il peut s'avérer nécessaire, pour les établissements de santé, d'être accompagné en amont du choix de la solution, au moment même de la définition de leurs besoins.

2) L'appui à la maîtrise d'ouvrage

702. Dans le cadre de son rapport rendu en septembre 2016, la Cour des Comptes a souligné les faiblesses actuelles des maîtrises d'ouvrage des projets informatiques développés par les établissements de santé[841]. La maîtrise d'ouvrage est pourtant fondamentale puisqu'elle est le point de départ de l'ensemble du projet. Elle se doit d'être solide si l'établissement souhaite voir son projet mené à bien. Ainsi la Cour des Comptes, au cours de ses contrôles a pu constater les lacunes suivantes : « *absence de réunion des compétences techniques requises, dimensionnement insuffisant des équipes, analyse imparfaite des besoins, compréhension insuffisante des attentes des utilisateurs tout au long du déploiement du projet* »[842].

703. Ces difficultés ne sont pas sans conséquences puisqu'une maîtrise d'ouvrage faible va entrainer des retards dans le calendrier de déploiement des solutions informatiques, et surtout des dépassements du budget fixé. A ce sujet, le constat est sans appel : à l'heure actuelle, et en ce qui concerne les établissements contrôlés par la Cour des Comptes à l'occasion de son enquête relative aux SIH[843], la moitié des opérations financées par le plan hôpital 2012 ont dépassé à la fois les enveloppes financières et les calendriers fixés[844].

704. A la suite de son audit des SIH, l'ANAP avait quant à elle constaté que les directions des systèmes d'information étaient encore « *trop souvent démunies pour gérer et piloter les projets en lien avec les professionnels métiers et industriels* »[845]. Alors que les ressources

---

[841] Cour des Comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », Rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, *op. cit.*, p.338.
[842] *Id.*, p. 338.
[843] A l'occasion de cette enquête, la Cour des comptes a contrôlé l'AP-HP, les HCL, 4 CHU, un CHR, un EPSM 32 CH, un centre de lutte contre le cancer, un GIP et un GIE.
[844] Cour des comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », Rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, *op. cit.*, p. 338.
[845] ANAP, « Audit des systèmes d'information hospitaliers auprès d'établissements représentatifs », *op. cit.*, p. 30.

techniques en interne des établissements sont aujourd'hui présentes, la gestion de projet reste une faiblesse des équipes informatiques des établissements de santé.

L'appel à une prestation d'appui à maîtrise d'ouvrage auprès d'une société extérieure permettrait aux établissements d'éviter ces écueils. Or, aujourd'hui, cela est encore rare[846], les établissements de santé n'ayant pas acquis le réflexe de faire appel à un appui externe en ce qui concerne la maîtrise d'ouvrage.[847]

[846] Cour des comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », Rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, *op. cit*., p. 333.
[847] ANAP, « Audit des systèmes d'information hospitaliers auprès d'établissements représentatifs », rapport final, mars 2014, p. 30.

Conclusion de la section

705. Avant même de développer le recours aux TIC et de les intégrer à la pratique quotidienne, les établissements doivent réfléchir à la construction de leur Système d'Information Hospitalier. Celle-ci doit se faire de manière stratégique et la mise en place du SIH doit devenir un projet à part entière de l'établissement de santé. Cette vision stratégique permettra aux établissements de santé d'anticiper des éventuels aléas et donc sécuriser, en amont, l'utilisation qui sera faite des TIC ainsi mises en place.

Le développement pérenne du SIH passe également par l'appel à des ressources expertes sur le sujet. Ainsi, le recrutement d'ingénieurs informatiques spécialisés et le recours à des sociétés prestataires sont deux solutions envisageables pour les établissements de santé, afin de s'entourer des expertises nécessaires.

Les solutions sont complémentaires et peuvent, bien évidemment, être mises en œuvre de manière concomitante. En effet, même en embauchant directement des ingénieurs informatiques experts dans leur domaine, les établissements de santé ne souhaitent pas se lancer dans la création et l'édition directe de solutions logicielles.

Les établissements de santé doivent, en tout état de cause, penser à s'entourer des ressources nécessaires et suffisantes afin de s'assurer de mener à bien et dans les meilleures conditions, le développement de leur SIH.

Section 2. Les pistes de sécurisation *a posteriori*

706. Le développement d'un SIH structuré va permettre aux établissements de santé d'intégrer de manière pérenne et sécurisée les TIC à la pratique de ses professionnels. Cependant, mettre à disposition un outil fiable et adapté ne fait pas tout. *A posteriori*, l'établissement de santé va pouvoir venir sécuriser leur utilisation quotidienne. Pour cela, il dispose de deux types de leviers : le levier juridique et le levier managérial.

Par le biais du levier juridique (paragraphe 1), l'établissement de santé va pouvoir rappeler voire parfois même édicter, la règle en matière de bon usage de l'outil ainsi mis à disposition. Il pourra également veiller à ce que les agents s'engagent à une utilisation correcte des TIC. Le levier managérial (paragraphe 2), quant à lui, va permettre à l'établissement de santé de former les agents à une utilisation adéquate des TIC et, dans l'hypothèse d'une violation des règles édictées, mettre en place des sanctions à l'encontre de l'agent.

§1. L'utilisation d'outils juridiques

707. Pour les établissements publics de santé, les enjeux d'une bonne utilisation des TIC par ses agents sont multiples. En premier lieu, l'établissement doit s'assurer que les outils sont utilisés de manière à réaliser les missions qui lui sont propres (le soin, la recherche et l'enseignement). Il doit s'assurer ensuite que cette utilisation permet d'assurer la continuité des soins, la sécurité des patients mais également la confidentialité des données de santé ainsi que celle des données personnelles recueillies. Enfin, il est essentiel pour l'établissement de s'assurer qu'il n'est pas fait une utilisation indue, abusive voire illégale, des outils informatiques qu'il met à disposition de ses agents. En effet, l'établissement de santé pourrait voir sa responsabilité engagée du fait des fautes commises par ses agents dans le cadre de l'utilisation des TIC ou par le biais de l'utilisation de ces outils. Les établissements de santé doivent donc trouver un équilibre entre les risques qu'ils encourent du fait d'une potentielle mauvaise utilisation des TIC par leurs agents et les conditions dans lesquelles ils souhaitent que ces outils soient utilisés, afin de répondre à leur mission première.

Pour réguler cela, l'établissement de santé a donc intérêt de faire le choix d'instaurer une limitation et un contrôle de l'utilisation qui est faite des TIC par ses agents (A). Pour accompagner cette démarche, il peut faire appel à un outil de droit souple de plus en plus utilisé : la charte informatique (B).

A. Le contrôle et la limitation de l'utilisation des TIC

« *Ce sont moins les NTIC – nouvelles technologies de l'information et de la communication – qui "mettent à l'épreuve le droit du travail" que le droit du travail qui se manifeste ici comme norme régulatrice de l'emploi des NTIC* »[848].

708. Aujourd'hui, il n'est pas rare que le matériel informatique mis à disposition des agents soit parfois utilisé à d'autres fins que le strict exercice de leurs missions professionnelles. Comme le soulignait Jean-Pierre GRIDEL[849], dans son étude consacrée à l'utilisation de l'outil informatique mis à la disposition du salarié pour les besoins de son activité professionnelle, l'outil informatique est « *susceptible de détournement dans son utilisation* ». Or, contrairement aux cas où il apparait clairement que le détournement du matériel mis à disposition doit être automatiquement sanctionné[850], le détournement de l'outil informatique à des fins privées ne peut s'envisager de la même manière.

En effet dans ce contexte particulier, les libertés fondamentales des agents (1) vont se confronter aux obligations professionnelles dont ils sont débiteurs vis-à-vis de leur employeur mais également au pouvoir dont dispose l'employeur de contrôler, voire restreindre, l'utilisation qui peut être faite par ses agents des outils qu'il leur met à disposition dans un but purement professionnel (2).

---

[848] LYON-CAEN, Gérard. « Débat autour de l'arrêt Nikon France », Semaine Sociale Lamy, nº 1046, 15 octobre 2001. Disponible sur [http://lamyline.lamy.fr], consulté le 16 janvier 2017.

[849] GRIDEL, Jean-Pierre. « L'entreprise et l'utilisation en justice de l'information issue de l'outil informatique mis à la disposition du salarié pour les besoins de son activité professionnelle. En hommage à la haute mémoire du professeur Pierre Catala », *Communication commerce électronique,* n° 7-8, juillet 2016, étude n° 13.

[850] *V.* notamment en ce sens : CE, 6 Mai 2011, n° 330020. Dans cette décision, la Haute juridiction a rappelé qu'« *un agent public qui détourne de l'objet de sa mission un véhicule de service pour l'utiliser à des fins personnelles, sans y être autorisé par l'administration, commet une faute personnelle détachable de l'exercice de ses fonctions* ».

1) Le droit à la vie privée dans le cadre professionnel : enjeux et limites

709. L'article 25 Septies de la loi Le Pors[851] prévoit que « *le fonctionnaire consacre l'intégralité de son activité professionnelle aux tâches qui lui sont confiées* ». De même, par principe, le matériel professionnel mis à la disposition d'un agent par son employeur ne peut faire l'objet que d'une utilisation strictement professionnelle et la jurisprudence considère que l'utilisation par un agent du matériel qui lui été fourni pour d'autres fins constitue une faute[852].

Cependant, en ce qui concerne l'utilisation de la messagerie professionnelle (a) ainsi que d'Internet et de l'ordinateur (b), ces principes souffrent de plusieurs exceptions et vont être mis en regard de certaines libertés fondamentales dont disposent tous les citoyens, et donc les agents dans le cadre de leurs fonctions professionnelles.

a) La messagerie professionnelle

710. En droit privé, c'est en 2001 à l'occasion du célèbre arrêt « Nikon »[853] que la Cour de Cassation s'est prononcée, pour la première fois, sur la protection de la vie privée sur le lieu de travail. A cette occasion, les juges ont eu à se pencher sur la question de l'utilisation de la messagerie professionnelle à des fins personnelles par un salarié. En l'espèce, un salarié de la société Nikon France avait signé, avec les sociétés Nikon Corporation et Nikon Europe BV, un accord de confidentialité lui interdisant de divulguer des informations confidentielles communiquées par ces deux sociétés. Quelques années plus tard, le salarié a été licencié pour faute grave, à la suite notamment de l'utilisation à des fins personnelles du matériel mis à disposition par son employeur. Saisi d'un pourvoi en cassation, la Haute juridiction est venue préciser que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ». Ainsi, nous pouvons constater

[851] Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires. Loi dite loi Le Pors. *JORF*, 14 juillet 1983, p. 2174.
[852] CAA Douai, 2 décembre 2010, n° 09DA01118.
[853] Cass. Soc., n°99-42942, 2 octobre 2001.

que pour les magistrats de la Cour de Cassation, « *le droit, principalement celui des libertés individuelles, n'a pas à s'incliner devant l'état de la technologie ; c'est à la technologie de s'adapter […] aux exigences fondamentales du droit* »[854]

711. Cet arrêt vient poser le principe du respect de l'intimité de la vie privée au sein de la sphère professionnelle en y appliquant de manière stricte le droit au secret des correspondances. Pour reprendre les termes de Gérard LYON-CAEN[855], le cloisonnement entre vie privée et vie professionnelle disparaît. Cette décision est parfaitement transposable aux administrations publiques, où l'agent pourra voir ses correspondances privées protégées par le secret des correspondances[856].

712. Ainsi, l'employeur ne peut pas accéder aux courriels de ses agents qui relèveraient de la sphère privée, sous peine de risquer une condamnation pénale, l'atteinte au secret des correspondances étant réprimée notamment par les articles 226-15[857] et 432-9[858] du Code pénal. Cependant, pour être protégé par le secret de la correspondance, il est nécessaire que ces messages soient identifiés comme ayant un caractère privé. En l'absence de réelle définition légale, malgré une tentative restée lettre morte[859], c'est à la définition construite par les juges qu'il faut s'en remette. Ainsi, ces derniers acceptent communément de considérer comme étant un message privé le courrier électronique dont l'objet précise la mention

---

[854] LYON-CAEN, Gérard. « Débat autour de l'arrêt Nikon France », Semaine Sociale Lamy, Nº 1046, 15 octobre 2001, disponible sur [http://lamyline.lamy.fr.]. Consulté le 16 janvier 2017.

[855] *Ibid.*

[856] Article 1er de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, *JORF* n° 162, 13 juillet 1991, p. 9167.

[857] L'article 226-15 du Code pénal dispose : « *le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions* ».

[858] L'article 432-9 du Code pénal dispose : « *le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu.* »

[859] *V.* notamment en ce sens la proposition de loi sénatoriale n° 385 de juin 2006, dont le but était de définir le courrier électronique professionnel.

"personnel" ou "privé"[860]. Au contraire, un message à caractère "mixte", émis par un agent public sur sa messagerie professionnelle et contenant, d'une part, des éléments d'ordre professionnel et, d'autre part, des opinions personnelles au sujet de l'organisation de son service est considéré comme relevant de la sphère professionnelle[861]. En revanche, un employeur peut sanctionner un agent qui, en accédant aux courriers électroniques privés d'un de ses collègues, se serait lui-même rendu coupable d'une atteinte au secret des correspondances privées[862].

Ainsi, une tolérance vis-à-vis d'une utilisation privée de la messagerie professionnelle est aujourd'hui communément admise, étant entendue que cet usage doit se faire dans des proportions raisonnables.

b) L'utilisation d'Internet et du matériel informatique à des fins privées

713. Là encore, le principe est le même : l'usage du matériel informatique ainsi que des connexions Internet mis à disposition de l'agent par son employeur doit être strictement professionnel. Cependant, une tolérance est admise dans la mesure où l'usage privé reste raisonnable. Le curseur quant au caractère raisonnable ou non de l'utilisation de l'outil informatique et d'Internet a été placé par la jurisprudence et par la CNIL. La CNIL, dans son rapport d'activité de 2003[863], considère qu' « *une interdiction générale et absolue de toute utilisation d'Internet à des fins autres que professionnelles ne parait pas réaliste dans une société de l'information et de la communication* ». Ainsi, l'autorité administrative indépendante considère qu'il est socialement admis qu'une utilisation à des fins personnelles du matériel professionnel puisse être effectuée, tant que cet usage n'amoindrit pas les conditions d'accès au réseau et ne diminue pas la productivité du salarié.

714. Cependant, là encore, les fichiers personnels doivent être identifiés comme tels, sous peine d'être accessible par l'employeur sans l'accord du salarié. En effet, pour la Cour de Cassation, il apparait que « *les dossiers et fichiers créés par un salarié grâce à l'outil*

---

[860] *V.* notamment en ce sens, CAA Nancy, 2 août 2007, Commune de Lons-le-Saunier c/ Mme E. Mazzier, n° 07NC00217.

[861] CA Rennes, 14 janvier 2010, n° 972010. Dans cette affaire, les juges ont estimé notamment que la réponse apportée à une question professionnelle par l'agent mis en cause était le prétexte qui avait conduit cet agent a exprimé son opinion personnelle. Dès lors, les juges ont considéré que : « *indépendamment du ton employé et de la restriction d'une réponse faite au seul expéditeur d'un message général, la correspondance litigieuse est bien d'essence professionnelle* »

[862] CE, 25 janvier 2006, n° 280165.

[863] CNIL, 24ème rapport d'activité, 2003, p. 497.

informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel »[864].

En revanche, cette protection de la vie privée ne va pas jusqu'à protéger les "favoris" de navigation sur Internet, qui ne présentent pas un caractère personnel[865]. Ainsi, l'historique de navigation Internet ne pourra jamais, contrairement aux fichiers informatiques, être protégé par le droit au respect de la vie privée, celui-ci ne pouvant jamais être identifié de manière directe comme étant "personnel". Par ailleurs, la jurisprudence se montre très claire à ce sujet et le contrôle des connexions Internet d'un salarié par son employeur est possible puisque ces connexions sont présumées avoir un caractère professionnel.[866]

2) Les possibilités de régulation et de contrôle offertes à l'employeur

715. Dans un souci à la fois de sécurité du réseau informatique mais également d'efficacité dans le fonctionnement de ses services, l'employeur va pouvoir, tout en respectant les libertés fondamentales des agents, contrôler voire limiter l'utilisation des outils informatiques des agents. En effet, un contrôle de l'utilisation qui peut être faite des TIC par les agents permet à l'établissement de prévenir une atteinte, interne ou externe, à son système d'information. Par ailleurs, l'établissement pourrait, comme nous l'avons souligné auparavant, voire sa responsabilité engagée du fait d'une utilisation prohibée des TIC par ses agents. Comme le soulignait l'avocat général de la Cour de Cassation, S. KEHRIG, dans le cadre de l'arrêt NIKON France, « *S'il est certain qu'en vertu de son pouvoir de direction, l'employeur a le droit de contrôler et surveiller l'activité de ses salariés pendant le temps de travail […], ce droit peut même d'ailleurs se transformer en devoir, eu égard aux règles de responsabilité civile du commettant […]* »[867]. Ce risque est le même pour les établissements de santé, qui sont, par principe, responsable du fait de leur agent, sauf à venir démontrer l'existence d'une faute détachable du service.

---

[864] Cass. Soc., 18 octobre 2006, Jérémy L.-F c/ Techni-soft, n° 04-48025.
[865] Cass. Soc., 9 février 2010, n° 08-45253.
[866] Cass. Soc., 9 juillet 2008, n° 06-45800.
[867] Conclusion de M. KEHRIG, avocat général. Disponibles sur [https://www.courdecassation.fr]. Consulté le 16 janvier 2017.

716. Le contrôle mis en place par l'employeur doit répondre au même principe que celui qui dirige l'utilisation privée des outils professionnels par l'agent : le principe de proportionnalité. Par ailleurs, il paraît évident que la mise en place d'un tel contrôle ne devra être motivé par l'unique volonté de l'employeur d'instaurer une surveillance de ses agents. En effet, la cybersurveillance des salariés est très encadrée et l'employeur ne sera pas libre de ses mouvements. Ce contrôle peut être deux ordres : soit global, soit ciblé.

717. En premier lieu en effet, l'employeur peut décider de mettre en place un contrôle global de l'ensemble des utilisations des TIC réalisées par ses agents. Par exemple, il lui est possible de contrôler l'ensemble des connexions Internet réalisées par ses agents, ou même utiliser des fichiers de journalisation pour connaitre l'ensemble des flux informatiques réalisés au sein du système d'information. Dans la même logique, il peut contrôler le "trafic" de la messagerie professionnelle, sans prendre connaissance du contenu de l'ensemble des e-mails échangés. Dans les deux cas, nous nous situons dans un contrôle que nous pouvons qualifier de "masse" et généralisé de l'utilisation des TIC. A ce niveau, il s'agit principalement pour l'employeur de s'assurer que son système d'information est correctement conçu pour supporter la charge qui lui est imposée, mais également s'assurer qu'il n'existe pas de failles de sécurité. Cependant, à partir du moment où ces pratiques induisent une collecte d'informations à caractère personnel, telles que définies par la loi Informatique et Libertés, l'employeur devra effectuer les déclarations nécessaires auprès de la CNIL. Par ailleurs, dans tous les cas, la mise en place d'un contrôle des accès et connexions induit, en vertu du principe de loyauté, une information a priori des agents. Si ces conditions sont remplies, alors l'employeur pourra par la suite, si la situation l'exige, utiliser ces éléments ainsi recueillis dans le cadre d'une procédure disciplinaire à l'encontre de son agent[868].

718. Dans un second temps, sous certaines conditions strictes, l'employeur va pouvoir également consulter les dossiers de son agent pourtant identifiés comme étant personnels. En effet, par principe, l'employeur peut demander à l'agent d'accéder aux fichiers identifiés comme étant personnels en présence de celui-ci ou si celui-ci a été informé préalablement. Dans ce cas, la violation de la vie privée, ou dans le cas des courriels, du secret des correspondances, ne sera pas constituée. Par ailleurs, selon la jurisprudence, l'employeur peut

[868] CA, Rouen, 11 septembre 2007, n° 07/180.

également accéder à ces fichiers, sans l'accord du salarié, en cas de risque ou événement particulier[869]. Cependant, encore faut-il que l'employeur puisse justifier d'un tel risque ou événement particulier.

Par ailleurs, comme la jurisprudence judiciaire a déjà eu l'occasion de le préciser[870], la présence de fichiers informatiques ou de courriels identifiés comme personnels ne fait pas obstacle à la mise en œuvre de l'article 145 du Code de procédure civile. Ainsi, un huissier pourra récupérer des copies des fichiers en présence du salarié. En l'espèce, il s'agissait d'un employeur qui pensait que le matériel informatique qu'il mettait à disposition de son employé servait à favoriser des actes de concurrence déloyale. Le juge a estimé que cette raison était légitime et a ordonné à un huissier de saisir une copie des éléments susceptibles de caractériser un acte de concurrence déloyale.

719. En revanche, il nous semble important de préciser que, même si l'administrateur réseau peut accéder à certains courriels d'ordre privé dans le cadre de sa fonction visant à assurer la sécurité du réseau informatique de l'entreprise, cela ne peut se faire qu'à certaines conditions. Ainsi, un employeur peut parfaitement confier à son administrateur réseau, soumis à une obligation de confidentialité, une enquête spécifique suite à un incident de sécurité, même si cette enquête conduit à la prise de connaissance par l'administrateur, de courriels protégés par le secret des correspondances[871]. Toutefois, l'administrateur réseau ne pourra en aucun cas se délier de son obligation de confidentialité pour communiquer ces messages à son employeur. A ce sujet, la Cour de cassation est venue préciser notamment que même si la sécurité du réseau informatique d'une entreprise justifie que son administrateur réseau fasse usage de l'ensemble des possibilités techniques qu'il a à sa disposition afin de prendre les mesures qui s'imposent, « *la divulgation du contenu des messages […] ne [relève] pas de ces objectifs* »[872].

720. Enfin, bien évidemment, en amont de ce contrôle, l'employeur peut légitimement limiter, voire même parfois bloquer les utilisations de l'outil informatique. A titre d'exemple,

---

[869] Cass. Soc., 17 mai 2005, n° 03-40701.
[870] Cass. Soc., 10 juin 2008, n° 06-19229.
[871] Cass. Soc., 17 juin 2009, SA Sanofi Chimie c/ M. GUZZI et a., n° 08-40274.
[872] CA Paris, 11ème chambre, F. et a., 17 décembre 2001.

il pourra mettre en place des dispositifs permettant le filtrage des sites Internet non autorisés (sites à caractère pornographique par exemple, mais également les sites des réseaux sociaux, s'il le juge utile). Il pourra également interdire la possibilité pour les agents de télécharger de nouveaux logiciels sur leur poste de travail. Pour des raisons de sécurité toujours, et afin d'éviter la propagation de virus informatique, l'utilisation des clés USB personnelles non sécurisées pourra être prohibée (même si, en pratique, l'employeur devra, dans la plupart du temps, proposer une solution alternative qui consistera, par exemple, à fournir lui-même des clés sécurisées). De même, dans le cadre de l'utilisation de logiciels, (comme cela est le cas pour les logiciels de dossiers médicaux par exemple) certains agents verront, en vue de leur fonction ou de leurs missions, leur droit d'accès à certaines données limité.

B. La mise en place d'une charte informatique

721. Le recours aux chartes informatiques, que cela soit au sein des entreprises privées ou des administrations publiques, s'est développé depuis plusieurs années. Définies par une circulaire de 2008[873] comme étant des « *outils permettant, à l'inverse du règlement intérieur dont le champ est légalement limité, de réunir en un document, selon un contenu et un degré de précision variables, les engagements et obligations respectifs de l'employeur et des salariés, dans le cadre de l'exécution du contrat de travail* », les chartes se révèlent être des très utiles pour l'employeur, à condition d'être utilisées convenablement. Elles permettent en effet à ce dernier de mettre à plat les « règles du jeu » en matière d'utilisation des TIC par ses agents.

« *A défaut de textes officiels et normatifs sur le sujet* »[874], la charte présente l'avantage de formaliser de manière claire et opposable les règles applicables, au sein de l'établissement, en matière d'utilisation des outils informatiques et des TIC. L'avantage majeur de cet outil est, bien entendu, sa grande souplesse. Encadré par aucun texte, contrairement au règlement intérieur de l'établissement de santé par exemple, aucun contenu a minima n'est imposé. Libre à l'établissement de l'élaborer avec l'ensemble des informations qu'il souhaite y faire figurer. En revanche, pour des questions pratiques, il est évident que cet outil ne doit pas

[873] Circulaire DGT 2008/22 du 19 novembre 2008 relative aux chartes éthiques, dispositifs d'alerte professionnelle et au règlement intérieur, Ministère du travail, des relations sociales, de la famille et de la solidarité, non parue au *JORF*.
[874] CAA Nancy, 2 août 2007, Cne Lons-le-Saunier, *JCP A*, 2007, n° 2039, note n° 07NC00217 de D. JEAN-PIERRE.

devenir un catalogue technique des modalités d'utilisation des TIC. La charte peut également interdire certaines utilisations des TIC, sans que cela puisse être contesté. Ainsi, une charte informatique qui interdit l'utilisation de la messagerie professionnelle à des fins politiques est légale[875].

722. Pour autant, bien évidemment, l'absence de charte ne veut pas dire absence de règles ou absences de sanctions. Dans certains cas, ce n'est pas la violation de la charte qui sera sanctionnée, mais bien la violation d'une obligation déontologique du professionnel, agent de la fonction publique[876]. La charte reste cependant le moyen le plus efficace d'informer les agents sur les usages qui ne seront pas tolérés. Elle présente également un intérêt pédagogique vis-à-vis des agents, en matière de sécurité informatique, car il ne faut pas oublier que « *la sécurité ne s'impose pas, elle s'inculque* »[877]. Cependant, afin d'être totalement efficace, la charte informatique devra être opposable aux agents. Car tout comme la jurisprudence reconnaît la possibilité de s'appuyer sur ces chartes pour sanctionner un salarié, elle rappelle également la nécessité que ces chartes soient, avant toute chose, opposable[878].

723. Au sein d'un établissement de santé, le Directeur d'établissement dispose de plusieurs solutions pour rendre opposable sa charte informatique. Il peut d'abord faire le choix d'annexer cette charte au contrat de travail des agents, permettant ainsi d'en faire un document contractuel opposable aux agents en cas de violation celle-ci. En revanche, cette possibilité n'est envisageable que pour les personnels contractuels. Pour les titulaires de la fonction publique hospitalière, cette solution sera impossible. En effet, par principe, les agents titulaires de la fonction publique sont régis par leurs statuts, issus de la loi (pour les fonctionnaires de la fonction publique hospitalière, il s'agit de la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière[879]) et du

[875] CAA Nancy, 2 août 2007, Cne Lons-le-Saunier, *op. cit.*
[876] CAA Paris, 12 février 2008, n° 06PA04287.
[877] CAPRIOLI & Associés, « Démarche pour la mise en place d'une charte "informatique et communications électroniques" dans les collectivités territoriales », disponible sur [http://www.caprioli-avocats.com]. Consulté le 16 janvier 2017.
[878] Conseil des prud'hommes de Paris, 10 juin 2014, n° 13/02093.
[879] Loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière, *JORF* du 11 janvier 1986, p. 535.

règlement[880]. Seuls des textes de cet ordre peuvent donc modifier les règles qui viendront régir leur statut.

724. Cependant, une autre solution existe au sein des établissements de santé afin de permettre de donner à la charte une valeur juridique suffisante à la rendre opposable. Il suffit, pour cela, d'en faire un élément du règlement intérieur. Cette solution est par ailleurs déjà validée par la jurisprudence pour les entreprises privées[881]. Il s'agit d'un avantage dont disposent les établissements de santé par rapport aux collectivités territoriales par exemple. Ainsi, en annexant au règlement intérieur de l'établissement la charte informatique, celle-ci deviendra de fait opposable à tous les agents de l'établissement, contractuels ou titulaires. Cela induit en revanche de respecter un circuit de validation interne préalable, qui inclut notamment une présentation en comité technique d'établissement. Toutefois, la jurisprudence n'exige pas toujours un passage devant les instances et notamment une consultation du Comité technique. Par exemple, une Cour Administrative d'Appel a déjà eu l'occasion de juger que l'agent qui méconnait les règles d'utilisation de la messagerie professionnelle, fixées au sein de la charte informatique, commet une faute disciplinaire, même si cette même charte n'a pas fait l'objet d'un examen en comité technique, le chef d'établissement disposant du pouvoir réglementaire en matière d'utilisation de la messagerie[882].

Néanmoins, l'employeur se doit d'informer ses agents des règles encadrant l'utilisation du matériel informatique qui leur est mis à disposition[883]. A l'occasion de plusieurs litiges aux Prud'hommes, la charte informatique a été progressivement reconnue comme opposable au salarié et sa violation a justifié dans plusieurs cas des licenciements pour faute grave. En 2006, par un arrêt en date du 21 décembre[884], la Cour de Cassation avait même fait référence de manière explicite à la charte informatique d'une entreprise, dont la violation avait entrainé le licenciement pour faute grave d'un salarié[885].

---

[880] Par exemple, le décret n° 91-155 du 6 février 1991 relatif aux dispositions générales applicables aux agents contractuels des établissements mentionnés à l'article 2 de la loi n° 86-33 du 9 janvier 1986 modifiée portant dispositions statutaires relatives à la fonction publique hospitalière, *JORF* n° 35 du 9 févier 1991, p. 2058.
[881] Cass. Soc., 15 décembre 2010, n° 09-42691.
[882] CAA Nantes, 2 juillet 2010, n° 10NT00319.
[883] WALLE, Emmanuelle. « A nouvelles technologies, nouvelles causes de licenciement », *Gaz. Pal.*, 23 avril 2011, n° 113, p. 20.
[884] Cass. Soc., 21 décembre 2006, n° 05-41165, J.-H. Pettre c/sté Ad 2 One SA.
[885] CAPRIOLI, Eric. « Charte informatique et droit du travail », *Communication commerce électronique*, n° 7-8, juillet 2001, commentaire 101.

La charte informatique est également un moyen pour l'employeur d'informer de manière loyale ses salariés de l'ensemble des mesures éventuelles de surveillance et de contrôle des accès et de l'utilisation des outils informatiques. Dès lors, elle permet ensuite l'utilisation de ces traces lors d'éventuelles procédures disciplinaires.

§2. L'utilisation d'outils managériaux

725. L'impact de l'introduction des TIC au travail fait l'objet de nombreuses études depuis plusieurs années. La doctrine s'est penchée à la fois sur les risques induits par l'introduction des TIC sur la santé du salarié[886] et ses conditions de travail, mais également sur les risques liés à un contrôle abusif des salariés par leur employeur[887], ou encore sur l'impact des TIC sur l'action syndicale[888]. Dernièrement, avec le développement du télétravail notamment, c'est le droit à la déconnexion qui a fait l'objet de multiples études[889].

726. L'introduction des TIC comme outil de travail induit pour l'employeur la nécessité d'accompagner la mise en place de ces outils mais également de veiller à leur bonne utilisation voire, de réguler d'éventuelles utilisations qui ne seraient pas en accord avec la loi ou les pratiques internes fixées par le biais de la charte informatique. Pour ce faire, l'employeur va disposer d'outils managériaux efficaces. En amont, l'administration hospitalière pourra et même, devra, assurer la formation des utilisateurs des TIC afin qu'ils puissent adapter leurs pratiques à ces nouveaux outils (A). Puis, dans l'hypothèse où l'agent n'aurait pas effectué une utilisation correcte de ses outils, l'employeur aura la possibilité de le sanctionner (B). Ces deux outils managériaux vont permettre aux établissements de santé de sécuriser l'utilisation des TIC à l'hôpital.

---

[886] *V.* notamment en ce sens : FANTONI-QUINTON, Sophie. LEBORGNE-INGELAERE, Céline. « L'impact des TIC sur la santé au travail », *JCP-S*, novembre 2013, n° 48, pp. 16-21.

[887] *V.* notamment en ce sens : De GIVRY, Emmanuel. « Tic et surveillance du salarié : regards de la CNIL », JCP-S, octobre 2013, n° 41, pp. 24-26 ; BAREGE, Alexandre. BOSSU, Bernard. « Les TIC et le contrôle de l'activité du salarié », *JCP-S*, octobre 2013, n° 41, pp. 13-23.

[888] *V.* notamment en ce sens : GAURIAU, Bernard. « Les TIC et l'action syndicale », *JCP-S*, octobre 2013, n° 41, pp. 18-24.

[889] *V.* notamment en ce sens : De MONTVALON, Luc. « Droit à la déconnexion : l'arbre qui cache la forêt ? », *Semaine sociale Lamy*, novembre 2016, n° 1743, pp. 19-20 ; MATHIEU, Chantal. PERETIE, Marie-Madeleine. PICAULT, Alex. « Le droit à la déconnexion, une chimère ? », *Revue droit du travail Dalloz*, octobre 2016, n° 10, pp. 592-598.

A. La formation des utilisateurs

727. La formation professionnelle des agents publics, obligation légale à la charge tant de l'employeur et de l'agent (1) va s'avérer être un outil managérial précieux (2) pour accompagner la mise en place des TIC.

1) La formation professionnelle, une obligation légale réciproque

728. Comme le prévoit la loi Le Pors, « *le droit à la formation professionnelle tout au long de la vie est reconnu aux fonctionnaires* »[890]. La formation professionnelle au cours de sa carrière est un droit essentiel de l'agent public, qui s'inscrit dans un cadre règlementaire et financier assez précis, prévu notamment, en ce qui concerne la fonction publique hospitalière, par le décret n° 2008-824 du 21 août 2008 relatif à la formation professionnelle tout au long de la vie des agents de la fonction publique hospitalière[891] et par la circulaire n° DHOS/RH4/2010/57 du 11 février 2010 relative à la mise en œuvre du congé de formation professionnelle des agents de la fonction publique hospitalière. Cependant, ce n'est que récemment que la formation professionnelle des agents publics a pris une place importante. En effet, jusqu'en 2007, les agents bénéficiaient d'un droit à une « *formation permanente* »[892]. S'inspirant des règles applicables en droit du travail, le droit de la fonction publique a évolué et consacré, au travers de la loi de 2007 de modernisation de la fonction publique[893], un droit fondamental pour l'agent public à la formation continue tout au long de sa vie professionnelle. Cette loi consacre notamment la reconnaissance de l'expérience professionnelle pour les promotions internes ainsi que dans les concours administratifs, et développe la validation des acquis de l'expérience (VAE). Elle introduit également le droit individuel à la formation, qui n'existait pas jusqu'alors dans la fonction publique.

---

[890] Article 22, loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires. Loi dite loi Le Pors. *JORF* du 14 juillet 1983, p. 2174.

[891] Décret n° 2008-824 du 21 août 2008 relatif à la formation professionnelle tout au long de la vie des agents de la fonction publique hospitalière, *JORF* n° 0196, 23 août 2008, p. 13285.

[892] L'article 22 de la loi Le Pors, dans sa rédaction applicable jusqu'en 2007 disposait que : « *Le droit à la formation permanente est reconnu aux fonctionnaires. Ceux-ci peuvent être tenus de suivre des actions de formation professionnelle dans les conditions fixées par les statuts particuliers.* »

[893] Loi n° 2007-148 du 2 février 2007 de modernisation de la fonction publique, *JORF* n°31, 6 février 2007, p. 2160.

Ainsi, et comme l'a souligné à juste titre Emmanuel AUBIN, en parlant de "travaillisation"[894] du droit de la fonction publique, le droit du travail a eu une véritable influence positive en la matière sur le droit de la fonction publique.

729. Ce droit fondamental de l'agent à la formation, opposable à l'administration, se traduit, pour l'employeur, en une obligation assez forte. Celui-ci devra notamment prendre à sa charge les frais de formation. De même, dans l'hypothèse où la formation de l'agent se déroulerait en dehors du temps de travail, il devra attribuer à l'agent une allocation de formation[895]. Mais l'obligation de l'employeur public va plus loin, puisqu'il doit également se montrer actif en la matière. Ainsi, les dispositions de l'article 37 du décret de 2008 lui imposent de mettre en place « *un document pluriannuel d'orientation de la formation des agents* » document qui devra être par ailleurs « *soumis pour avis au comité technique d'établissement* ». En outre, « *ce document d'orientation est fondé sur l'analyse de l'évolution des effectifs, des emplois, des compétences et des missions de l'établissement. Il porte sur les priorités, les objectifs et les moyens de la formation professionnelle des agents au regard de ces évolutions. Il prend également en compte l'analyse de la situation comparée des hommes et des femmes et l'accès de tous les agents à la formation. Dans le cadre ainsi défini, le chef d'établissement arrête tous les ans le plan de formation, après avis du comité technique d'établissement qui se réunit, à cet effet, au cours du dernier trimestre précédant la période couverte par ce plan. Les plans de formation des établissements prennent en compte les priorités nationales de formation et les plans de santé publique définis par le ministre chargé de la santé. Le suivi de la réalisation du plan ainsi que l'évaluation de ses résultats doivent associer le comité technique d'établissement.* »[896]

L'obligation qui pèse sur les établissements de santé en matière de formation est donc importante et la formation professionnelle doit faire l'objet, au sein des établissements de santé, d'un projet construit par l'employeur.

---

[894] AUBIN, Emmanuel. « Les dispositions relatives à la formation professionnelle des fonctionnaires tout au long de la vie », *AJDA*, 2007, p. 511.

[895] L'article 16 du décret n° 2008-824 du 21 août 2008 relatif à la formation professionnelle tout au long de la vie des agents de la fonction publique hospitalière prévoit que : « *Les heures de formation réalisées par un agent dans le cadre du droit individuel à la formation en dehors du temps de travail donnent lieu au versement d'une allocation de formation d'un montant égal à 50 % du traitement horaire de l'agent concerné.* »

[896] Article 37, décret n° 2008-824 du 21 août 2008 relatif à la formation professionnelle tout au long de la vie des agents de la fonction publique hospitalière, *JORF* n° 0196, 23 août 2008, p. 13285.

730. Cependant, cette obligation n'est pas à sens unique, et il arrive parfois que le droit à la formation de l'agent soit également assorti de contraintes pour celui-ci. Par ailleurs, dans certains cas, l'agent va être débiteur, vis-à-vis de son employeur, d'une obligation de se former et l'irrespect de cette obligation pourra être sanctionné. En effet, la formation est également parfois une obligation pour l'agent. Une obligation légale tout d'abord puisque l'article 22 de la loi Le Pors dispose que : « *ceux-ci peuvent être tenus de suivre des actions de formation professionnelle dans les conditions fixées par les statuts particuliers.* » Mais avant cette modification de la loi Le Pors, intervenue en 2007, la jurisprudence avait déjà précisé qu'une administration pouvait imposer à un agent une formation en rapport avec ses fonctions exercées[897].

731. Par ailleurs, les fonctionnaires sont tenus, par principe, à une obligation d'obéissance hiérarchique. Ainsi, le refus par un agent d'assister à une formation qui lui est imposée par son supérieur hiérarchique pourrait conduire à des sanctions disciplinaires. A titre d'exemple, dans une décision en date du 9 avril 2009, la Cour Administrative de Nancy[898] a eu à se prononcer sur une décision de blâme prononcé à l'encontre d'un fonctionnaire qui avait refusé une formation. En l'espèce, il s'agissait d'un caporal-chef des sapeurs-pompiers professionnel, qui avait refusé de participer à la première séance de formation instituée par une décision du conseil d'administration du service départemental d'incendie et de secours de la Moselle. Il ressortait également des éléments du dossier que cet agent avait par ailleurs incité ses collègues à refuser cette formation. Un blâme lui a été infligé par son employeur. La Cour Administrative d'Appel a considéré que cette sanction disciplinaire n'était pas entachée d'erreur manifeste d'appréciation.

A noter qu'en droit privé, l'obligation de formation pèse également lourdement sur le salarié, qui est tenu de se former dans le cadre de l'exécution de son contrat de travail. Par exemple, la jurisprudence a déjà reconnu qu'un salarié qui refusait une formation proposée par son employeur afin d'assurer le maintien de ce salarié dans son emploi, pouvait être licencié pour motif disciplinaire[899].

---

[897] ANTOINE, Dominique. « La formation professionnelle dans la fonction publique en France – Compte rendu d'un rapport de la promotion René Cassin de l'ENA », *RF adm. publ*., 2002, n° 104, p. 611.
[898] CAA de Nancy, 9 avril 2009, n° 08NC00449.
[899] *V*. notamment en ce sens, Cass. Soc. 12 mai 2004, n° 02-40772 ; Cass. Soc. 18 mars 2009, n° 08-40378.

2) La formation professionnelle, un outil managérial stratégique

732. Les dispositions de l'article 1er du décret de 2008[900] précise que « *la formation professionnelle tout au long de la vie des agents titulaires et non titulaires de la fonction publique hospitalière a pour but de leur permettre d'exercer efficacement leurs fonctions durant l'ensemble de leur carrière, d'améliorer la qualité du service public hospitalier, de favoriser leur développement professionnel et personnel et leur mobilité. Elle contribue à créer les conditions d'un égal accès aux différents grades et emplois entre les hommes et les femmes.* »

733. La formation professionnelle continue présente de nombreux avantages managériaux. Elle permet notamment aux agents d'adapter leurs compétences aux nouvelles exigences des emplois, et notamment aux exigences des nouveaux outils[901]. En cela, la formation professionnelle « *participe à la qualité et à la mutabilité du service public* »[902], puisqu'elle permet l'évolution des agents, de leurs compétences et éventuellement de leurs postes. La formation professionnelle permet également à l'employeur d'améliorer la gestion des ressources humaines[903]. Dans le cadre de l'introduction des TIC dans la pratique médicale, la formation est évidement essentielle. Elle touche par ailleurs un domaine assez vaste, ce qui peut la rendre complexe. En effet, il s'agit aussi bien de former les agents à l'utilisation des logiciels médicaux (logiciel dossier informatique, logiciel de gestion de la pharmacie, logiciel d'imagerie) que de les former aux nouvelles pratiques, comme la télémédecine. D'ailleurs en la matière, l'obligation de formation des utilisateurs est clairement actée dans le décret de 2010, faisant de celle-ci l'une des conditions préalables à la mise en œuvre d'une action de télémédecine. Ainsi, l'article R. 6316-9 du Code de la santé publique, introduit par le décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine prévoit que : « *Les organismes et les professionnels libéraux de santé qui organisent une activité de télémédecine s'assurent que les professionnels de santé et les psychologues participant aux activités de télémédecine ont la formation et les compétences techniques requises pour l'utilisation des dispositifs*

[900] Décret n° 2008-824 du 21 août 2008 relatif à la formation professionnelle tout au long de la vie des agents de la fonction publique hospitalière, *JORF* n°0196 du 23 août 2008, p. 13285.
[901] AUBIN, Emmanuel. « Les dispositions relatives à la formation professionnelle des fonctionnaires tout au long de la vie », *AJDA*, 2007, p. 511.
[902] FORTIER, Charles. « Le défi de la continuité du service public de l'éducation nationale : assurer les remplacements », *AJDA*, 2006, n° 33, pp. 1822-1829.
[903] ESPAGNO, Delphine. « La formation professionnelle, enjeu de la modernisation de la fonction publique », *AJFP*, 2007, p. 116.

correspondants ». Le texte va même plus loin puisqu'il fait également peser, sur les établissements de santé comme sur les professionnels libéraux organisant une activité de télémédecine, une obligation de formation vis-à-vis des patients[904].

734. En termes de management, la formation est un levier important qui présente plusieurs avantages pour l'employeur. D'abord elle assure à l'employeur un gain de performance. En effet, en permettant à ses agents de mettre à jour, d'acquérir ou de perfectionner les compétences techniques nécessaires à son poste, il s'assure que ses agents soient toujours adaptés à leur poste et donc productifs. Toujours dans cette logique, la formation va permettre à l'employeur de s'assurer que son agent s'adapte aux évolutions qui interviennent sur son poste ou, dans le cas qui nous intéresse, sur les outils utilisés. Enfin, la formation professionnelle des agents à l'utilisation des TIC va permettre à l'employeur de sécuriser les pratiques, en limitant les risques de mésusages ou de mauvaise utilisation. Il s'agit ici pour l'employeur d'un moyen d'anticiper au mieux les risques liés à une mauvaise utilisation des TIC par ses agents.

B. La sanction d'une mauvaise utilisation des TIC

735. Au sein de la fonction publique hospitalière, la procédure disciplinaire est encadrée de manière très stricte par les textes réglementaires (1). Mais, sous réserve du respect de cette procédure, le Directeur d'établissement, en tant qu'autorité détentrice du pouvoir de nomination, sera libre de prononcer une sanction disciplinaire à l'encontre de l'un de ses agents, si cela s'avère nécessaire (2). Dans le cadre de l'utilisation des TIC dans la pratique médicale, ce pouvoir permettra de sanctionner le non-respect de leurs obligations déontologiques par les agents, mais également une éventuelle utilisation des TIC qui ne serait pas en accord avec les règles applicables, que celles-ci soient issues des textes législatifs et réglementaires, ou simplement des règles internes, tel que nous l'avons vu précédemment.

[904] Article R. 6316-3 du Code de la santé publique : « *Lorsque la situation l'impose, la formation ou la préparation du patient à l'utilisation du dispositif de télémédecine* ».

1) Le cadre d'exercice du pouvoir disciplinaire

736. Au terme des dispositions de la loi Le Pors, les agents publics disposent de droits, mais ils sont également soumis à plusieurs obligations professionnelles et déontologiques. Celles-ci ont d'ailleurs été renforcées par la loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires[905]. La violation de ces obligations constitue alors une faute qui peut être sanctionnée disciplinairement. Par principe, c'est à l'autorité investie du pouvoir de nomination, à savoir, le directeur d'établissement, qu'il appartient de mettre en place, s'il l'estime opportun, une procédure disciplinaire. Cette procédure s'organise dans un cadre précis et strict, et la décision de sanction disciplinaire pourra être soumise à l'appréciation du juge administratif.

737. L'ensemble de la procédure disciplinaire va être dirigée par le respect du principe du contradictoire. A chaque étape de la procédure, l'agent devra avoir connaissance des faits qui lui sont reprochés et pourra également accéder à l'ensemble des documents écrits venant étayer ces faits (rapports écrits, témoignages ou tout autre élément de preuve). D'ailleurs, le droit d'obtenir communication de son dossier administratif est un droit fondamental de l'agent mis en cause, tout comme celui de se faire assister par la personne de son choix. L'absence du respect du contradictoire, empêchant l'agent de pouvoir préparer correctement sa défense, est régulièrement sanctionné par le juge administratif[906]. Pour certaines sanctions envisagées (les sanctions du deuxième, troisième et quatrième groupe[907]), la saisine de la Commission

---

[905] Loi n° 2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires, *JORF* n°0094, 21 avril 2016.

[906] *V.* notamment en ce sens : CE, 5 mai 1944, Dame veuve Trompier-Gravier, n° 69751, Rec., p. 133. Dans cet arrêt, la Haute juridiction précise qu'en cas de sanction administrative ou disciplinaire, un agent qui n'a pas été invité à présenter ses moyens de défense, est fondée à soutenir que la décision attaquée a été prise dans des conditions irrégulières et est entachée d'excès de pouvoir ; CAA Versailles, 19 février 2009, n 07VE02328. A l'occasion de cette décision, les juges ont précisé que dans le cadre d'une procédure disciplinaire, le rapport disciplinaire doit être communiqué à l'agent et ne doit pas se référer à d'autres éléments non versés au dossier de l'agent ; CE, 21 novembre 2012, M. A C/ la communauté de communes du Grand Cahors, n° 345140. Cet arrêt précise que dans le cadre d'une procédure de discipline, un agent doit être invité, dans un délai de nature à lui permettre d'assurer sa défense, à prendre connaissance du rapport qui saisit de son cas le conseil de discipline. A défaut, la procédure de discipline engagée est irrégulière.

[907] L'article 81 de la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière prévoit que : « *les sanctions disciplinaires sont réparties en quatre groupes : Premier groupe : L'avertissement, le blâme ; Deuxième groupe : La radiation du tableau d'avancement, l'abaissement d'échelon, l'exclusion temporaire de fonctions pour une durée maximale de quinze jours ; Troisième groupe : La rétrogradation, l'exclusion temporaire de fonctions pour une durée de trois mois à deux ans ; Quatrième groupe : La mise à la retraite d'office, la révocation. Parmi les sanctions du premier groupe, seul le blâme est inscrit au dossier du fonctionnaire. Il est effacé automatiquement du dossier au bout de trois ans si aucune sanction n'est intervenue pendant cette période. L'exclusion temporaire de fonctions, qui est privative de toute rémunération,*

Administrative Paritaire Locale, réunie en Conseil de discipline, est obligatoire. Celui-ci rendra un avis, qui n'aura qu'une valeur consultative. La décision finale sera rendue par le directeur d'établissement.

2) La sanction d'un mésusage des TIC

738. La jurisprudence relative aux sanctions du fait d'une mauvaise utilisation des TIC est assez fournie. Elle se base principalement sur des violations par les agents publics de leurs obligations fondamentales telles que définies au sein de la loi Le Pors. En effet, même dans le cadre de l'utilisation des TIC, les agents demeurent soumis au respect du secret professionnel, de la confidentialité mais également débiteur d'une obligation de neutralité et de laïcité.
C'est souvent la violation de ces obligations qui amène à des sanctions, les TIC n'étant qu'un moyen comme un autre ayant amené la réalisation de la faute. Ainsi, il a été jugé qu'un enseignant qui portait à la connaissance de collègues des éléments considérés comme confidentiels par le biais d'un message électronique manque à son obligation de discrétion professionnelle et l'avertissement prononcé à son encontre à cette occasion n'est pas, aux yeux du juge administratif, une sanction disproportionnée au regard des faits[908].

739. Toujours en ce qui concerne l'usage de la messagerie, l'employeur pourra sanctionner les agents qui auront envoyé depuis leur messagerie professionnelle des courriels ne respectant pas leurs obligations déontologiques. Ainsi, le manquement à l'obligation de discrétion professionnelle[909], à l'obligation de réserve[910] ou même le manquement à l'obligation d'obéissance hiérarchique[911], pourront être sanctionnés. Enfin, tout comme un employeur sera sanctionné dans l'hypothèse d'une violation du secret des correspondances de

---

peut être assortie d'un sursis total ou partiel. Celui-ci ne peut avoir pour effet, dans le cas de l'exclusion temporaire de fonctions du troisième groupe, de ramener la durée de cette exclusion à moins de un mois. L'intervention d'une sanction disciplinaire des deuxième ou troisième groupes pendant une période de cinq ans après le prononcé de l'exclusion temporaire entraîne la révocation du sursis. En revanche, si aucune sanction disciplinaire autre que l'avertissement ou le blâme n'a été prononcée durant cette même période à l'encontre de l'intéressé, ce dernier est dispensé définitivement de l'accomplissement de la partie de la sanction pour laquelle il a bénéficié du sursis. »

[908] CAA Nantes, 8 mars 2007, n° 06NT01199.

[909] *Ibid*. Sanction de 1er groupe (avertissement) prononcée à l'encontre d'un enseignant qui avait révélé des éléments relatifs à la notation des épreuves de mathématiques au baccalauréat.

[910] CAA Paris, 21 novembre 2006, n° 04PA00634.

[911] CAA Nancy, 2 août 2007, Cne Lons-Le-Saunier, n° 07NC00217. A cette occasion, les magistrats ont rappelé que le fait pour un agent de ne pas respecter les prescriptions en matière d'utilisation de la messagerie professionnelles fixées par une note de service peut donner lieu à sanction disciplinaire, pour désobéissance hiérarchique.

sa part, un agent qui ne respecterait pas le secret des correspondances privées, pourra être sanctionné disciplinairement.

740. Ainsi, la jurisprudence a eu plusieurs fois l'occasion de se prononcer sur le caractère fautif de l'accès par un agent à la messagerie d'un de ses collègues. Le Conseil d'Etat, dans une décision du 13 mai 2005[912], est venu confirmer la sanction d'exclusion temporaire des fonctions pour une durée de deux ans, prononcée à l'encontre d'un inspecteur général de l'éducation nationale. En l'espèce, l'agent sanctionné, chargé de présider le concours du CAPES d'allemand, s'était connecté à plusieurs reprises à la messagerie électronique de l'inspecteur chargé de présider le concours du CAPES d'anglais. Ayant pris connaissance des sujets à cette occasion, il avait ensuite créé une adresse électronique à partir de laquelle il avait faussement informé la direction en charge de l'organisation du concours que des candidats avaient pu se procurer les sujets.

Le mésusage des TIC à l'hôpital pourra donc donner lieu à sanctions disciplinaires de la part de l'employeur.

[912] CE, juge des référés, 16 mai 2005, n° 280166, JurisData n° 2005-068570.

Conclusion de la section

741. Les établissements de santé disposent d'un panel d'outils leur permettant de sécuriser la mise ne place et surtout l'utilisation des TIC en leur sein.
D'abord, ils peuvent avoir recours à des outils juridiques. C'est le cas notamment de la charte informatique, qui leur permettra d'acter un certain nombre de règles qu'ils souhaitent voir s'appliquer en la matière. Ces chartes sont souvent accompagnées d'un contrôle et d'une limitation de l'utilisation des outils informatiques par les agents.

Par ailleurs, les établissements de santé peuvent également utiliser des outils managériaux qui vont leur permettre d'accompagner l'utilisation progressive des TIC mais également de sanctionner en cas de comportement déviant.

L'accompagnement de l'intégration des TIC à la pratique professionnelle se fera par le biais de la formation aux outils et notamment grâce à la formation professionnelle continue des agents. La possibilité de sanctionner un comportement déviant est quant à elle accordée au directeur de l'établissement, en tant qu'autorité détentrice du pouvoir de nomination. A ce titre, il pourra prononcer des sanctions disciplinaires à l'encontre d'un agent.

Conclusion du chapitre

742. Les établissements de santé peuvent être les acteurs de la sécurisation de l'utilisation des TIC en leur sein, en intervenant, à chaque étape de la vie des TIC dans l'établissement, que cela soit au moment du développement, au moment de la mise en place ou encore lors de leur utilisation courante, afin de sécuriser les pratiques.

743. En amont, lors du développement et de la mise en place des TIC, les établissements vont pouvoir gérer de manière stratégique le développement de leur SIH. Il est en effet essentiel pour les établissements de santé que la mise en place de leur SIH devienne un projet à part entière, intégré au projet global de l'établissement. Car le SIH n'est pas une quantité négligeable qui pourra s'adapter aux pratiques le moment venu. Il s'agit au contraire aujourd'hui d'un outil stratégique essentiel, auquel les pratiques actuelles vont devoir s'adapter. Afin de gérer au mieux ce projet, les établissements peuvent d'entourer d'experts du domaine. Deux choix s'offrent alors à eux : embaucher directement ces ressources, ou faire appel à des prestations de service auprès de sociétés spécialisées. Dans les faits, les établissements de santé auront intérêt à cumuler les deux solutions.

Puis, une fois les TIC mises en place, les établissements de santé vont pouvoir sécuriser leur utilisation par le biais d'outils juridiques et d'outils managériaux. Ainsi, la mise en place d'une charte informatique permettra d'encadrer au mieux l'utilisation des TIC. Par ailleurs, par le biais de la formation, les établissements de santé pourront accompagner leurs agents dans l'utilisation de ces nouveaux outils et donc l'évolution de leurs pratiques professionnelles. Enfin, dans l'hypothèse d'une utilisation des TIC qui ne serait pas en adéquation avec les obligations professionnelles des agents ou avec la charte informatique de l'établissement, le directeur pourra sanctionner disciplinairement l'agent fautif.

A l'instar du CHRU de Lille, qui s'est engagé pleinement dans l'accompagnement et le suivi du développement de l'informatisation des pratiques médicales en son sein, les établissements de santé, en s'inscrivant dans une telle démarche, en tireront de sérieux bénéfices.

Chapitre 2

Un exemple de sécurisation réussie : le CHRU de Lille

744. Le Centre Hospitalier Régional Universitaire de Lille (CHRU) est un des plus grands CHRU de France, régulièrement classé parmi les trois meilleurs hôpitaux de France par les différents palmarès des hôpitaux[913], et positionné au 3ème rang français pour les études et les essais cliniques (SIGREC). En 2013, le CHRU de Lille disposait d'une capacité d'un peu plus de 3000 lits. Son activité représentait 199 956 prises en charge en hospitalisation, 1 401 291 venues en consultation. En termes de moyens humains, le CHRU emploie 15 303 professionnels, dont 7592 soignants et 3576 médecins actifs ou en formation.

745. Le CHRU de Lille intervient au sein d'une région qui, avec environ 4 millions d'habitants, se caractérise par une des plus importantes densités de population en France. Il représente un centre de recours essentiel au sein d'une région où les indicateurs de santé de la population sont en-deçà de la moyenne nationale. Le CHRU de Lille assure également un rôle majeur dans la permanence des soins, notamment grâce à son service d'urgence qui a comptabilisé, en 2013 plus de 88 000 passages. Enfin, pour certaines activités de haute spécialisation, le CHRU de Lille est le seul établissement de prise en charge pour le Nord-Pas-de-Calais voire, de l'interrégion Nord-Ouest

746. Le CHRU de Lille s'attache à être au cœur des innovations technologiques, en acquérant un équipement de pointe et en renouvelant régulièrement son parc d'équipement biomédical. Il s'engage également dans le développement de l'utilisation des TIC, et plus particulièrement dans le cadre de la télémédecine, en développant une politique active en la matière. En effet, dès 1991, il a mis en place une équipe dédiée au développement des projets de télémédecine dans la région. Aujourd'hui de nombreux réseaux de télémédecine ont été mis en œuvre (TELURGE, TELEEG, TELEIMAGERIE, LOGINAT, Flandre Ophtalmo) et de nouveaux projets sont actuellement à l'étude. C'est dans ce contexte particulier que l'établissement doit, aujourd'hui, développer un SIH efficient, sécurisé et pérenne.

---

[913] *V.* notamment le classement effectué par Le Point chaque année. Disponible sur [http://www.lepoint.fr], consulté le 20 mars 2017.

747. En 2016, le CHRU de Lille, ainsi que 40 autres établissements publics de santé, ont été ciblés par la Cour des comptes pour une étude de leur système d'information[914]. Ce contrôle du CHRU de Lille a fait l'objet d'un rapport, rendu en juillet 2016, qui a servi à alimenter l'étude nationale de la Cour des comptes sur l'état du développement des SIH. Ce fut l'occasion pour l'établissement d'effectuer son propre bilan. Ainsi, d'une manière générale, l'organisation interne du CHRU, qu'il s'agisse de la gouvernance de son SIH ou des projets qu'il développe, démontre la volonté de l'établissement de sécuriser l'utilisation des TIC en santé en son sein (Section I). Par ailleurs, le CHRU de Lille porte une attention toute particulière à la protection des données informatisées (Section II).

[914] Cour des comptes, « La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer », rapport annuel de la Cour des comptes sur l'application des lois de financement de la sécurité sociale, 2016.

Section 1. Une volonté marquée de sécuriser l'utilisation des TIC en santé

748. Afin de développer une offre de soins performante, le CHRU de Lille s'appuie de plus en plus fortement sur son SIH qui est devenu un outil indispensable à tous les professionnels dans leurs relations avec les patients mais également entre eux. Le SIH est également un outil précieux dans la mise en place et le maintien de liens avec les professionnels et partenaires extérieurs. Dans ce contexte, le développement d'un SIH sécurisé est un enjeu fondamental pour le CHRU de Lille, qui doit assurer aux patients la sécurité des soins dispensés et la confidentialité des données qui les concernent mais également garantir aux professionnels de santé la disponibilité de leurs outils informatiques.

C'est pourquoi le CHRU de Lille a choisi de structurer une partie de son organisation autour de la sécurité du SIH (Paragraphe I), tout en veillant à diffuser, en son sein, une culture de la sécurité informatique (Paragraphe II).

§1. Une organisation interne tournée vers la sécurité du SIH

749. Le CHRU de Lille a très vite fait le choix de mettre en place une stratégie liée au développement de son SIH. A l'occasion de la réflexion portant sur le nouveau projet d'établissement (projet 2012-2016), des dysfonctionnements liés à la gestion des projets informatiques avaient été constatés[915]. L'organisation a alors été repensée (A) afin de permettre au CHRU de Lille de mettre en place une gestion optimale des projets liés au développement de son SIH. D'ailleurs, en matière de sécurité du SIH, le CHRU a eu l'occasion de développer plusieurs projets ambitieux (B), sur lesquels il est intéressant de s'arrêter.

[915] Chambre régionale des comptes, « CHRU de Lille, enquête système d'information hospitalier », rapport d'observations définitives, mars 2016, p. 9.

A. Présentation de l'organisation du CHRU en matière de SIH

750. Le CHRU de Lille a à cœur de s'assurer de la sécurité de son système d'information afin de garantir notamment la confidentialité des données de santé de ses patients. Par ailleurs, son statut de centre de recours et d'opérateur d'importance vitale au sens de la protection civile lui impose de fortes exigences en matière de sécurité et de disponibilité de ses équipements.

Depuis plusieurs années, son organisation interne reflète cette volonté de sécuriser les pratiques en matière de TIC en santé. En matière de gestion de son SIH, il a ainsi mis en place une gouvernance axée autour de trois instances (1) et s'est doté de ressources spécifiques en matière de sécurité. Par ailleurs, le CHRU de Lille a construit une véritable stratégie autour du développement de son SIH (2).

1) La gouvernance du SIH

751. Le CHRU de Lille a mis en place un schéma de gouvernance de la politique du système d'information composé de trois instances : le Département des Ressources Numériques (DRN) en charge du fonctionnement et de la cohérence du SIH ; le Comité Stratégique du Système d'Information (CSSI), composé de membres de la Direction et en charge de vérifier la cohérence stratégique du SIH avec l'ensemble des objectifs de l'établissement et enfin le Comité Opérationnel du Système d'Information (COSI), qui vérifie que les applications développées répondent correctement aux besoins des utilisateurs afin d'être réellement utilisées.

Le COSI et le CSSI ont été particulièrement actifs lors de l'élaboration du Schéma Directeur des Systèmes d'Information (SDSI) du CHRU de Lille. Cependant, une fois ce schéma mis en place, ces instances se sont moins réunies[916].La Chambre régionale des comptes relève dans son rapport que le CSSI, contrairement à son objectif affiché, ne remplit pas son rôle de priorisation des projets et n'est qu'une instance de validation des propositions formulées par le COSI. A titre d'exemple, le CSSI n'a jamais fait appel à des expertises ou analyses, grâce auxquelles il aurait pu se prononcer sur la priorisation des projets, à l'appui de

[916] *Id.*, p. 10.

critères techniques ou économiques objectivés. La Chambre a d'ailleurs préconisé de revoir cette organisation à l'occasion de la mise en place du prochain projet d'établissement du CHRU de Lille[917].

752. Le DRN pour sa part est le fruit d'une récente réorganisation. Ainsi, l'ancienne Direction des Systèmes d'Information (DSI) du CHRU de Lille a été réorganisée et a disparu au profit d'une délégation, directement rattachée au Directeur général. Cette réorganisation a eu pour objectif de donner plus de visibilité aux chefs de projet informatique en créant notamment une sous-direction dédiée.

753. Par ailleurs, le CHRU de Lille dispose d'un Responsable de la Sécurité du Système d'Information (RSSI), qui a la particularité d'avoir également la casquette de Correspondant Informatique et Liberté (CIL). Ce dernier travaille en étroite collaboration avec la Direction des Affaires Juridiques (DAJ). Il a en charge la conception et l'animation de la démarche sécurité du SIH, en veillant notamment à ce que les niveaux de sécurité soient conformes à la réglementation et aux normes applicables en la matière. C'est à lui qu'il revient de garantir la sécurité, la disponibilité et l'intégrité du SIH de l'établissement.

Au CHRU de Lille, le RSSI est accompagné dans ses missions par un prestataire extérieur, dans le cadre notamment de la démarche SMSSI engagée par le CHRU de Lille dès 2011[918]. Son rôle est essentiel puisque c'est lui qui sera garant de la cohérence des projets envisagés avec la réglementation applicable dans le domaine de la sécurité informatique. A ce titre, il valide, par exemple, l'ensemble des conventions passées avec des prestataires de service informatique, sur le volet sécurité.

754. Enfin, de manière ponctuelle, la DRN fait appel à la DAJ afin de sécuriser certains projets. A titre d'exemple, la DAJ a eu l'occasion d'aider à la rédaction des conventions de télémédecine, lors de la mise en place ou du renouvellement de certains réseaux de télémédecine. D'ailleurs, la DAJ est représentée dans la plupart des comités de pilotages des projets informatique (COPIL télémédecine ou COPIL dossier patient par exemple) ou, *a minima*, associée au titre d'expert.

---

[917] Chambre régionale des comptes, « CHRU de Lille, enquête système d'information hospitalier », *op. cit.*, p. 9.
[918] *V. Infra.* n° 760 à 763.

2) La gestion stratégique du SIH

755. Le CHRU de Lille a souhaité gérer de manière stratégique le développement de son SIH. Pour cela, il a fait le choix de développer un projet consacré au SIH, faisant partie intégrante du projet d'établissement 2012-2016. Ainsi, dans ce cadre, le volet "système d'information" du projet d'établissement est venu définir les orientations stratégiques du CHRU de Lille en matière de système d'information, orientations elles-mêmes déclinées dans le cadre du Schéma Directeur du Système d'Information (SDSI).

Ce schéma directeur a pour ambition de définir les cibles à atteindre afin de soutenir les objectifs stratégiques de l'établissement en matière de SI, tout en tenant compte des besoins exprimés par les utilisateurs. Ceux-ci avaient d'ailleurs été recensés en amont de l'élaboration du projet SIH, par le COSI. Le SDSI permet également d'établir un plan d'action permettant d'atteindre la cible fixée, par le bais d'une mise en œuvre progressive mais pérenne du SIH. Par ailleurs, cela garantit une cohérence de l'ensemble du SIH.

756. Afin d'élaborer le SDSI, le CHRU de Lille a défini huit orientations stratégiques, elles-mêmes déclinées en objectifs opérationnels. Bien évidemment, la première orientation fixée concerne l'amélioration de la qualité et de la sécurité de prise en charge du patient et l'aide à la prise de décision médicale et soignante par le biais du système d'information hospitalier. Le but ici est de développer la prise en charge des patients par le biais des TIC en développant notamment les logiciels d'aide à la décision médicale, mais également la prescription informatisée, dans le cadre du circuit du médicament. La deuxième orientation concerne le développement d'un SIH contribuant à la performance médico-économique de l'établissement. En effet, faciliter la diffusion de données fiables dans le cadre du PMSI est un enjeu stratégique important pour l'établissement de santé. Le développement d'un SIH efficace en la matière est donc nécessaire. La troisième orientation concerne le patient de manière plus directe puisqu'il s'agit, pour le SIH, de permettre au patient d'être un acteur de sa prise en charge et de proposer une prise en charge personnalisée et globale. A ce titre, le CHRU de Lille s'est engagé dans la création et la mise en place d'une plate-forme patient, accessible depuis Internet, et par laquelle les patients pourront prendre des RDV en ligne.
Le système d'information doit également permettre de faciliter la continuité d'accès, notamment à l'extérieur de l'établissement (orientation n° 4), venir en appui des activités de recherche des professionnels de l'établissement (orientation n° 5) et permettre à

l'établissement de remplir sa mission hospitalo-universitaire en matière d'enseignement (orientation n° 6). D'une manière plus pratique, le SIH doit garantir la sécurité des données et pouvoir fonctionner en continue afin que les applications soient toujours accessibles (orientation n° 7). Enfin, le CHRU doit mettre en place un SIH ergonomique pour ses agents, afin d'améliorer leurs conditions de travail (orientation n° 8).

L'ensemble de ces orientations ont été mises en œuvre aux travers, notamment, du développement de cinq projets informatiques identifiés comme étant prioritaires : le projet "Circuit informatisé du médicament et des produits de santé", le projet "Informatisation de la production de soins, le projet "Système d'Archive et de Partage des Images (PACS)", le projet "Informatisation des blocs opératoires et des sites interventionnels" et le projet "Multimédia au lit du patient".

B. Le développement de projets ambitieux relatifs à la sécurité

757. Conscient des enjeux mais également des fortes responsabilités qui pèsent sur lui en matière de sécurité informatique, le CHRU de Lille a fait le choix de développer des projets ambitieux en matière de sécurité du SIH.

Il nous semble utile de nous attarder plus particulièrement sur deux d'entre eux, qui ont particulièrement modifié l'organisation du CHRU en termes de sécurité informatique : le projet "carte d'établissement", d'une part (1), et le projet Système de Management de la Sécurité des Systèmes d'Information (SMSSI), d'autre part (2).

1) Le projet carte d'établissement

758. Comme nous avons pu le constater, pendant longtemps, le législateur exigeait l'utilisation de la Carte de Professionnel de Santé (CPS) pour la transmission de données de santé par voie électronique. Afin de se mettre en conformité avec les dispositions du décret "confidentialité", le CHRU de Lille s'est engagé dès 2007 dans le déploiement d'une carte d'établissement. Cette carte a pour objectif initial de concilier les exigences des textes de loi et les contraintes du fonctionnement hospitalier. Ainsi, la carte d'établissement devait se substituer à la CPS, grâce à des certificats constituant en quelque sorte une version dématérialisée de la CPS, et embarqués sur la carte d'établissement. Dans ce cadre, le CHRU

de Lille était le site pilote national d'une démarche d'expérimentation menée par le Groupement pour la Modernisation des Système d'Information Hospitalier (GMSIH), le Groupement d'Intérêt Public des Cartes de Professionnels de Santé (GIP CPS) et la Direction de l'Hospitalisation et de l'Organisation du Soin (DHOS).

759. Cette carte magnétique est une carte multi-usage qui contrôle l'accès au système d'information, permet l'identification, l'authentification et la traçabilité des accès au sein des différentes applications informatiques. Mais elle permet également un accès aux parkings, aux bâtiments dont l'accès est limité et au self. Déployée de manière très large sur l'établissement, cette carte est aujourd'hui remise de manière systématique aux nouveaux employés, accompagnée de la charte d'utilisation de cette carte, qui doit être signée. En pratique, la carte d'établissement permet non seulement de sécuriser l'accès au SIH et aux données qu'il contient mais également d'assurer la traçabilité des actions réalisées au sein des différents logiciels qui composent le SIH. Enfin, elle permet aussi de signer électroniquement les documents et de gérer plus facilement l'ensemble des droits d'accès accordés aux agents.

Un second projet mis en place par le CHRU de Lille a également retenu notre attention.

2) Le projet Système de Management de la Sécurité du Système d'information (SMSSI)

760. Le Système de Management de la Sécurité du Système d'Information est un système de gestion de l'ensemble des politiques mises en place dans le cadre de la sécurité du SIH.
Ce système permet de mettre en œuvre une démarche ayant pour but de maîtriser la sécurité du SIH. Le SMSSI permet de garantir la disponibilité et l'intégrité du SIH, mais également de garantir la confidentialité des données sensibles et des traces informatiques. Il permet également de faciliter les démarches de certification de l'établissement (la sécurité du SI est en effet évaluée au travers du critère 5b). En termes d'affichage enfin, le SMSSI permet de démontrer l'effort de l'établissement dans la garantie de la sécurité de son SIH.

761. Par principe, un SMSSI est élaboré selon une norme. La plus connue en la matière, et celle actuellement mise en œuvre au CHRU de Lille, est la norme ISO 27001. Au CHRU de Lille, le projet SMSSI a été amorcé en 2011. Il a démarré par une phase d'étude de 2011 à 2013, pendant laquelle un diagnostic et une analyse des risques ont été réalisés. Cette analyse

a été réalisée à partir d'un diagnostic technique ainsi que des besoins de sécurité identifiés lors des différentes réunions de travail organisées par l'équipe de prestataire en charge du projet, avec les différents services du CHRU de Lille. A l'issue de cette analyse a été dressée une cartographie des risques de sécurité liés aux différentes activités (production de soin, facturation, …) et aux données du CHRU de Lille.

762. L'ensemble des travaux menés dans le cadre du projet SMSSI a permis d'élaborer un référentiel de sécurité, qui présente les enjeux de la démarche sécurité, les rôles et responsabilité de l'ensemble des acteurs ainsi que les règles de sécurité du SIH. Ce référentiel sécurité se compose de trois documents : la Politique Générale du Système d'Information (PGSSI) qui fixe les principes applicables en matière de gouvernance de la sécurité du SIH ; les politiques opérationnelles, qui fixent les règles de sécurité et la charte d'utilisation du SIH, qui rappelle les droits et obligations des utilisateurs du SIH. Par ailleurs, ce projet a été l'occasion de proposer une méthodologie d'intégration de la sécurité dans les projets permettant de garantir un niveau de sécurité équivalent pour l'ensemble des projets développés. Désormais, l'ensemble des projets informatiques doivent donc être soumis à l'équipe en charge de la sécurité afin de réaliser une analyse de risques préalable. Cela permet donc d'assurer une amélioration continue de la sécurité du SIH au CHRU de Lille.

763. Cette démarche SMSSI est aujourd'hui renforcée par les nouvelles obligations règlementaires qui pèsent sur les établissements de santé en matière de sécurité de leur SIH. En effet, face aux menaces pesant sur les SIH des établissements de santé, et suite à quelques incidents graves de sécurité[919], le législateur est venu renforcer le cadre juridique applicable en la matière. Ainsi, la loi de modernisation de notre système de santé[920] a introduit au sein du Code de la santé publique un article L 1111-8-2 qui prévoit que « *les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information* ». Le décret n°2016-1214 du 12 septembre 2016 relatif aux conditions

[919] Selon le Ministère des Affaires Sociales, plus de 1300 attaques informatiques contre des établissements de santé ont été recensées en 2015, dont 18 attaques ciblées. Chiffres disponibles sur [http://www.ticsante.com], consultés le 20 mars 2017. Les établissements de santé sont particulièrement ciblés par les attaques de type "ranconware", qui visent à paralyser l'ensemble du SIH et bloquer l'accès aux données tant que n'est pas versée une rançon.

[920] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *JORF* n° 0022 du 27 janvier 2016, texte n° 1.

selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information[921] précise, quant à lui, les conditions et modalités de mise en œuvre du signalement des incidents graves de sécurité des systèmes d'information. Selon ce texte, « *sont considérés comme incidents graves de sécurité des systèmes d'information les événements générateurs d'une situation exceptionnelle au sein d'un établissement, organisme ou service, et notamment : les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins ; les incidents ayant des conséquences sur la confidentialité ou l'intégrité des données de santé ; les incidents portant atteinte au fonctionnement normal de l'établissement, de l'organisme ou du service* ». Nous ne pouvons toutefois que constater le caractère imprécis de la définition de la notion d'incident grave. Le RSSI aura donc un rôle majeur à jouer dans ce cadre, puisqu'il lui appartiendra de conseiller le directeur général de l'établissement, en charge de la déclaration des incidents auprès de l'ARS. Celle-ci, pour sa part, sera chargée de faire remonter auprès de l'ASIP santé, parmi ces incidents, ceux qu'elle aura qualifié de significatifs, c'est-à-dire ceux « *ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé et les incidents susceptibles de toucher d'autres établissements, organismes ou services* ». A noter que ces dispositions n'entreront en vigueur qu'à compter du 1er octobre 2017.

Le projet SMSSI est donc un projet majeur du CHRU de Lille dans la sécurisation de son SIH.

[921] Décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information, *JORF* n°0214 du 14 septembre 2016, texte n° 15.

§2. La diffusion d'une culture de la sécurité informatique

764. La sécurité du SIH n'est pas seulement l'affaire du directeur de l'établissement de santé. Tous les utilisateurs du SIH doivent y participer et c'est pourquoi le CHRU de Lille s'attache à diffuser une véritable culture de la sécurité informatique auprès de ses agents. Pour cela, le CHRU de Lille sensibilise au quotidien ses agents, par le biais de différentes actions de formation et de communication (A). Par ailleurs, le CHRU de Lille a mis en place une règlementation interne, par le biais de chartes informatiques, afin de rappeler aux agents leurs obligations en matière d'utilisation du SIH (B).

A. La sensibilisation des utilisateurs du SIH

Les utilisateurs du SIH du CHRU de Lille sont régulièrement sensibilisés aux enjeux liés à la sécurité. Cette sensibilisation passe par des actions de formation (1), mais également par des actions de communications ciblées (2).

1) Les formations

765. Le CHRU de Lille a souhaité sensibiliser ses agents à la question de la sécurité du SIH et aux risques encourus en cas de mauvaises pratiques. Ces formations ont pris plusieurs formes, afin de toucher le plus grand nombre d'agents.

D'abord, à chaque journée d'accueil des nouveaux recrutés, ainsi qu'à la session d'accueil des nouveaux internes, une présentation relative aux bons usages des outils informatiques et, notamment, de la carte d'établissement, est réalisée. Les principes de base liés à la sécurité du SIH (mot de passe fort, ne pas prêter ses identifiants, …) sont alors rappelés.

Puis, de manière ponctuelle, la Direction des Affaires Juridiques est amenée à dispenser des formations sur ce sujet. Celles-ci ont plutôt pour but de rappeler aux agents les règles applicables en matière de confidentialité et de secret professionnel, dans le cadre de l'usage des TIC en santé. Ces formations sont programmées en fonction des demandes des

services, et peuvent être adaptées, soit au public concerné, soit aux problématiques rencontrées par le service. Cette formule permet plus de souplesse, mais aussi une meilleure réactivité face aux besoins des équipes. Elle permet également d'adapter le message délivré. A titre d'exemple, les formations suivantes ont pu être dispensées : "confidentialité et système d'information", "la confidentialité" ou encore " le secret professionnel".

En 2016, une demande plus particulière s'est développée au sein des services : la formation relative aux bons usages des réseaux sociaux. En effet, les services ont pu constater une augmentation des mésusages liés à l'utilisation des réseaux sociaux. Une offre spécifique à cette problématique s'est donc développée.

Par ailleurs en 2015, le CIL, en lien avec la Direction des Affaires Juridiques, avait proposé plusieurs sessions de formation sur la thématique "rappel des obligations en matière d'accès au dossier médical". Ces sessions avaient pour but, d'une part, de rappeler la législation applicable en matière de secret professionnel et, d'autre part, celle relative à la Loi Informatique et Libertés. Plusieurs créneaux d'une heure trente, avec inscription libre, ont été programmés. Malheureusement, cette formation n'a suscité que peu d'inscriptions et l'action n'a pas été reconduite sur 2016.

Enfin, dans le cadre de la démarche SMSSI, une plateforme e-learning dédiée à la sécurité SI a été mise à disposition des agents du CHRU de Lille, afin de les accompagner dans le développement de bonnes pratiques et les sensibiliser à la sécurité.

A ces actions de formation des agents s'ajoutent des actions de communication interne.

2) Les actions de communication

766. Le RSSI du CHRU de Lille, en lien avec son équipe sécurité et dans le cadre du projet SMSSI, organise de façon régulière des actions de communication en lien avec la sécurité du SIH. Ainsi, régulièrement, des e-mails sont transmis à l'ensemble des agents possédant une boite professionnelle, afin de leur rappeler commun réagir face à un e-mail suspect. Cette

action permet d'éviter les tentatives de *phishing*[922], ou de ranconware, en invitant les utilisateurs du SIH à signaler ce genre de courriel au RSSI.

Le RSSI a également eu l'occasion de mettre en place une campagne de communication, intitulée "l'ordinateur à l'hôpital, ce n'est pas comme à la maison", qui avait pour but de rappeler les règles de bonne utilisation des outils informatiques. De même, un espace dédié à la sécurité du système d'information a été mis en place sur le site Intranet du CHRU de Lille, regroupant notamment des fiches de bonnes pratiques de sécurité SI à destination des professionnels.

Il a également mis à disposition de ses personnels six bornes de décontamination de clés USB, avec six antivirus mis à jour tous les quarts d'heure.

L'ensemble de ces démarches permet de diffuser, au sein du CHRU de Lille, une véritable culture de la sécurité informatique. Ainsi, chaque agent participe, à son niveau, à maintenir l'intégrité, la sécurité et la confidentialité des données.

En parallèle de la sensibilisation des agents, le CHRU de Lille a souhaité rédiger des chartes informatiques.

B. La mise en place de chartes informatiques

767. En 2012, le RSSI, en lien étroit avec la Direction des Affaires Juridiques, et appuyé par une société de conseil extérieure, a rédigé quatre chartes informatiques afin d'encadrer l'utilisation du SIH. Ces chartes ont pour objet de fixer les règles d'utilisation du système d'information hospitalier. Elles ont été mises en place dans le cadre du projet SMSSI et en lien avec la Politique de Sécurité des Systèmes d'Information. Ces quatre chartes s'adressent à quatre types d'acteurs différents.

[922] Le phishing (hameçonnage ou filoutage) est une technique par laquelle des personnes malveillantes se font passer pour de grandes sociétés ou des organismes financiers qui vous sont familiers en envoyant des mèls frauduleux et récupèrent des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds. Définition du ministère de l'économie et des finances.

La première s'adresse à l'ensemble des agents du CHRU de Lille appelés à utiliser le SIH. Elle est annexée au règlement intérieur du CHRU et, à ce titre, dispose de la même force. Elle est par ailleurs accessible aux agents via l'Intranet de l'établissement. La deuxième s'oppose aux tiers, extérieurs au CHRU de Lille et qui, dans le cadre de prestations de service, seraient amenées à accéder au SIH du CHRU. Cette charte est systématiquement annexée aux contrats de prestations de service.

La troisième charte concerne une population plus spécifique puisqu'elle s'applique aux administrateurs (administrateurs des réseaux, d'applications informatiques, de bases de données,…), qu'ils soient internes au CHRU de Lille, ou prestataire de service.
Enfin, la dernière charte concerne l'infogérant du CHRU de Lille, c'est-à-dire le prestataire en charge de la gestion, l'exploitation, l'optimisation et la sécurisation du système d'information du CHRU de Lille.

768. Lors de leur mise en place, ces chartes ont toutes suivi le même processus d'élaboration et ce afin de leur conférer une force contraignante. Ainsi, elles ont fait d'abord l'objet d'une présentation, pour information, au sein de l'instance représentative du personnel de l'établissement (Comité Technique d'Etablissement). Puis, après avoir été également soumises à l'approbation du directoire, elles ont été annexées au règlement intérieur de l'établissement, et publiées sur le site Intranet de l'établissement. Ces chartes, qui constituent une source de droit dit "mou", permettent ainsi au CHRU de Lille de donner une force contraignante aux règles qu'il a souhaité mettre en place en son sein. Une violation de celles-ci pourrait entrainer une sanction disciplinaire, dans le cadre des agents, ou une rupture du contrat pour les prestataires de services.

Conclusion de section

769. Le CHRU de Lille, conscient des enjeux liés à la sécurité et au bon fonctionnement de son SIH, a mis en place une organisation tournée vers la sécurité. A l'occasion de l'élaboration de son projet d'établissement, il s'est ainsi inscrit dans une gestion stratégique du développement de son SIH, s'attachant à mettre en place un SIH à la fois efficace et sécurisé. Ainsi, sa gouvernance interne repose sur des instances en charge de la cohérence de l'ensemble des projets informatiques et l'établissement de santé a fait le choix de créer un poste de RSSI, directement en charge de la sécurité du SIH. Par ailleurs, l'ensemble du développement du SIH est pensé de manière stratégique et directement intégré au projet d'établissement. Dans ce contexte, le CHRU de Lille a notamment développé deux projets ambitieux : le projet carte d'établissement, d'une part, et le projet SMSSI, d'autre part.
Le CHRU de Lille s'attache également à sensibiliser l'ensemble des utilisateurs de son SIH aux enjeux liés à la sécurité de celui-ci. Plusieurs actions ont donc été développées dans ce sens.

D'abord, le CHRU forme ses agents régulièrement aux questions liées à la sécurité du SIH, mais également au bon respect de la confidentialité. Des campagnes de sensibilisation sont régulièrement mises en œuvre afin de rappeler régulièrement aux agents les bonnes pratiques à appliquer. Par ailleurs, il a mis en place des chartes informatiques, à valeur contraignante, afin de rappeler aux utilisateurs du SIH leurs obligations en matière d'utilisation des TIC.

Ainsi, le CHRU de Lille, de par son organisation interne, mais également au travers des différentes actions de communication et de sensibilisation qu'il mène, démontre sa volonté de sécuriser l'utilisation des TIC en santé par ses agents.

Section 2. Une volonté affirmée de protéger les données de santé

770. En tant que centre hospitalier universitaire, le CHRU de Lille est amené à produire une quantité importante de données de santé sous forme dématérialisée. Ces données, nécessaires à la bonne prise en charge des patients, présentent également un intérêt non négligeable pour la recherche en santé. Il est donc nécessaire pour le CHRU de Lille de s'assurer que la fiabilité, l'intégrité et surtout, la confidentialité de ces données soient maintenues.

En ce qui concerne plus particulièrement la confidentialité, le CHRU de Lille a fait le choix d'être innovant, et de confier cette mission à une commission créée spécifiquement pour cela. La même logique a été adoptée en ce qui concerne la gestion des démarches CNIL. (paragraphe 1). Ces commissions, et, plus particulièrement, la Commission Confidentialité de l'Information Médicale (CCIM), présentent un bilan d'action assez positif (paragraphe 2).

§1. La création de structures ad'hoc pour gérer la confidentialité des données de santé

771. Afin de répondre correctement aux nombreuses questions à la fois juridiques et techniques que pose le développement du système d'information hospitalier, et plus particulièrement la mise en place du dossier médical informatisé, le CHRU de Lille a fait le choix de créer deux commissions internes, à composition pluridisciplinaire, afin de trancher les questions en suspens.

C'est ainsi que, dans un premier temps, la commission confidentialité de l'information médicale (CCIM) a été installée en 2011 (1). Puis, dans un cadre plus spécifique, afin d'aider le CIL dans ses missions, une commission informatique et liberté a été créée en 2016 (2).

A. La Commission Confidentialité de l'Information Médicale (CCIM)

La CCIM a été créée pour répondre à un besoin accru de s'assurer de la confidentialité des données, au moment où le CHRU de Lille développait son dossier patient informatisé (1). Au fil des ans, son organisation et ses missions ont été amenées à évoluer (2).

1) Contexte de la création de la CCIM

772. En 2010, dans une logique d'informatisation croissante de la pratique médicale, le CHRU de Lille a entamé le déploiement d'un nouveau logiciel de gestion du dossier patient informatisé. Le choix opéré a été celui d'en faire le logiciel pivot du SIH, autour duquel les autres applications informatiques devront s'organiser. La mise en place de ce logiciel a alors nécessité une réflexion relative à l'attribution des droits d'accès en son sein. Non seulement ces droits devaient être en adéquation avec les besoins des différents agents, selon leur fonction, mais également avec les règles juridiques applicables en matière de secret professionnel. En théorie, il suffisait d'appliquer les règles relatives au secret partagé à l'équipe de soins tel que défini à l'article L 1110-4 du Code de la santé publique. Cependant, la traduction de ce principe juridique dans le cadre d'une matrice technique des droits d'accès s'est révélée être plus complexe que prévue.

773. Initialement, cette mission a été confiée à un groupe de travail, composé en majorité de médecins, de médecins du Département de l'Information Médicale, de techniciens de la direction des systèmes d'information, des représentants du prestataire, fournisseur de la solution logicielle et du Directeur des affaires juridiques. Ce groupe de travail a eu à préciser, pour chaque profil utilisateur, le contenu accessible, c'est-à-dire à quelles parties du dossier le profil est susceptible de donner accès et, le périmètre accessible, c'est-à-dire à quel niveau de structure ce profil permet d'accéder (ensemble de l'établissement, pôle ou service). Cette matrice des droits d'accès a été ensuite validée par l'ensemble des instances du CHRU de Lille et ce, afin de pouvoir être parfaitement opposable à l'ensemble des utilisateurs.

A l'occasion du déploiement de ce logiciel, et de l'application effective des règles d'accès, des difficultés sont apparues quant au bon respect de la confidentialité des données de santé.

Par ailleurs, alors qu'il appartenait à la commission médicale d'établissement de trancher l'ensemble des questions liées à la confidentialité des données médicales informatisées, ce

dispositif a vite montré des limites, les réponses apportées n'étant pas suffisamment concrètes et rapides. Se posaient notamment les questions concrètes relatives à la gestion des rendez-vous médicaux des détenus, visibles dans le logiciel, à l'accès aux dossiers médicaux des personnels du CHRU par leurs collègues, accès constaté de manière récurrente, ou encore à la nécessité de rendre strictement confidentiel l'accès à certains services (comme la psychiatrie ou encore les consultations médico-judiciaires).

774. En parallèle, il est très vite apparu clairement que le praticien responsable de l'information médicale[923], pour assurer au mieux son rôle de conseil auprès du Directeur Général en matière de confidentialité, devait être assisté dans ses missions. En effet, le médecin responsable de l'information médicale ne pouvait, seul, assumer ces missions de conseil, pour lesquelles une réponse juridique, éthique mais aussi technique était nécessaire. Ainsi, il a été décidé de créer une structure *ad'hoc* chargée d'analyser les interrogations portant sur la confidentialité des données médicales et de mettre en place les procédures nécessaires pour en garantir le respect.

La commission confidentialité de l'information médicale – CCIM – s'est ainsi réunie pour la première fois le 29 mars 2011.

775. Le choix a été fait de placer cette commission sous l'autorité directe du Directeur Général, étant entendu qu'elle devrait présenter un bilan de son activité devant la CME. Par ailleurs, à défaut de consensus au sein du groupe sur la solution à mettre en place, les difficultés persistantes étant soumises, pour avis, à la CME avec les solutions envisageables, de manière à ce que le Directeur Général puisse ensuite arrêter les mesures à prendre, conformément aux dispositions de l'article R. 6113-6 du Code de la santé publique. La commission s'est donc vue confier, à l'origine, un rôle de conseil et d'éclairage vis-à-vis du Directeur Général.

---

[923] Selon les dispositions de l'article R. 6113-6 du Code de la santé publique, le médecin responsable de l'information médicale conseille le directeur général de l'établissement sur la durée de conservation des archives médicales, la réception des demandes des usagers concernant leur droit d'accès et de rectification prévu par la loi informatique et libertés du 6 janvier 1978 et les droits d'accès aux données médicales nominatives ou l'élimination des dossiers archivés Par ailleurs, même si c'est au directeur général qu'il appartient, de prendre toutes dispositions utiles pour préserver la confidentialité des données médicales nominatives, notamment en ce qui concerne les d'attribution et de contrôle des autorisations d'accès, ceci doit se faire en lien avec le Président de la CME et le médecin responsable de l'information médicale.

776. Cette structure, à majorité médicale, est pilotée par le médecin responsable de l'information médicale et composée d'un médecin en charge du dossier patient, un médecin représentant du comité opérationnel du système d'information COSI, un médecin désigné par la CME, un représentant de la sous-commission qualité et sécurité des soins, un représentant de la coordination générale de soins, un représentant de la direction du système d'information hospitalier, le correspondant CNIL et un représentant de la direction des affaires juridiques . A l'ensemble de ces membres peuvent être associées de manière ponctuelle des personnes ressources sur certains sujets, tel que le responsable des archives ou le représentant des secrétaires médicales par exemple.

2) Missions et évolution de la CCIM

777. Les premiers travaux de la CCIM ont avancé difficilement. Assez rapidement, la commission s'est trouvée en charge de nombreuses questions stratégiques à résoudre, sans en avoir ni le pouvoir, ni la légitimité pour trancher correctement et efficacement ces questions. En effet, cette commission qui n'avait initialement qu'un rôle d'éclairage, a commencé à rendre des avis, sans aucune force contraignante ni réelle légitimité. Par ailleurs, à l'occasion de ses rapports d'activité, la CCIM a constaté que des risques majeurs existaient en termes de respect de la confidentialité des données de santé, liés à la fois à l'organisation des droits d'accès aux différentes applications du SIH ainsi qu'à l'absence totale de suivi et d'analyse des accès aux données par les utilisateurs.

778. Elle a donc souhaité proposer une réorientation de ses priorités ainsi une augmentation de ses moyens. En 2014, soit trois ans après sa mise en place, la CCIM a formulé à l'intention de la Direction générale du CHRU de Lille une proposition de fonctionnement en termes de gestion de la confidentialité médicale. L'organisation proposée reposait sur, d'une part, une gestion de la confidentialité au sein du SIH par le département de l'information médicale, avec l'appui et la validation systématique de la CCIM et, d'autre part, sur la gestion opérationnelle assurée par le Département de l'information médicale, en lien avec l'ensemble des directions techniques compétentes (et notamment la direction des ressources numériques). L'ensemble des actions à mener pour aboutir à une organisation optimisée et pérenne en matière de gestion de la confidentialité, ainsi que les moyens humains et financiers à

mobiliser, était également précisé dans cette proposition. Cependant, bien que la direction générale de l'établissement ait, à maintes reprises, réaffirmé le besoin d'organiser la gestion de la confidentialité, et a confirmé le rôle prépondérant de la CCIM en la matière, aucune présentation en Directoire du projet n'a eu lieu.

779. Toutefois, la CCIM a continué sa réorganisation afin de poursuivre au mieux ses travaux. C'est ainsi que 4 nouveaux grands axes de travail ont été redéfinis : la définition des droits d'accès, la gestion de ces droits, l'analyse des pratiques et des traces d'accès et enfin l'information et la communication autour de la confidentialité. En parallèle, la Département de l'Information Médicale a obtenu la création d'un poste de médecin à 60% consacré à la confidentialité. Le redimensionnent des attributions et des moyens de la CCIM a permis de donner une toute nouvelle envergure à cette commission, dont les travaux ont été plus riches sur les années 2015 et 2016.

Cette commission est amenée à évoluer dans les années à venir, sa charge de travail et son champ d'action ne cessant d'augmenter. Une organisation plus structurée doit être mise en place et sa légitimité doit être définitivement ancrée.

B. Le Comité CNIL

780. Le CHRU de Lille, bien que doté d'un agent occupant la fonction de Correspondant Informatique et Libertés à 50% de son temps, n'arrivait pas à faire face à l'ensemble des formalités exigées en la matière. Très rapidement, la Direction des Affaires Juridiques et le CIL ont travaillé en étroite collaboration afin d'améliorer le respect des règles en la matière. En ce sens, et comme nous l'avons vu précédemment, une campagne de sensibilisation par le biais de formations avait été mise en place, sans réel succès. Par ailleurs, afin de satisfaire à l'obligation légale d'information des patients relative aux traitements de données les concernant, une information par voie d'affichage, d'une part, et par le biais du livret d'accueil, d'autre part, a été réalisée. Cependant, face à la technicité et à la récurrence de certaines problématiques (notamment liées à l'encadrement de la recherche en santé), il a été décidé de créer un comité dédié, véritable dispositif transverse, au côté du Correspondant Informatique et Libertés, permettant de garantir la protection des données à caractère personnel, notamment par des actions en amont, telle que l'élaboration des mesures adaptées à

la protection des données mais également des action concrètes, comme l'instruction des demandes spécifiques ou complexes et, bien entendu, le suivi des évolutions législatives et règlementaires sur la question, particulièrement fournies ces dernières années.

781. Ce comité a été pensé par le CIL comme une émanation de la CCIM. Ainsi, on retrouve dans la composition de ce comité des membres également présents à la CCIM (notamment le DIM et la Direction des Affaires Juridiques). Sa composition est multidisciplinaire, avec toutefois une forte représentation des acteurs de la recherche médicale, et notamment les coordonnateurs des attachés de recherches cliniques, en prise directe avec les démarches CNIL et les problématiques qu'elles peuvent poser.

Très pragmatique, ce comité entend apporter des réponses pratiques aux questions qui lui sont soumises. Il participe à la diffusion de l'information en matière de législation Informatique et Libertés. Ainsi, à l'occasion de la publication des méthodologies de référence, le comité a travaillé à l'élaboration d'un support d'information.

782. Son premier chantier a consisté en un travail de simplification des démarches CNIL au sein de l'établissement. Au CHRU de Lille, un accès Intranet à une rubrique dédiée est mise en place depuis plusieurs années. Cependant, les déclarations de traitement n'étaient pas nombreuses, par manque de visibilité et de clarté de cette rubrique. Par ailleurs, les démarches pouvaient parfois paraitre trop longues ou fastidieuses pour les responsables de traitement (notamment dans le cas des thèses), qui préféraient les contourner. Ainsi, le premier travail du Comité CNIL a été d'améliorer cette procédure. Le formulaire de déclaration a été modifié et des questions plus précises ont été ajoutées, permettant de qualifier plus facilement le traitement (notamment pour la recherche) et de limiter les demandes de précisions auprès du déclarant.

Une nette évolution des déclarations a alors été observée. Ainsi, en mars 2017, une augmentation de 44% des déclarations par rapport à 2016 a pu être constatée. Pour compléter ce dispositif, une permanence CNIL a été mise en place, de manière hebdomadaire, et assurée par des membres de l'équipe sécurité du SIH.

Actuellement, le comité continue son travail d'étude des situations plus complexes, tout en suivant l'évolution de la législation applicable afin d'adapter ses pratiques.

§2. Bilan des réalisations de ces structures novatrices

783. Il nous apparait intéressant à ce stade de nos recherches de nous attarder sur les résultats obtenus par la création de ce type de structures et plus particulièrement sur les réalisations de la CCIM, commission ayant vécu suffisamment longtemps pour qu'un premier bilan soit dressé.

Les pistes de travail de cette commission ont été nombreuses. Il nous semble cependant intéressant de nous arrêter plus particulièrement sur le travail de réflexion autour de la mise ne place d'une règlementation interne en matière de confidentialité de l'information (A) ainsi que sur le travail portant sur l'analyse des traces d'accès et la réponse apportée aux accès indus (B). Enfin, il faut préciser que l'action de cette commission a été reconnue par l'ARS au niveau régional, qui lui a décerné, en 2015, le label « droit des usagers » (C), reconnaissant ainsi le travail particulièrement novateur mais aussi protecteur des droits des patients de cette commission.

A. L'élaboration d'une réglementation interne

784. Partant du principe que pour être opposables, les règles relatives à la confidentialité devaient être parfaitement connues des utilisateurs, la CCIM a mené et, mène encore à ce jour, un chantier de mise en place d'une règlementation interne.

Cette règlementation se compose de deux parties : d'un côté un règlement intérieur de l'information médicale, plutôt général, et de l'autre, des règlements intérieurs d'application, spécifiques à chacun des logiciels. Ces deux chantiers, qui sont encore en cours d'élaboration à l'heure actuelle, méritent tout de même que l'on s'y attarde.

L'idée de rédiger un règlement intérieur de l'information médicale au CHRU de Lille n'est pas nouvelle. En réalité, quand la CCIM s'est emparée de la question, il s'agissait plutôt

d'une mise à jour d'un précédent règlement, initialement rédigé en 2001 mais jamais appliqué faute de validation institutionnelle. Le but premier de ce règlement est de remettre à plat l'ensemble des règles applicables en matière de partage et d'utilisation des données issues de l'activité médicale. Il représente un atout particulièrement précieux dans le cadre de la recherche et des modalités d'accès et de réutilisation des données de santé dans le cadre d'une recherche rétrospective notamment.

785. Débutée en 2014, cette mise à jour n'a cependant pas abouti à l'heure actuelle. Deux éléments peuvent expliquer les difficultés rencontrées par la CCIM dans la gestion de ce travail. D'une part, la commission est régulièrement saisie par d'autres problématiques considérées comme plus urgentes, notamment en termes de droits d'accès au SIH. Victime en quelques sortes de son "succès", mais n'ayant pas d'équipe dédiée pour gérer l'ensemble des missions et demandes confiées, la CCIM ne peut s'atteler à tous les chantiers confiés et doit donc en prioriser certains. Dans ce contexte, la rédaction du règlement intérieur de l'information médicale n'a malheureusement jamais été priorisé.

D'autre part, la thématique de la recherche médicale, et plus particulièrement des modalités de partage de l'information médicale au sein de l'établissement dans un but de réutilisation à des fins de recherche, est un sujet particulièrement sensible et stratégique. Ce sujet nécessite un arbitrage institutionnel avant de pouvoir être intégré au sein du règlement intérieur de l'information médicale. C'est pourquoi aujourd'hui, le CCIM n'a pas encore adopté son règlement intérieur.

786. Sur ce sujet, un parallèle peut être effectué avec les règlements intérieurs du Département de l'Information Médicale (DIM), qui existent dans certains établissements hospitaliers. En effet, dans les établissements qui ne se sont pas dotés d'une commission dédiée à la protection de la confidentialité, le Médecin responsable de l'information médicale, et donc, par extension, le DIM, doivent gérer cette mission. De manière classique, ces règlements intérieurs reprennent les missions du DIM, sa place dans l'établissement et les

moyens qui lui sont attribués. Les rôles des différents acteurs ainsi que les règles de traitement et de transmission de l'information y sont également présents[924].

Le travail de règlementation interne de la CCIM concerne également les différents logiciels médicaux composant le SIH du CHRU de Lille. Partant de l'exemple de la charte informatique rédigée en 2012 et annexée au Règlement Intérieur de l'établissement, la CCIM a souhaité dupliquer ce modèle. L'idée était donc de rédiger le règlement intérieur d'utilisation de chaque application logicielle sur un modèle identique. Ces règlements ont deux objectifs principaux : d'une part, définir clairement les droits d'utilisation des différents profils dans l'application et, d'autre part, rappeler aux utilisateurs leurs obligations, notamment en termes de sécurité et de confidentialité.

La rédaction de ces règlements intérieurs des applications médicales a débuté en 2015 et demeure en cours aujourd'hui.

La CCIM a également travaillé sur un autre sujet important : celui des accès indus aux données de santé.

B. Analyse et sanction des accès indus

787. Sur une période de 18 mois, entre 2013 et 2015, le CHRU a vu le nombre de plaintes de professionnels de santé, pris en charge au sein du CHRU de Lille, pour accès indu à leur dossier médical informatisé, augmenter de manière significative.

Ces plaintes sont en réalité de deux sortes : d'un côté, les plaintes qui émanent d'agents qui craignent une rupture dans la confidentialité de leur données, souvent par manque de confiance dans le SIH et, d'un autre côté, les plaintes résultant de constats objectifs de l'existence d'une violation du secret professionnel. S'est alors posée, pour la CCIM, la question de la position à adopter.

---

[924] *V*. notamment en ce sens : Le département d'information médicale. Information, informatique et programme de médicalisation des systèmes d'information, *Fascicule Informations Hospitalières*, n°27, 1990, pp. 60-63 ; plusieurs règlement intérieurs de DIM sont disponible sur Internet. C'est le cas notamment du Centre Hospitalier Edouard Toulouse à Marseille, ou celui du Centre Hospitalier de Montperrin.

En effet, l'outil informatique permet une traçabilité des accès au dossier médical informatisé. Cependant, la CCIM a dû réfléchir aux modalités d'exploitation de ces traces, d'un point de vue technique, bien évidemment, mais surtout d'un point de vue juridique. Une réflexion a été menée pour savoir sur quels fondements ces traces d'accès pourraient être transmises aux personnes qui en feraient la demande. La CCIM souhaitait, en effet, rendre accessible aux patients, qu'ils soient agents du CHRU de Lille ou non, l'ensemble des traces d'accès à leur dossier médical.

788. Ainsi, partant du principe que les traces d'accès à un dossier médical informatisé faisaient partie intégrante de ce dossier, lui-même communicable au patient, au titre des dispositions prévues par l'article L. 1111-7 du Code de la santé publique, la CCIM a considéré que celles-ci pourraient donc être communiquées à toute personne en faisant la demande. Cependant, dans un souci de loyauté vis-à-vis de ses agents, une communication large a été effectuée à ce sujet, avant que la procédure de communication des traces soit effective. Au deuxième semestre 2015, cette procédure a été définitivement mise en place. Les demandes n'ont cessé, depuis, d'augmenter. Cependant, nous pouvons constater que le nombre de demandes reste très faible en proportion de l'activité du CHRU de Lille. Ainsi, depuis la mise en place de cette procédure, 32 demandes de communication de traces d'accès ont été enregistrées et traitées. Huit de ces demandes émanaient de patients, 19 d'agents pris en charge au CHRU de Lille et cinq de cadres d'agents suspectant un comportement inadéquat. Dans ce contexte, la DAJ a, par ailleurs, rencontré six personnes ayant demandé ces traces d'accès, afin notamment de les renseigner sur les suites possibles à donner.

Par ailleurs, il a été décidé que les accès indus aux dossiers médicaux, constatés à cette occasion, feraient l'objet d'une transmission auprès du Département des Ressources Humaines, afin d'envisager, au cas par cas, des sanctions disciplinaires, ou, *a minima*, un rappel des règles applicables. Cette procédure permet au CHRU d'être transparent vis-à-vis de ses patients mais également de les rassurer. En effet, il n'est pas rare qu'une suspicion de violation du secret professionnel soit infondée, et la transmission des traces permet de calmer les craintes du patient à ce sujet. Elle permet également de sensibiliser les agents aux règles applicables en matière de partage de l'information médicale et leur rappeler leurs obligations en matière de secret professionnel et de confidentialité.

La CCIM, fortes de ces actions, a souhaité concourir au label "droits des usagers" du Ministère de la santé.

C. La labellisation de l'action de la CCIM

789. En 2015, la CCIM a souhaité concourir au label "droits des usagers", mis en place par le Ministère de la santé via les ARS depuis 2011. Elle a ainsi soumis son projet intitulé « démarche qualité et gestion des risques de la CCIM ». Ce projet d'optimisation de la confidentialité des données de santé était en réalité composé de trois projets unitaires et indissociables, développés en 2015 : la participation à la semaine sécurité patient, la réalisation d'une démarche d'évaluation des pratiques professionnelles et la rédaction des règlements intérieurs des applications médicales. Ces trois projets, menés de front, avaient pour but d'améliorer la culture des professionnels, de réglementer de manière claire et applicable, et d'améliorer en conséquence le respect des droits des usagers.

Il est intéressant de nous attarder sur le contenu de ces trois projets, qui ont permis à la CCIM d'obtenir son label "droit des usagers"[925].

790. En 2015, la CCIM a participé aux actions internes du CHRU menées à l'occasion de la Semaine Sécurité Patient. L'action de la CCIM, à cette occasion, s'est matérialisée par une présentation de la Commission et de ses travaux auprès des professionnels du CHRU de Lille sur un stand dédié au sein des différents hôpitaux de l'établissement. Ainsi, lors de cette action, les membres de la CCIM ont pu rappeler à de nombreux professionnels les principes du secret médical et du secret professionnel, et ont eu l'occasion de distribuer des documents de communication[926], portant sur le respect de la confidentialité des données médicales dans la pratique de soin et dans la recherche en santé. Certains des stands ayant été installés dans le hall d'entrée des hôpitaux, les patients intéressés ont également eu l'occasion de poser leurs questions relatives à la sécurité et à la confidentialité de leurs données de santé. D'une manière plus générale, cette action a été l'occasion d'une campagne de communication

[925] Les modalités d'obtention de ce label sont reprises en annexe de nos travaux, annexe II.
[926] Ces documents sont repris en annexe de nos travaux, annexe III.

massive au sujet de la CCIM et de ses actions, encore trop méconnus des professionnels de l'établissement en 2015.

791. Par ailleurs, la CCIM a réalisé en 2015 un audit interne, sous forme d'évaluation des pratiques professionnelles (EPP) et portant sur l'accès aux données médicales informatisées et leur partage. Ce travail a été réalisé suite à une augmentation des plaintes pour accès indu au dossier médical informatisé mais également en raison de l'observation de mésusages importants dans l'utilisation du système d'information. Les objectifs poursuivis par cet audit étaient multiples. Du point de vue des professionnels du CHRU, il visait principalement à les sensibiliser sur la problématique de la confidentialité des données en les faisant réfléchir sur leurs propres pratiques. Du point de l'établissement, ce questionnaire permettait de faire connaitre auprès des professionnels l'existence de la CCIM et le travail réalisé au niveau institutionnel au sujet de la confidentialité.

Un questionnaire de 30 questions[927] a donc été mis en ligne sur l'Intranet de l'établissement pendant deux mois et l'ensemble des agents du CHU étaient invités à y répondre. Deux mille trois cent deux personnes ont participé (sur les 15 000 personnes environ, travaillant au CHU)[928].

A l'issue de cet EPP, des risques de rupture de la confidentialité ont été repérés à plusieurs niveaux. A partir de ces résultats, la CCIM va pouvoir engager des actions correctrices. Par ailleurs, les résultats de cet audit ont fait l'objet d'une large communication, à l'échelle de l'établissement, mais au-delà également puisque les travaux de la CCIM, et plus spécifiquement ce travail d'audit, ont fait l'objet d'une communication à l'occasion d'une journée d'études consacrée au secret professionnel et organisée par le CHRU de Lille, en partenariat avec la faculté de droit de l'Université de Lille Droit et Santé. Cette communication a également été publiée au sein de la Revue Générale de Droit médical, lui assurant une certaine visibilité, parmi les professionnels du droit de la santé[929].

---

[927] Ce questionnaire est repris en annexe de nos travaux, annexe IV.
[928] DUMESNIL, Chloé, « Informatisation des données et protection du secret : l'exemple des travaux de la commission de confidentialité des informations médicales du CHRU de Lille », *RGDM*, n° 61, décembre 2016, p. 79.
[929] *Id.*, pp. 77-79.

792. Enfin, comme nous l'avons vu précédemment, la CCIM a travaillé à la rédaction des règlements intérieurs des principales applications informatiques présentesay au sein du SIH du CHRU de Lille.

Ces trois actions ont composé le projet global « démarche qualité et gestion des risques de la CCIM », qui a reçu le label régional Droits des usagers 2015.

Conclusion de la section

793. Le CHRU de Lille a créé deux commissions *ad'hoc* afin de gérer, d'une part la protection de la confidentialité des données de santé et, d'autre part, l'ensemble des formalités CNIL.

En effet, face à l'augmentation constante du nombre de données sensibles produites et enregistrées au sein du SIH, le CHRU de Lille a confié à la CCIM la mission de veiller au strict respect des règles de partage de celles-ci. Par ailleurs, afin d'aider la CIL dans ses missions, un Comité CNIL s'est mis en place, permettant notamment de simplifier et rendre plus visibles les démarches préalables nécessaires à la mise en place d'un nouveau traitement de données au sein du CHRU de Lille.

Ces deux commissions présentent une composition pluridisciplinaire sensiblement identique. Ainsi, l'ensemble des acteurs concernés par la confidentialité des données y sont représenté, notamment le DIM, le CIL, la communauté médicale, la communauté soignante, la DRN et la DAJ.

En instaurant ces commissions le CHRU de Lille a démontré sa volonté de protéger activement les données de santé de ses patients. Aujourd'hui, le bilan des actions de ces commissions, et plus particulièrement de la CCIM, est globalement positif, même si cette commission manque encore aujourd'hui d'une légitimité forte et de moyens humains suffisant pour mener à bien toutes ses missions.

Conclusion du chapitre

794. Le CHRU de Lille a souhaité inscrire le développement et la pérennisation de son SIH dans la stratégie globale de l'établissement. Le Schéma Directeur des Systèmes d'Information (SDSI) a donc été adopté à l'occasion du projet d'établissement 2012-2016. A cette occasion, huit grandes orientations ont été définies, elles-mêmes mises en œuvre par le biais de cinq projets prioritaires.

Par ailleurs, deux projets importants en termes de sécurité du SIH ont été mis en œuvre et menés à bien au CHRU de Lille. D'une part, le projet "carte d'établissement", qui a permis de fournir à l'ensemble des agents de l'établissement une carte permettant d'assurer le contrôle des accès, mais également l'authentification et la traçabilité des actions au sein des différentes applications informatiques. D'autre part, le projet "SMSSI", démarche qui a permis au CHRU de Lille de garantir l'intégrité et la disponibilité de son SIH, mais également d'élaborer une méthodologie permettant d'intégrer de manière systématique la sécurité au sein des projets informatiques développés.

Le CHRU s'attache également à diffuser auprès de ses agents une véritable culture de la sécurité du SIH, par le biais de formations mais également d'actions de communication et de sensibilisation. Enfin, le CHRU de Lille démontre une réelle volonté de protéger les données de santé qu'il produit. Ainsi, il a créé deux structures *ad'hoc* pour mener à bien cette mission : la CCIM et le comité CNIL. La CCIM, commission particulièrement novatrice, présente un bilan d'actions positif, même si son manque de moyens et des interrogations quant à sa place au sein de l'établissement, freinent l'avancée de ses travaux.

Conclusion du titre

795. Afin de sécuriser au mieux l'utilisation des TIC au sein des établissements de santé, ces derniers doivent intervenir à chaque étape, depuis la mise en place des TIC jusqu'à leur utilisation quotidienne. Face aux lacunes des pouvoirs publics et, aux difficultés causées par les imprécisions du droit, les établissements peuvent agir et impulser la sécurisation des pratiques qui leur manque. Finalement ils bénéficient d'une marge de manœuvre, qui leur permet d'être inventifs et d'élaborer des solutions qui leurs sont parfaitement adaptées, créant ainsi le contexte propice au développement de techniques de plus en plus innovantes. Cependant, il leur faut pour cela penser de manière globale leur politique de développement des SIH. Cette réflexion doit être amorcée en amont, en développant une véritable stratégie, au sein même du projet d'établissement. Les établissements ne doivent pas oublier qu'ils disposent par ailleurs d'outils juridiques et managériaux qui pourront leur permettre d'assurer une utilisation des TIC qui sera fiable et respectueuse des contraintes juridiques, déontologiques et éthiques.

En la matière, le CHRU de Lille constitue un exemple de sécurisation réussie. Soucieux d'instaurer les meilleures conditions possibles pour le développement de son SIH, il a su gérer de manière stratégique différents projets relatifs à la sécurité, tout en assurant une sécurisation accrue des données de santé.

Conclusion de la seconde partie

796. A ce stade de notre étude, nous avons pu constater que les pouvoirs publics avaient un rôle stratégique à jouer dans la sécurisation de l'utilisation des TIC en santé. Une impulsion nationale doit être donnée en la matière, afin d'assurer la cohérence des projets développés et seule une gouvernance forte de l'e-santé pourra y parvenir. Le déploiement des projets pourra quant à lui se faire au niveau régional, en s'appuyant sur les ARS, mais également sur la dynamique qui apparaitra avec la naissance des GHT.

Bien qu'une inflation législative dans le domaine soit, évidemment, à proscrire, « *certains points de droits constituent clairement des verrous au regard du développement de l'e-santé* »[930]. Ainsi, le cadre doit être rénové afin d'accompagner l'innovation dans le numérique en santé et assurer la sécurité juridique nécessaire à la bonne utilisation des TIC dans la pratique médicale.

Dans cette dynamique générale de sécurisation, les établissements de santé ont un rôle essentiel à jouer. Ils peuvent en effet identifier leurs besoins et sécuriser au mieux leurs pratiques quotidiennes. A titre d'exemple, le CHRU de Lille s'attache à sécuriser au mieux l'utilisation des TIC dans la pratique quotidienne de ses agents.

[930] ROBIN, Jean-Yves. « L'urgence numérique. Faire de la France un leader de l'e-santé », *L'Harmattan*, 2015, p. 193.

Conclusion générale

« *Nous sommes à la croisée des chemins […] les prochaines années seront déterminantes pour le devenir de notre modèle et le numérique peut être notre meilleur allié comme notre pire ennemi pour préserver ce qui doit l'être et transformer ce que nous choisirons collectivement de réformer* »[931].

797. A l'issue de nos travaux, nous pouvons constater que l'utilisation des TIC dans la pratique médicale ne fait pas l'objet d'un cadre juridique spécifique et unifié. Réfléchir à l'appréhension des TIC en santé par le Droit, c'est faire appel à différentes sources du droit. Tout comme il n'existe pas une seule utilisation possible des TIC dans la pratique médicale, il n'existe pas un seul cadre juridique applicable. Les établissements de santé vont donc devoir réfléchir au cas par cas et repérer les différentes contraintes juridiques qui s'imposent à eux.

798. D'une manière générale, l'informatisation des données de santé, conséquence première de l'introduction des TIC dans la pratique médicale, relève du droit commun de la protection des données personnelles. Cependant, le caractère particulier et multiple de ces données exige le respect de différentes règlementations applicables. Elles nécessitent également une protection particulière, et le législateur ne s'est pas contenté de protéger le secret professionnel. A cela, il a souhaité ajouté un cadre relatif à l'hébergement et à la communication des données de santé informatisées. Ce cadre montre cependant certaines limites.

799. Les TIC en santé ont également permis de chambouler les pratiques habituelles en matière de prise en charge du patient. Désormais, celle-ci peut être entièrement dématérialisée, les professionnels de santé pouvant envisager une prise en charge à distance, en s'appuyant notamment sur des dossiers médicaux partagés. Ces dossiers médicaux, communément appelés dossiers médiaux électroniques ne bénéficient aucunement d'un statut

[931] ROBIN, Jean-Yves. « L'e-santé en question », *I2D – Information, données & documents*, 2016/3 (Volume 53), p. 58.

édicté par la loi, à l'exception de l'un d'entre eux : le Dossier Médical Partagé. Pour ce dossier ambitieux, placé sous le contrôle direct du patient, et accessible via une plateforme unique entièrement dématérialisée, le législateur a souhaité mettre en place un régime exorbitant de droit commun[932]. La prise en charge dématérialisée du patient par le biais d'un outil de télémédecine a également fait l'objet d'un cadre spécifique mais celui-ci, sous des aspects de simplicité, impose de trop nombreuses contraintes administratives aux établissements de santé. A cela s'ajoute un bouleversement des pratiques et des règles habituelles en matière de droit des patients et de responsabilité professionnelle.

800. L'utilisation des TIC dans la pratique médicale répond ainsi tantôt à des règles de droit commun et tantôt à des règles spécifiques. Les établissements de santé peuvent rapidement se retrouver perdus face à l'ensemble de ces différentes règles de droits qui sont autant d'obstacles sur leur voie du développement de pratiques innovantes en matière de TIC en santé. Le droit perd alors son rôle de sécurisation et, plus qu'un simple frein aux initiatives, il peut parfois être source d'incertitudes.

Pour y remédier, plusieurs voies doivent être empruntées.

801. Une impulsion doit être donnée au niveau national. Une vision globale du numérique en santé est en effet nécessaire afin de favoriser l'innovation et d'assurer aux différents acteurs impliqués un environnement propice. C'est pourquoi la gouvernance des Systèmes d'Information en Santé se doit d'être solide, lisible et force de proposition. Par ailleurs, le cadre juridique actuel applicable aux TIC en santé doit être repensé. Ceci représente certainement, aujourd'hui, l'exercice le plus complexe. Le droit en place doit être l'allié des acteurs concernés et non l'ennemi redouté. Il faut donc un cadre adapté aux exigences de ces technologies innovantes, c'est-à-dire un cadre souple et réactif. Cependant, la rénovation du cadre juridique ne doit pas passer, à notre sens, par l'édiction de nouvelles règles mais par une simplification de celles déjà en place.

802. Les établissements de santé ont également un rôle essentiel à jouer dans la sécurisation de leurs pratiques. Ils doivent pour cela envisager de manière stratégique le développement et

[932] *V*. notamment en ce sens, ZORN-MACREZ, Caroline. « Données de santé et secret partagé », *op. cit.*, p. 305.

la gestion de leur système d'information hospitalier. Cette vision leur permettra d'anticiper les éventuelles contraintes et mener à bien leurs différents projets. Par ailleurs, ils disposent d'outils juridiques et managériaux efficaces pour leur permettre d'encadrer l'utilisation des TIC dans la pratique médicale par leurs agents. Ils accompagneront ainsi ces nouvelles pratiques, en rappelant les règles applicables et en formant leurs agents à l'utilisation appropriée des TIC. Ils peuvent aussi sanctionner des comportements déviants et ainsi assuré une utilisation sereine et respectueuse des contraintes juridiques, éthique et déontologique des TIC dans la pratique médicale. L'exemple du CHRU de Lille et de l'ensemble des actions qu'il a pu mettre en place démontre bien que les établissements de santé peuvent être à l'origine d'une sécurisation réussie de leurs pratiques.

803. Nos travaux nous ont donc permis d'appréhender le cadre juridique dans lequel s'inscrit l'utilisation des TIC dans la pratique médicale et constater ses lacunes. Aujourd'hui une sécurisation de l'utilisation des TIC en santé est nécessaire. Notre étude ne se veut pas exhaustive et si les possibilités du numérique en santé sont nombreuses, les questionnements juridiques qui s'y rapportent le sont tout autant. Ce dont nous sommes certains, c'est que le numérique en santé représente l'avenir du système de santé actuel, et il est essentiel de s'inscrire dans cette démarche d'utilisation croissante des TIC dans la pratique médicale.

Table des Annexes

Annexe I : Schéma de l'organisation en briques fonctionnelles d'un SIH type.

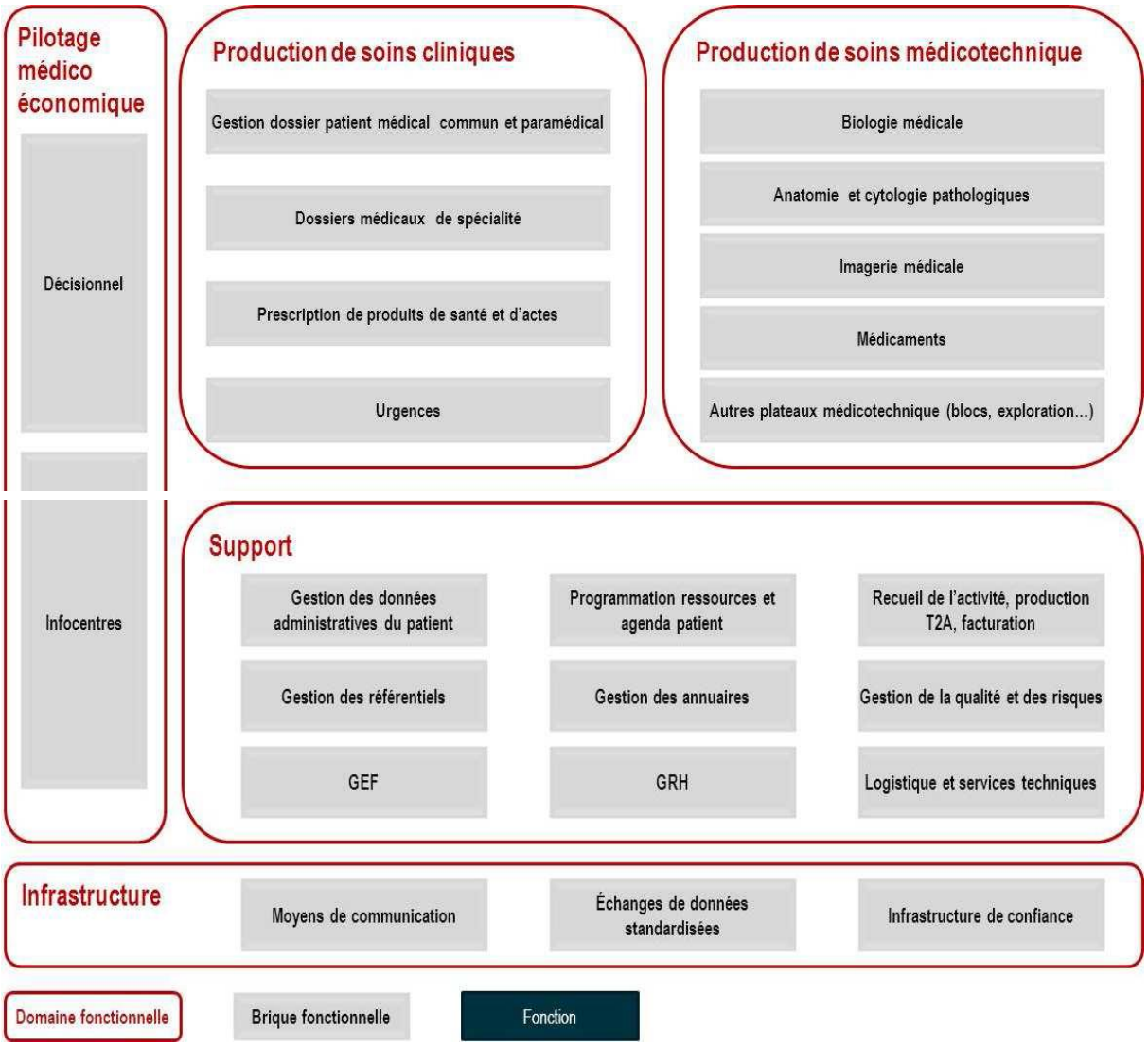
Annexe II : Présentation et modalités d'obtention du label "droits des usagers"

Annexe III : Documents de communication de la CCIM

Annexe IV : Questionnaire d'évaluation des pratiques professionnelles de la CCIM

Annexe I. Schéma de l'organisation en briques fonctionnelles d'un SIH type

Ce schéma est issu des travaux en cours menées par l'ASIP Santé et l'ANAP sur les SI de santé.



Annexe II : Présentation et modalités d'obtention du label "droits des usagers"

Parcours de santé : usagers, vos droits

Cahier des charges du label et du concours
2016-2017

Mai 2016

1

STRATÉGIE
NATIONALE
DE SANTÉ

I | Le contexte

Le label « Droits des usagers de la santé » a été initié dans le cadre du dispositif « 2011, année des patients et de leurs droits ». Il vise à valoriser des expériences exemplaires et des projets innovants en matière de promotion des droits des usagers. Reconduit en 2015 et étendu au champ médico-social et social, le bilan de la labellisation s'avère très positif :

- une dynamique régionale effective et constante avec 21 régions sur 26 impliquées ;
- une répartition territoriale confortée avec plus de 160 projets examinés par les commissions spécialisées « Droits des usagers » (CSDU) des conférences régionales de la santé et de l'autonomie (CRSA) ;
- un nombre de candidats au concours en augmentation ;
- plus de 60 projets labellisés en région, tous valorisés sur l'espace « Droits des usagers de la santé » du site du ministère chargé de la santé :

www.espace-droits-usagers.sante.gouv.fr

Dans ce contexte, il a été décidé de rééditer l'expérience de labellisation en 2016-2017, en tenant compte d'une part, du retour d'expérience de l'édition 2015, de l'avis de la commission spécialisée « droits des usagers » (CSDU) de la conférence nationale de santé (CNS), des observations formulées par les agences régionales de santé (ARS) et d'autre part, des résultats de l'étude réalisée par l'école des hautes études en santé publique (EHESP) à l'initiative du ministère et relative à la participation des usagers ou de leurs représentants.

En 2015, les projets labellisés concernaient majoritairement les actions d'information, de formation des professionnels de santé intégrant la participation des usagers et de leurs représentants.
Dans une moindre mesure, les projets labellisés portaient sur des initiatives en lien avec la médiation en santé, le traitement des réclamations et des plaintes ou encore l'évolution du système de santé.
L'édition 2016-2017 accompagne voire préfigure la mise en œuvre des lois dites : vieillissement, santé et fin de vie et renforçant les droits des usagers dans la logique de parcours – de santé, de soins, de vie – et intégrant les recommandations de la conférence nationale de santé et la nécessité d'une identification d'un « dénominateur commun » des droits individuels et collectifs qui « traverse » le secteur des soins de ville, le secteur hospitalier et le secteur social et médico-social, tant en établissement qu'à domicile au moyen d'une charte de la personne dans son parcours de santé et des professionnels l'accompagnant.
Elle permet une continuité entre le dispositif de labellisation et la 6ème édition du concours « Droits des usagers de la santé » qui viendra récompenser, les meilleurs projets labellisés, dans la limite de 2 par région. La sélection est faite par les ARS, après avis de la CSDU des CRSA, et en lien, le cas échéant, avec les DRJSCS, puis communiquée au ministère chargé de la santé. Un jury représentant les différentes composantes du système de santé examinera les projets labellisés sélectionnés par les ARS et décernera des prix à 5 lauréats dont les projets auront été jugés particulièrement exemplaires.

A titre d'exemple, le jury du concours 2015 a récompensé 5 lauréats parmi les projets labellisés en région :

-Association Médecins du Monde de Rouen (Haute-Normandie) | Prévention et réduction des risques pour les personnes travailleuses du sexe
-Centre hospitalier d'Argenteuil (Ile-de-France) | Intégration des proches dans la prise en charge du patient en réanimation
-Hôpital local Jean-Baptiste-Caron de Crèvecœur-le-Grand (Picardie) | Accompagnement de la douleur à domicile
-Hospitalité Saint-Thomas-de-Villeneuve de Lamballe (Bretagne) | Développement de la démocratie en santé
-EPSM Lille Métropole (Nord-Pas-de-Calais) | Chronique du tiers exclu

Les 5 projets mettent en avant **des démarches intégrant pleinement la participation des usagers, des patients ou des résidents aux projets** de la simple information à la co-construction des projets en tant que telle.

Par ailleurs, **les initiatives « ouvrant les murs » des établissements de santé, des services de soins ou des structures spécialisées** et permettant, ainsi, d'aller à la rencontre des populations concernées – entre autre à domicile – ont été particulièrement distingués par le jury.

Enfin, l'une des actions promue illustre concrètement la démocratie sanitaire en développant **les actions de type participatif** au sein d'un établissement de santé.

Les 5 projets sont modélisables, transposables : ils s'inscrivent dans la durée, s'attachent à favoriser l'appropriation des droits par tous – y compris par des populations en situation difficile -. Ils ont une visée pédagogique, sont originaux ou comblent un vide : chacun d'entre eux a reçu du ministère un prix de 2 000€.

En 2016-2017 comme en 2015, le label et le concours seront ouverts à tous les acteurs du système de santé qui souhaitent s'engager dans une action innovante autour de la promotion des droits des usagers, et aux collectivités territoriales qui développent, pour certaines, des projets expérimentaux au niveau de leurs territoires.

Concernant les professionnels de santé, le label converge vers les objectifs poursuivis par le conseil national de l'ordre des médecins en faveur du renforcement du respect du droit à l'information et à l'accompagnement des patients, tant par les médecins libéraux qu'hospitaliers et salariés.

II | Le périmètre du label et du concours 2016-2017 « Droits des usagers de la santé »

Les thématiques privilégiées

En 2016-2017 comme en 2015, les axes thématiques s'appuient sur les recommandations issues des rapports sur les droits des usagers de la CNS et sur la

mission confiée à la CNS en vue d'élaborer une charte de la personne dans son parcours personnalisé de santé et des professionnels l'accompagnant.

Six axes thématiques, non exhaustifs, seront particulièrement privilégiés :

- renforcer et préserver l'accès à la santé – y compris à la prévention – pour tous, notamment par **une information adaptée** aux personnes vulnérables (mineures, majeures protégées, en perte d'autonomie, souffrant de troubles psychiques, intellectuellement déficientes etc.), étrangères, placées sous main de justice, etc. ;
- sensibiliser les professionnels de santé au moyen d'**actions de formation** aux droits des usagers ;
- favoriser **la médiation en santé** dans les structures de soins, médico-sociales et à domicile en mobilisant, entre autres, les médiateurs tels que les médiateurs médicaux, les médiateurs non-médicaux, les personnes qualifiées, etc. ;
- faire converger les droits des usagers des structures de soins, sociales et médico-sociales, notamment au travers de **la participation des représentants des usagers et des usagers** (Commission des usagers (CDU), Conseil de la vie sociale (CVS) et de la mise en place de dispositifs expérimentaux adaptés aux parcours (organisation territoriale pour l'exercice des droits impliquant les établissements, conseils généraux, ordres et organisations professionnels, ARS, les conseils territoriaux de santé, etc.) ;
- renforcer **l'effectivité** des droits des usagers par le traitement des réclamations et des plaintes en lien avec les représentants des usagers, quels que soient les destinataires de ces plaintes ou réclamations (établissements, conseils généraux, ordres et organisations professionnels, ARS, les conseils territoriaux de santé, etc.) et par l'analyse systématique des motifs notamment à partir des rapports des CDU ou des CVS et la mise en œuvre de mesures d'amélioration ;
- accompagner **les évolutions du système de santé** dans le respect des droits des usagers (e-santé, télémédecine, maisons et centres de santé, soins de santé transfrontaliers, développement de la chirurgie ambulatoire, etc.).

Ces thématiques, sont indicatives et serviront de guide pour l'attribution du label et des prix du concours.

Les candidats admissibles à la labellisation 2016-2017

Ils relèvent des 4 catégories éligibles au label « Droits des usagers de la santé », en phase avec le champ de compétence et le périmètre d'action des ARS voire des DRJSCS :

- les associations et les fondations exerçant leur activité dans le domaine de la santé et le secteur médico-social comme les associations d'usagers ou les associations et organisations professionnelles ;
- les établissements de santé, sociaux et médico-sociaux ;
- les professionnels de santé exerçant une activité libérale en ville, que ce soit à titre individuel ou dans le cadre d'un regroupement (réseaux de santé, structures de proximité, maison ou centre de santé, etc.) ou de service d'intérêt général dédiés à la prévention (services de PMI, santé scolaire et universitaire, santé au travail) ou encore dans un service de soins à domicile ;

- les institutions et les organismes susceptibles de conduire des actions de promotion des droits : ARS, agences sanitaires, collectivités territoriales, caisses d'assurance maladie, mutuelles, organismes de recherche, etc.

La nature des projets labellisables

Toute action visant à promouvoir les droits individuels et collectifs des usagers est susceptible d'être labellisée, dans la mesure où elle présente **un caractère innovant et reproductible**.

L'implication des usagers dans les projets retenus pour la labellisation est une condition indispensable. La participation des usagers ou leurs représentants varie de l'information, à la co-décision en passant par la concertation et la co-construction.

Les résultats du label et du concours 2015 peuvent être consultés à titre indicatif pour illustrer la nature des projets attendus dans ce cadre.

Des critères de sélection sont proposés infra : ils pourront être adaptés à des spécificités locales.

III | Les modalités de labellisation des projets et leur sélection au concours

L'information sur le dispositif de labellisation

Les modalités de lancement du label au niveau régional – appels à projets, actions médiatiques, etc – sont laissées à l'appréciation de chaque ARS et DRJSCS, sachant que l'ensemble des informations sera disponible prochainement sur l'espace internet « Droits des usagers du système de santé » du ministère chargé de la santé :

www.espace-droits-usagers.sante.gouv.fr

L'analyse et la sélection des projets

Comme en 2015, il est proposé de confier l'attribution du label « Droits des usagers de la santé » aux ARS, après avis des CSDU des CRSA et en lien, le cas échéant, avec les DRJSCS. Les critères de sélection pourront être mis en cohérence avec les priorités des plans stratégiques régionaux de santé en matière de droits des usagers.

Pour être recevables, les initiatives présentées satisferont aux caractéristiques suivantes :

- être modélisables et/ou transposables à l'ensemble du champ d'activité décrit supra ;
- associer les usagers ou leurs représentants, que ceux-ci soient à l'origine du projet ou qu'ils y participent. L'implication de ces derniers s'apprécie de l'information à la co-décision en passant par la concertation et la co-construction ;
- s'inscrire dans la durée ;

- favoriser l'appropriation des droits par tous, y compris par les populations dont la situation rend difficile l'accès à leurs droits ;
- se traduire par des supports informationnels et pédagogiques.

Lire à titre indicatif la grille d'analyse des projets labellisés au concours figurant en annexe I

Le calendrier

Le recueil des candidatures à la labellisation débutera à la réception de l'instruction ministérielle.

Les ARS proposeront les meilleurs projets labellisés admis à concourir au niveau national jusqu'au **10 février 2017** dans la limite de 2 par région. Les projets sélectionnés par les ARS seront accompagnés d'un avis motivé.

Le jury du concours national se réunira le **9 mars 2017** : les résultats seront annoncés au niveau national le **18 avril 2017**.

La valorisation des projets labellisés au niveau national

Les projets labellisés feront l'objet d'une valorisation, notamment par la mise en ligne d'informations au sein de l'espace « Droits des usagers de la santé » du ministère chargé de la santé : cela, au moyen du formulaire ad hoc à renseigner en ligne. L'objectif est de porter à la connaissance du plus grand nombre les projets labellisés ainsi que les initiatives des lauréats du concours afin d'en favoriser la reproductibilité.

Un suivi et une mise à jour seront assurés par les ARS pour les projets labellisés au niveau régional et par le bureau des « Usagers de l'offre de soins » de la direction générale de l'offre de soins (DGOS) pour les lauréats du concours national.

Lire à titre indicatif la grille de suivi des projets labellisés au concours, en annexe II.

Une cérémonie nationale de remise de prix viendra clore la campagne 2016-2017 pour récompenser les initiatives sélectionnées par le jury du concours.

IV | La protection des données à caractère personnel et la publicité des projets primés

Les porteurs des projets labellisés dans le cadre de ce dispositif autorisent le ministère chargé de la santé à divulguer leurs identités. Ils l'autorisent également à diffuser gracieusement, sur le site internet du ministère, le mode opératoire de leurs initiatives, y compris s'il s'agit d'un support vidéo.

Annexe I – Grille d'évaluation des projets labellisés admis à concourir

Nom du participant : **Catégories :** – les associations et les fondations exerçant leur activité dans le domaine de la santé et le secteur médico-social comme les associations d'usagers ou les associations et organisations professionnelles ; – les établissements de santé, sociaux et médico-sociaux ; – les professionnels de santé exerçant une activité libérale en ville, que ce soit à titre individuel ou dans le cadre d'un regroupement (réseaux de santé, structures de proximité, maison ou centre de santé, etc.) ou de service d'intérêt général dédiés à la prévention (services de PMI, santé scolaire et universitaire, santé au travail) ou encore dans un service de soins à domicile ; – les institutions et les organismes susceptibles de conduire des actions de promotion des droits : ARS, agences sanitaires, collectivités territoriales, caisses d'assurance maladie, mutuelles, organismes de recherche, etc. **Thématiques :** – renforcer et préserver l'accès à la santé – y compris à la prévention – pour tous, notamment par **une information adaptée** aux personnes vulnérables (mineures, majeures protégées, en perte d'autonomie, souffrant de troubles psychiques, intellectuellement déficient, étrangères, placées sous main de justice, etc.) ; – sensibiliser les professionnels de santé au moyen **d'actions de formation** aux droits des usagers ; – favoriser la **médiation en santé** dans les structures de soins, médico-sociales et à domicile en mobilisant, entre autres, les médiateurs tels que les médiateurs médicaux, les médiateurs non-médicaux, les personnes qualifiées, etc. ; – faire converger les droits des usagers des structures de soins, sociales et médico-sociales, notamment au travers de **la participation des représentants des usagers et des usagers** (CDU, CVS) et de la mise en place de dispositifs expérimentaux adaptés aux parcours (organisation territoriale pour l'exercice des droits etc.) ; – renforcer **l'effectivité** des droits des usagers par le traitement des réclamations et des plaintes, l'analyse systématique des motifs notamment à partir des rapports des CDU ou des CVS et la mise en œuvre de mesures d'amélioration ; – accompagner **les évolutions du système de santé** dans le respect des droits des usagers (e-santé, télémédecine, maisons et centres de santé, soins de santé transfrontaliers, chirurgie ambulatoire, etc.).	

Critères d'éligibilité		
Capacité du projet à être modélisable et/ou transposable à l'ensemble du périmètre de l'offre sanitaire ou médico-sociale		… / 5
Capacité du projet à s'inscrire dans la durée		… / 5
Capacité du projet à favoriser l'appropriation des droits par tous, y compris par les populations dont la situation rend difficile l'accès à leurs droits		… / 2.5
Implication des usagers ou de leurs représentants (information, concertation, co-construction, co-décision).		… / 2.5
Originalité du projet/caractère innovant		… / 2.5
Appréciation générale (sur les supports informationnels, pédagogiques, les réalisations concrètes et mesurables)		… / 2.5
Total note		**… / 20**
Points forts	**Points faibles**	

Intitulé du projet :

Nom du rapporteur :

Appréciation générale sur le projet

Propositions du rapporteur

9

Annexe II – Grille de suivi des projets labellisés ou lauréats au concours

Année d'obtention du label (prix) :

Intitulé de votre projet :

Bref rappel des objectifs :

Catégorie dans laquelle votre projet concourt :

- **Droits collectifs : oui / non | Droits individuels : oui / non**

- **Thématique (cocher la case correspondante) :**

renforcer et préserver l'accès à la santé – y compris à la prévention – pour tous, notamment par **une information adaptée** aux personnes vulnérables (mineures, majeures protégées, en perte d'autonomie, souffrant de troubles psychiques, intellectuellement déficientes, etc), étrangères, placées sous main de justice, etc. ;

sensibiliser les professionnels de santé au moyen **d'actions de formation** aux droits des usagers ;

favoriser **la médiation en santé** dans les structures de soins, médico-sociales et à domicile en mobilisant, entre autre, les médiateurs tels que les médiateurs médicaux, les médiateurs non-médicaux, les personnes qualifiées, etc. ;

faire converger les droits des usagers des structures de soins, sociales et médico-sociales, notamment au travers de **la participation des représentants des usagers et des usagers** (CDU, CVS) et de la mise en place de dispositifs expérimentaux adaptés aux parcours (organisation territoriale pour l'exercice des droits) ;

renforcer **l'effectivité** des droits des usagers par le traitement des réclamations et des plaintes, l'analyse systématique des motifs notamment à partir des rapports des CDU ou des CVS et la mise en œuvre de mesures d'amélioration ;

accompagner **les évolutions du système de santé** dans le respect des droits des usagers (e-santé, télémédecine, maisons et centres de santé, soins de santé transfrontaliers, chirurgie ambulatoire, etc.).

Autre (précisez) :

- **Catégorie (cocher la case correspondante) :**

association, fondation des domaines de la santé et médico-social ;

établissement de santé ou établissement médico-social ;

professionnel de santé exerçant une activité libérale à titre individuel ou regroupé, dans un service d'intérêt général dédié à la prévention, dans un service de soins à domicile ;

institution ou organisme susceptible de conduire des actions de promotion des droits : ARS, agence sanitaire, collectivité territoriale, caisse d'assurance maladie, mutuelle, organisme de recherche, etc.

Capacité de modélisation et/ou de transposition à l'ensemble du périmètre de l'offre sanitaire ou médico-sociale de votre projet	*Le projet a-t-il donné lieu à transposition dans une autre structure ?* *Avez-vous été contacté pour avoir des informations sur votre projet ?* *Si oui, quelles suites ont été données ?*
Capacité du projet à s'inscrire dans la durée	*Le projet se poursuit-il ? si oui, va-t-il évoluer ?* *Si non, pour quelle raison n'est-il pas poursuivi ?*
Capacité du projet à favoriser l'appropriation des droits par tous, y compris par les populations dont la situation rend difficile l'accès à leurs droits	*Avez-vous pu mesurer une meilleure appropriation des droits ?* *Si oui, comment et auprès de quel public ?*
Implication des usagers ou de leurs représentants (information, concertation, co-construction, co-décision).	*Les usagers sont-ils toujours partie prenante de votre projet ? si oui, dans quelle mesure ?* *Si non, pour quelle raison ?*
Originalité du projet/caractère innovant	*Votre projet vous semble-t-il encore original/ innovant ? si oui, dans quelle mesure, si non, pour quelle raison ?* *Imaginez-vous adapter votre projet pour qu'il soit à nouveau original/innovant ?*
Appréciation générale (sur les supports informationnels, pédagogiques, les réalisations concrètes et mesurables)	*Vos supports sont-ils toujours adaptés, pensez-vous les faires évoluer, si oui, comment ?* *si non, pourquoi ?*
L'attribution du label (prix) droits des usagers de la santé a-t-il été une aide dans le déploiement de votre projet ?	*Dans quelles circonstances avez-vous eu besoin de vous prévaloir de l'attribution du label ou du prix pour mener à bien votre projet ? quels ont été les effets positifs ou négatifs de l'attribution du label (prix) droits des usagers de la santé ?*
Points forts	**Points faibles**
Quels sont les points forts que vous retenez de votre expérience ? constatez-vous des points forts que vous n'aviez pas envisagés initialement ? si oui, lesquels ?	*Quelles sont les difficultés que vous avez rencontrées ? comment les avez-vous surmontées ?*

Annexe III : Documents de communication de la CCIM

Commission Confidentialité de l'Information Médicale

Etre acteur de sa santé

La confidentialité, c'est aussi notre métier !

La CCIM, c'est quoi ?

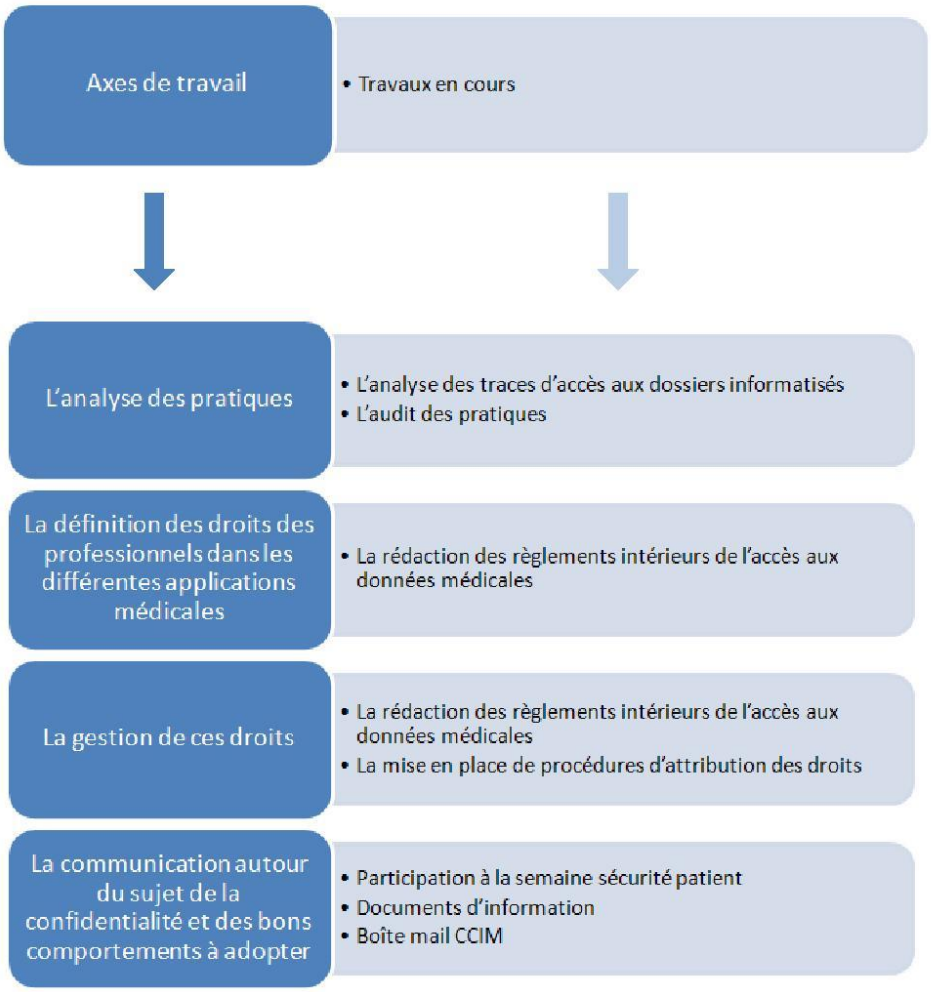
C'est une **commission** crée en 2011, composée de **représentants de divers services ou instances** du CHRU de Lille (COSI, DIM, DRN, SIAM, CME, DAJ, SCQSS, CSIRMT, CGS), du correspondant Informatique et Liberté, et pilotée par le Dr Theis (médecin responsable de l'information médicale et chef de service du DIM).

Quelles sont ses missions ?

Elle a **deux missions principales** :

- analyser les questions portant sur la confidentialité des données médicales
- définir puis mettre en place les procédures nécessaires pour en garantir le respect.

Semaine sécurité patient
Commission Confidentialité de l'Information Médicale
CCIM@chru-lille.fr



COSI : Comité Opérationnel du Système d'Information
DIM : Département d'Information Médicale
DRN : Département des Ressources Numériques
SIAM : Service de l'Information et des Archives Médicales
CME : Commission Médicale d'Etablissement
DAJ : Direction des Affaires Juridiques
SCQSS : Sous-Commission Qualité et Sécurité des Soins
CSIRMT : Commission des Soins Infirmiers de Rééducation Médico-Techniques
CGS : Coordination Générale des Soins

Semaine sécurité patient
Commission Confidentialité de l'Information Médicale
CCIM@chru-lille.fr

Réutilisation des données de santé dans le cadre de la recherche

Etre acteur de sa santé

La confidentialité, c'est aussi notre métier !

Faut-il informer les patients de la réutilisation de leurs données ?

La recherche non-interventionnelle réalisée au sein du CHRU sur les données des patients pris en charge ne nécessite pas l'accord individuel des patients. Ceux-ci doivent néanmoins être informés au moment de leur prise en charge, de la réutilisation possible de leurs données à des fins de recherche, et doivent pouvoir manifester leur opposition à ce moment-là.

Une recherche interventionnelle ou une recherche dont le promoteur est externe à l'établissement nécessite l'accord individuel des patients avant tout traitement de données (sauf dérogations accordées par la CNIL[1]).

Quand faut-il déclarer un fichier de données?

Toute réutilisation de données de santé doit faire l'objet d'une déclaration ou d'une demande d'autorisation à la CNIL. Voir intranet onglet

[1] Commission National de l'informatique et des libertés.

Semaine sécurité patient
Commission Confidentialité de l'Information Médicale
CCIM@chru-lille.fr

Comment protéger les données recueillies?

Les fichiers de données individuelles non cryptés ne doivent pas sortir de l'établissement.

Exceptions : les données ne permettant pas l'identification des individus ou les données agrégées (= non individuelles).

Qui est responsable de la protection des données ?

Le « responsable du traitement » des données (au sens de la CNIL) est responsable de la sécurité de celles-ci. Sa responsabilité pénale est engagée. En outre, tout professionnel en possession d'un fichier de données individuelles est tenu d'assurer au mieux la sécurité de ce fichier.

Semaine sécurité patient
Commission Confidentialité de l'Information Médicale
CCIM@chru-lille.fr

Secret professionnel

Etre acteur de sa santé

La confidentialité, c'est aussi notre métier !

Le secret médical et le secret professionnel n'ont pas les mêmes fondements juridiques mais ils concourent au même objectif **: le respect de la vie privée du patient.**
Nous parlerons ici de secret professionnel en considérant qu'il couvre le champ d'application du secret médical.

Qu'est-ce que le secret professionnel ?

Le secret professionnel couvre l'ensemble des informations concernant le patient et s'impose à l'ensemble du personnel du CHRU.

Le respect du secret professionnel se définit de deux manières:

- Un professionnel ne doit **jamais divulguer des informations** personnelles des patients, dont il a eu connaissance dans le cadre de sa fonction.

Semaine sécurité patient
Commission Confidentialité de l'Information Médicale
CCIM@chru-lille.fr

- Un professionnel ne doit **jamais chercher à obtenir des informations** sur une personne s'il ne participe pas à sa prise en charge.

Le secret professionnel, est-ce important ?

Oui, le secret professionnel est un droit fondamental pour chaque patient. Le respecter, c'est respecter nos patients.

Dans quel cadre est-il autorisé d'accéder à des informations médicales ?

En principe, **seule l'existence d'une relation de soin avec le patient permet l'accès à ses données de santé** et autorise la consultation de son dossier médical.

Néanmoins il existe des **dérogations prévues par décret**. Elles concernent notamment les activités de tarification, d'analyse de l'activité, de pharmacovigilance et de recherche.

Hors les cas prévus par la loi, si un professionnel divulgue ou accède à des informations médicales, il peut être poursuivi pour violation du secret professionnel.

Quelles sont les sanctions encourues en cas de non-respect du secret professionnel ?

Sanction pénale : jusqu'à un an d'emprisonnement et 15 000€ d'amende.

Sanction civile : paiement de dommages et intérêts selon le préjudice subi.

Sanction disciplinaire : pour faute professionnelle.

Semaine sécurité patient
Commission Confidentialité de l'Information Médicale
CCIM@chru-lille.fr

Annexe IV : Questionnaire d'évaluation des pratiques professionnelles de la CCIM

Centre Hospitalier Régional
Universitaire de Lille

Questionnaire relatif au secret professionnel et au respect de la confidentialité des données médicales contenues dans le dossier patient informatisé

Dans le cadre du renforcement de la politique de confidentialité, la CCIM (Commission Confidentialité de l'Information Médicale) réalise un audit afin de connaitre les pratiques actuelles en matière de confidentialité des données médicales. Pour ce faire, elle a mis en place le présent questionnaire.
Ce questionnaire de 25 questions dure entre 5 à 10 minutes. Il est **strictement anonyme, les connexions ne seront pas tracées** et il est important de répondre en toute sincérité à toutes les questions.
Merci par avance pour le temps que vous accorderez à ce questionnaire.

A) Profils et accès au système informatique :

1) Dans le cadre de votre fonction avez-vous une session personnelle pour accéder à un ordinateur (prénom.nom + mot de passe)? **OUI / NON** *(si NON, renvoi à la question 3)*

2) Si OUI, comment vous connectez- vous à votre session ?
   - O prénom.nom + mot de passe
   - O carte d'établissement + code PIN
   - O les deux
   - O je n'utilise jamais ma session personnelle

3) De par votre fonction, avez-vous accès aux applications médicales utilisées au CHRU de Lille (Sillage, Diane, ResUrgences, etc.) ? **OUI / NON** *(si NON, renvoi à la question 13)*

4) Avez-vous déjà donné votre mot de passe à quelqu'un d'autre ou utilisé le mot de passe de quelqu'un d'autre pour accéder à une application médicale (Sillage, Diane, ResUrgences…) ?
   - O J'ai déjà donné mon mot de passe à quelqu'un d'autre
   - O J'ai déjà utilisé le mot de passe de quelqu'un d'autre
   - O Les deux
   - O NON *(si NON, renvoi à la question 6)*

5) Si OUI, pour quelle(s) raison(s) ? *(plusieurs choix possibles)*
   - O Oubli du mot de passe
   - O Oubli de la carte d'établissement
   - O Nouveau professionnel sans compte
   - O Nouveau stagiaire sans compte
   - O Autres, précisez : *Question ouverte*

6) Travaillez-vous sur un poste partagé ? **OUI / NON / les 2** *(si NON, renvoi à la question 8)*

7) Comment travaillez-vous sur cet ordinateur partagé ?
   - O J'utilise la session générique de l'ordinateur
   - O Je travaille sur la session déjà ouverte (celle de quelqu'un d'autre)
   - O Je prends le temps de me déconnecter et de me connecter avec ma session personnelle
   - O Autres, précisez : *Question ouverte*

Contact : Joséphine Beharel, élève juriste
Josephine.BEHAREL@CHRU-LILLE.FR
V8 12/06

B) Accès au dossier médical informatisé du patient :

8) Par votre fonction, êtes-vous amenés à consulter des dossiers médicaux informatisés de patients ? **OUI / NON** *(si NON, renvoi à la question 13)*

9) Dans quelle(s) circonstance(s) vous arrive-t-il d'aller voir des dossiers médicaux informatisés de patients que vous n'avez pas pris en charge ?
   - O Pour aller consulter votre dossier personnel
   - O Pour consulter le dossier d'un membre de votre famille pris en charge au CHRUL
   - O Pour un proche qui vous a demandé des renseignements sur quelqu'un de sa famille pris en charge au CHRUL
   - O Par curiosité
   - O Pour se renseigner sur un personnel du CHRUL
   - O Pour inclure des patients dans une recherche
   - O Pour répondre à un avis médical
   - O Pour l'activité de tarification
   - O Pour la maintenance d'un logiciel
   - O Pour anticiper une prise en charge d'un patient dans le service
   - O Je ne le fais jamais
   - O Autre, précisez : *Question ouverte*

10) Selon vous, est-il permis de consulter le dossier médical informatisé d'un patient que vous n'avez pas pris en charge ? **OUI / NON**

11) Si vous utilisez Sillage, utilisez-vous « la demande d'accès étendu » dans Sillage ? *(si « jamais » ou « je n'utilise pas sillage » ou « non concerné », renvoi à la question 13)*
   - O Non concerné car mon profil me donne accès à toutes UF
   - O Jamais
   - O Au moins une fois par jour
   - O Au moins une fois par mois
   - O Au moins une fois par trimestre
   - O Au moins une fois par an
   - O Je ne sais pas ce qu'est l'accès étendu dans Sillage
   - O Je n'utilise pas Sillage

12) Dans quel cas utilisez-vous l'accès étendu dans Sillage ? *Question ouverte*

C) Connaissance des règlementations sur la confidentialité :

13) Lors de votre arrivée au CHRU de Lille, avez-vous eu des informations sur le comportement à adopter concernant le secret professionnel? **OUI / NON**

14) Avez-vous déjà vu ou lu des documents du CHRU de Lille sur le comportement à adopter par rapport au secret professionnel? **OUI / NON** *(si NON, renvoi à la question 16)*

15) Si OUI, lesquels ? *Réponse ouverte*

16) Saviez-vous que, dès que vous allez consulter un dossier patient informatisé, votre connexion est tracée et qu'il est possible de savoir quand, à quelle heure, et quelle(s) action(s) vous avez effectuée(s)? **OUI / NON**

17) Vous faites-vous soigner au CHRU de Lille ? **OUI / NON**

Contact : Joséphine Beharel, élève juriste
Josephine.BEHAREL@CHRU-LILLE.FR

18) Avez-vous déjà pensé à vous faire soigner dans un autre établissement parce que vos collègues pourraient consulter votre dossier médical informatisé ? **OUI / NON**

19) Selon vous, en cas de non-respect du secret professionnel, quel est le montant maximum de l'amende encourue ? *Liste déroulante* *(jusqu'à 1 000€, jusqu'à 5 000€, jusqu'à 10 000€, jusqu'à 15 000€)*

20) Selon vous, en cas de non-respect du secret professionnel, quelle est la durée maximale de la peine d'emprisonnement encourue ? *Liste déroulante* (aucune, jusqu'à 1 mois, jusqu'à 4 mois, jusqu'à 8 mois, jusqu'à 12 mois, jusqu'à 18 mois)

D) Communication des données médicales patients :

21) Emportez-vous des fichiers de données médicales informatisées de patients et/ou des dossiers médicaux papier à l'extérieur de l'établissement ? **OUI / NON / NON CONCERNE** *(non concerné : car pas d'accès aux données patients) (non et non concerné, renvoi à la question 23)*

22) Si OUI, pourquoi ? : *Question ouverte*

23) Avez-vous déjà communiqué des données médicales non cryptées de patients :
- O par mail
- O par les réseaux sociaux
- O par le partage collectif (ex : dropbox)
- O je n'ai jamais communiqué de données médicales de patients

24) Avez-vous déjà lu ou vu des affiches CNIL du CHRU de Lille ? **OUI / NON**

25) Est-ce que ces affiches se trouvent dans votre service ? **OUI / NON**

E) Questions générales :

Age : *Liste déroulante* ans

Depuis combien d'années travaillez-vous au CHRU de Lille ? *Liste déroulante* années

Personnel soignant/ Personnel non soignant ? *Liste déroulante*

Pôle/ Service/ Métier ? *Liste déroulante*

Question facultative : Dans le cadre d'une campagne de communication sur la confidentialité, quel serait le meilleur moyen pour vous, de communiquer des informations afin que celles-ci soient connues et comprises par tout le personnel du CHRU ?

Question ouverte

Contact : Joséphine Beharel, élève juriste
Josephine.BEHAREL@CHRU-LILLE.FR

MERCI DE VOTRE PARTICIPATION

« Parce que les professionnels du CHRU de Lille sont aussi des patients comme les autres… ».

En tant que personnel du CHRU de Lille, vous avez des droits mais aussi des devoirs.

Vos droits :

- Seul le personnel hospitalier vous prenant en charge au CHRU de Lille peut avoir accès à votre dossier médical informatisé ; excepté les cas de dérogation, expressément prévus par la loi (article L1110-4 Code de la Santé Publique)
- Si vous avez des doutes sur une personne qui aurait pu consulter votre dossier médical informatisé, vous pouvez faire part de votre crainte à votre cadre Supérieur de Santé ou directement à la Délégation des Affaires Juridiques (DAJ).

Vos devoirs :

- Il est strictement interdit de consulter le dossier médical informatisé d'un patient que vous n'avez pas pris en charge.

Pour information :

- Lorsque vous vous connectez à un dossier patient informatisé, cette connexion est tracée et identifiable.
- En cas de connexion irrégulière, cette trace peut constituer un commencement de preuve en cas de plainte.
- En cas de consultation irrégulière d'un dossier patient informatisé vous encourez une peine d'un an d'emprisonnement et une amende de 15 000 euros.
- http://intrachru/intranet-gapi/SSI/

Pour toutes questions supplémentaires, vous pouvez contacter la CCIM par mail CCIM@CHRU-LILLE.FR

La Commission Confidentialité de l'Information Médicale (CCIM) est une commission qui a été mise en place en 2011 dans le but d'analyser les questions portant sur la confidentialité des données médicales, puis de définir et de mettre en place les procédures pour en garantir le respect. Cette commission est pilotée par le Dr Theis, médecin responsable de l'information médicale. Elle est composée de représentants du SIAM (Secteur d'Information et des Archives Médicales), de la CME (Commission Médicale d'Etablissement), de la sous-commission qualité de la coordination générale des soins, du DRN (Département des Ressources Numériques), de la DAJ (Délégation des Affaires Juridiques), du COSI (Comité Opérationnel du Système d'Information), du DIM (Département de l'Information Médicale), ainsi que le CIL (Correspondant Informatique et Libertés) du CHRU.

Contact : Joséphine Beharel, élève juriste
Josephine.BEHAREL@CHRU-LILLE.FR
V8 12/06

Bibliographie

I/ Ouvrages, manuels et thèses

A. Ouvrages et manuels généraux

B. Ouvrages spéciaux

C. Contributions à un ouvrage

D. Thèses

II/ Articles et doctrines

III/ Rapports et études

IV/ Avis et délibérations

V/ Décisions commentées

I. Ouvrages, manuels et thèses

A. Ouvrages et manuels généraux

- CAPITANT, Henri. *Introduction à l'étude du droit civil*, A. Pédone, 5ème édition, 1929.

- CHAPUS, René. *Droit administratif général*, Tome 1, 15ème édition, Montchrestien, 2001.

- CORNU, Gérard. *Vocabulaire juridique*, PUF, 2011.

- Montesquieu. *De l'esprit des lois*, Partie 6, Livre XXIX « De la manière de composer les lois », 1758.

B. Ouvrages spéciaux

- BENSOUSSAN, Alain. *Informatique et libertés*, Francis Lefebvre, Paris, 2010.

- CATALA, Pierre. *Le droit à l'épreuve du numérique*, PUF, 1998.

- COELS, Jean-Marie, *Le droit des obligations à l'épreuve de la télémédecine*, PUAM, 2006.

- DESGENS-PASANAU, Guillaume. *La protection des données à caractère personnel*, Lexis-Nexis, 2ème édition, Paris, 2016.

- DUPONT, Marc. BERGOIGNAN-ESPER, Claudine. PAIRE, Christian. *Droit hospitalier*, Dalloz, 7éme édition, 2009.

- DUPUY, Olivier, *La gestion des informations relatives au patient*, Les études hospitalières, 2005.

- DUSSERRE, Liliane. DUCROT, Henry. ALLAERT, François-André. *L'information médicale, l'ordinateur et la loi*, Editions médicales internationales, 2éme édition, 1999.

- HOERNI, Bernard. *Ethique et déontologie médicale*, 2ème édition, Masson, 2000.

- LAUDE, Anne. TABUTEAU, Didier. *Droit de la santé*, 3ème édition, PUF, 2012.

- LECHOPIR, Nicolas. *Les valeurs de la recherche. Enquête sur la protection des données personnelles en épidémiologie*, Michalon, 2011.

- MACKAAY, Ejan. *Nouvelles technologies et propriété : actes du colloque tenu à la Faculté de droit de l'Université de Montréal, les 9 et 10 novembre 1989*, Thémis, 1991.

- MATTATIA, Fabrice. *Internet et les réseaux sociaux : que dit la loi ?*, 2ème édition, Eyrolles, 2016.

- MOQUET-ANGER, Marie-Laure. *Droit hospitalier*, 3ème édition, LGDJ, 2013.

- PY, Bruno. *Le secret professionnel*, L'Harmattan, 2005.

- SAISON-DEMARS, Johanne. *Droit hospitalier*, 3ème édition, Gualino, 2011.

- RIGAUX, François. POULLET, François. LEONARD, Thierry. *La vie privée une liberté comme les autres ?*, Larcier, 1992.

C. Contribution à un ouvrage

- CADIET, Loïc. *La notion d'information génétique en droit français*, *In La génétique humaine, de l'information à l'informatisation*, Thémis/Litec diffusion, 1992, p. 52.

- CAVERS, David. « Law and science, some points of confrontation », *in* « Law and the social role of science», *Rockefeller University Press*, 1966, p. 5.

- POULLET, Yves. LEONARD, Thierry, *Les libertés comme fondement de la protection des données nominatives*, *in* La vie privée, une liberté parmi les autres ?, Larcier, 1992.

- VERGES, Etienne. « L'évolution scientifique et technologique au prisme du droit : aperçu d'une relation à plusieurs facettes », *In* « Variations évolutions métamorphose », *PU St Etienne*, Institut universitaire de France, 2012, p. 371.

D. Thèses

- ETIEN-GNOAN, N'Da Brigitte. *L'encadrement juridique de la gestion électronique des données médicales*, thèse Lille, 2014.

- ZORN-MACREZ, Caroline. *Secret partagé et données de santé : pour un droit de la personne à la protection de ses données de santé partagées*, PUN, 2010.

- CAVALIER, Mathilde. *La propriété des données de santé*, thèse Lyon, 2016.

II. Rapports et études

- ASIP Santé.
    - *Programme de relance du DMP et des systèmes d'information partagés de santé*, synthèse de la concertation, Juillet 2009.
    - *Rapport d'activité,* 2012.

- Association Française des Hébergeurs Agréés de données de santé. *Les hébergeurs agréés de données de santé, acteurs clés de la confiance numérique en santé*, livre blanc de l'association française des hébergeurs agréés de données de santé, 2014.

- BRAIBANT, Guy. *Données personnelles et sociétés de l'information*, rapport au 1er ministre, La Documentation française, 1998.

- CATALA, Pierre. TRICOT, Bernard. *Rapport de la commission Informatique et libertés*, La Documentation française, 1975.

- CHAMBRE REGIONALE DES COMPTES. *CHRU de Lille, enquête système d'information hospitalier*, rapport d'observations définitives, 2016.

- COMITE D'AGREMENT DES HEBERGEURS.
    - Premier rapport d'activité, 2011.
    - Deuxième rapport d'activité, 2012-2013.

- CONSEIL D'ETAT
    - *Les autorités administratives indépendantes*, rapport public, La Documentation française, 2001.
    - *Le Droit souple*, étude annuelle du Conseil d'Etat, questions/réponses, 2013.
    - *Le numérique et les droits fondamentaux*, rapport public, La Documentation française, 2014.
    - *Le numérique et les droits fondamentaux*, étude annuelle, La documentation française, 2014.

- CONSEIL NATIONAL DE L'ORDRE DES MEDECINS
    - *Télématique de santé*, 2006.

- *L'informatisation de la santé*, livre blanc, 2008.
- *La télémédecine*, livre blanc, 2009.
- *Déontologie sur le web*, livre blanc, 2009.
- *Télémédecine et autres prestations médicales électroniques*, rapport de mission, 2016.

- COUR DES COMPTES

  - *Le partage des données entre les systèmes d'information,* rapport public annuel sur la sécurité sociale, chapitre X, 2007.
  - *L'accès en ligne aux dossiers médicaux*, rapport public annuel sur la sécurité sociale, Chapitre VII, 2008.
  - *Les systèmes d'information dans les E.P.S*, rapport public annuel sur la sécurité sociale, Chapitre VIII, 2008.
  - *La gestion du GIP Dossier médical personnel*, rapport public annuel, chapitre VI, 2009.
  - *Le coût du dossier médical personnel depuis sa mise en place*, communication à la commission des finances de l'assemblée nationale, 2012.
  - *La modernisation des systèmes d'information hospitaliers : une contribution à l'efficience du système de soins à renforcer*, rapport sur l'application des lois de financement de la sécurité sociale, Chapitre VIII, septembre 2016.

- DIONIS du SEJOUR, Jean. ETIENNE, Jean-Claude. *Les télécommunications à haut débit au service du système de santé*, rapport de l'office parlementaire d'évaluation des choix scientifiques et technologiques, La documentation française, 2004.

- DOOR, Jean-Pierre, *Rapport d'information sur le dossier médical personnel*, rapport déposé par la commission des affaires culturelles familiales et sociale de l'Assemblée Nationale, La documentation française, janvier 2008.

- DOSIERE, René. VANNESTE, Christian. *Rapport d'information sur les autorités administratives indépendantes*, rapport fait au nom du comité d'évaluation et de contrôle des politiques publiques, AN, 28 octobre 2010.

- ETIENNE, Jean-Claude. LASBORDES, Pierre. *Le dossier médical personnel (DMP) : quel bilan d'étape pour quelles perspectives ?*, rapport fait au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologique, Sénat, 2009.

- FAGNIEZ, Pierre-Louis, *Le masquage d'informations par le patient dans son DMP*, rapport au ministre de la santé et des solidarités, janvier 2007.

- FAROUDJA, Jean-Marie. *Questions sur l'informatisation des dossiers médicaux, le partage et l'hébergement des données,* rapport de la commission nationale permanente, adopté lors des assises du Conseil National de l'ordre des médecins du 18 juin 2005.

- FIESCHI, Marius. *Les données du patient partagées : la culture du partage et de la qualité des informations pour améliorer la qualité des soins*, rapport au ministre de la santé de la famille et des personnes handicapées, La Documentation française, janvier 2003.

- FOYER, Jean. *Rapport au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la république sur : le projet de loi (n° 2516) relatif à l'informatique et aux libertés, la proposition de loi (n° 1004) de Pierre-Bernard Cousté tendant à créer une commission de contrôle des moyens d'informatique afin d'assurer la protection de la vie privée et des libertés individuelles des citoyens , la proposition de loi (n° 3092) de François Villa et plusieurs de ses collègues sur les libertés, les fichiers et l'informatique*, Assemblée Nationale, t.1, n° 3125, Paris, 1977.

- GAGNEUX, Michel. *Refonder la gouvernance de la politique d'informatisation du système de santé. Douze propositions pour renforcer la cohérence et l'efficacité de l'action publique dans le domaine des systèmes d'information de santé*, La Documentation française, mai 2009.

- GAGNEUX, Michel. BOARETTO, Yann. CHOLLEY, François. *Rapport sur le dossier médical personnalisé (DMP),* Inspection générale des finances, La Documentation française, novembre 2007.

- GAGNEUX, Michel. COMBLE, Pierre-Henri. De KERGOMMEAUX, Loïc. *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé,* Inspection générale des affaires sociales, Avril 2008.

- GARREC, René. *Rapport n° 146 fait au nom de la commission des lois*, Projet de loi relatif aux archives, Sénat, décembre 2007.

- GRATIEUX, Laurent. OLLIVIER, Laurent. *Audit de l'organisation et du pilotage des organismes œuvrant à l'informatisation du système de santé*, IGAS, Rapport n° 2006-113, novembre 2006.

- GT33CSIS-CSF. *Permettre l'émergence d'une stratégie industrielle en matière de e-santé, en soutien de la politique de santé publique, en associant les industriels. Lever les freins au déploiement de la télémédecine*, rapport élaboré par le groupe de travail

sur la télémédecine réuni dans le cadre du Comité Stratégique de Filière Santé, mai 2015.

- Haute Autorité de Santé

  - *Efficience de la télémédecine : état des lieux de la littérature internationale et cadre d'évolution*, juillet 2013. disponible sur [http://www.has-sante.fr] Consulté le 15 mai 2017.

  - *Les protocoles de coopération article 51 de la loi HPST*, Rapport d'activité de la HAS 2013, disponible sur [http://www.has-sante.fr] Consulté le 15 mai 2017.

- JÉGOU, Jean-Jacques.

  - *L'informatisation dans le secteur de la santé : prendre enfin la mesure des enjeux*, rapport d'information fait au nom de la commission des finances, Sénat, 2005.

  - *Systèmes d'information de santé : le diagnostic est posé, le traitement s'impose*, rapport d'information fait au nom de la commission des finances, Sénat, 17 octobre 2007.

- LABORDES, Pierre.

  - *Rapport sur le Dossier médical personnel (DMP) : quel bilan d'étape pour quelles perspectives ?*, office parlementaire d'évaluation des choix scientifiques et technologiques, La Documentation française, 2008.

  - *La télésanté : un nouvel atout au service de notre bien-être*, La documentation française, 2009.

- PICARD, Jean-Marie. *Dossier Médical Personnel : proposition de contenu*, enquête qualitative menée auprès de professionnels sous l'égide de la CNAMTS.

- PONSOT, Dominique, *Valeur juridique des documents conservés sur support photographique ou numérique*, La documentation Française, septembre 1995.

- SENAT. *La qualité de la loi*, les documents de travail du Sénat, série études juridiques, septembre 2007.

- SIMON, Pierre. ACKER, Dominique. *La place de la télémédecine dans l'organisation des soins*, Direction de l'Hospitalisation et de l'Organisation des Soins, 2008.

- TÜRK, Alex. *Rapport relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Sénat, 2003.

- VASSELLE, Alain. *Rapport n°424 fait au nom de la commission des affaires sociales*, projet de loi relatif à l'assurance maladie, juillet 2004.

III. Articles

- ABIKHZER, Franck. « Le délai raisonnable dans le contentieux administratif : un fruit parvenu à maturité ? », *AJDA*, 2005, p. 985.

- ALLAERT, François-André. QUANTIN, Catherine. « Le dossier personnel du patient : réflexions sur le portail d'accès unique et le masquage du dossier », *IRBM*, 2009, p. 144

- ANTOINE, Dominique. « La formation professionnelle dans la fonction publique en France – Compte rendu d'un rapport de la promotion René Cassin de l'ENA », *RF adm. publ.*, 2002, n° 104, p. 611.

- AYELA, Christophe. « Le droit de la preuve en France », *Gaz. Pal.*, 2012, n° 45, p. 15.

- BACACHE-GIBEILI, Mireille. « Le secret médical partagé », *Gaz. Pal.*, 2008, n° 365, p. 44.

- BAHR, Anne. BULACH, Claudette. FABER, Stéphanie « Comment appliquer la loi Informatique et Libertés à la recherche médicale ? », *RGDM*, 2012, n° 45, p. 54.

- BALLET, Philippe. « Où en est la procédure d'agrément des hébergeurs de données de santé à caractère personnel ? », *Gaz. Pal.*, 2007, n° 109, p. 20.

- BANAT-BERGER, Françoise. « Archives et protection des données personnelles », *Revue Lamy Droit de l'Immatériel*, 2013, n° 95, p. 93.

- BARBRY, Eric. « L'ordonnance relative aux communications électronique : cherchez la faille », *Gaz. Pal.*, 2011, n° 288, p. 12.

- BAREGE, Alexandre. BOSSU, Bernard. « Les TIC et le contrôle de l'activité du salarié », *JCP-S*, 2013, n° 41, p. 13.

- BARY, Marion. « L'existence contestable d'un droit subjectif à l'information », *LPA*, 2010, n° 195, p. 15.

- BEAUJEAN, Isabelle. « L'inquiétant devenir des dossiers des patients conservés par les établissements publics de santé au-delà du délai de 25 ans », *RDS*, n° 45, 2012, p. 36.

- BERANGER, Jérôme. Le COZ, Pierre. « Réflexion éthique sur la pluridisciplinarité et la confidentialité de l'information en imagerie médicale via les nouvelles technologies de l'information et de la communication », *Cancer/radiothérapie*, 2012, n° 16, p. 215.

- BERGOIGNAN-ESPER, Claudine. « Le respect du secret médical dans la législation de notre pays: réalité ou illusion ? », *D.*, 2008, p. 1918.

- BERGONZOL, Frédéric. « Preuves de force chez les Tiers de confiance », solutions et logiciels [en ligne], 2011, disponible sur [http://www.solutions-numeriques.com], consulté le 15 mai 2017.

- BICLET, Philippe.

    - « Hébergement et échange des données de santé », *Médecine et droit*, 2010, p. 159.
    - « Le dossier médical dans tous ses états », *Médecine et droit*, 2006, p. 174.

- BOILEAU Chrystelle. « L'équipe médicale : une existence évidente pour le professionnel de santé, mais discutable pour le juriste », *RGDM*, 2004, n° 14, p. 34.

- BOIZARD, Maryline. « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », *Communication commerce électronique*, n° 3, mars 2016, étude 6.

- BORGETTO, Michel. LE GOFFIC, Caroline. « La télémédecine », *RDSS*, 2011, n° 6, p. 985.

- BOSSI, Jeanne.

    - « Comment organiser la protection des données de santé ? », *RDSS*, 2010, n° 2, p. 208.

    - « Le rôle de l'agence des systèmes d'information partagés de santé dans la procédure d'agrément », *Actualités JuriSanté*, 2011, n°74, p. 9.

    - « La circulation des données de santé », *RGDM*, 2004, numéro spécial, p. 55.

    - « Le cadre juridique du partage d'information dans les domaines sanitaires et médicosocial. Etat des lieux et perspectives. », *Médecine et droit*, 2013, p. 6.

- BOUDIN, Agnès. DESMARAIS, Pierre. « La fourniture de prestations de service par un établissement de santé public », *JCP Administrations et collectivités territoriales*, 2012, p. 2041.

- BOUNEDJOUM, Amira. « Réforme européenne des données personnelles : les nouveautés pour les droits des personnes », *JCS Entreprises et Affaires*, 2016, n° 22, p. 1327.

- BOURDAIRE-MIGNOT, Camille. « Téléconsultation : quelles exigences ? Quelles pratiques ? », *RDS*, 2011, p. 1003.

- BOURGEOIS, Matthieu. BOUNEDJOUM, Amira. « Réforme européenne des données personnelles : registres internes et DPO, la nécessaire réorganisation des entreprises », *JCP Entreprises et Affaires*, n° 22, juin 2016, p. 1326.

- BOYER-BEVIERE, Bénédicte « Les principales réformes de la loi n° 201-300 du 5 mars 2012 sur les recherches impliquant la personne humaine, *RGDM*, n° 44, 2012, p. 225.

- BRAC DE LA PERRIERE, Marguerite. FERRE, Elise. « L'hébergement des données de santé, des textes à la pratique », *Gaz. Pal.*, 2011, n° 204, p. 21.

- BRISSY, Stéphane. « Les définitions des catégories de recherches sur la personne et leurs évolutions », *Gaz. Pal.*, 2009, n° 143, p. 11.

- BRUNET, François. « De la procédure au procès : le pouvoir de sanction des autorités administratives indépendantes », *RFDA*, 2013, n° 28, p. 113.

- CAMBON, Linda. « Objets connectés, mobiles, communicants en prévention : dépasser l'outil, penser l'intervention… », *Santé Publique*, 2016, vol. 28, n° 1, p. 5.

- CAPRIOLI, Eric.

    - « Le Conseil d'Etat annule deux sanctions prononcées par la CNIL », *Communication commerce électronique*, 2010, n° 2, p. 42.
    - « Charte informatique et droit du travail », *Communication commerce électronique*, n° 7-8, juillet 2001, commentaire 101.

- CARCASSONNE, Guy. « Penser la loi », *Pouvoirs*, septembre 2005, p. 39.

- CASSIA, Paul. « La sécurité juridique, un « nouveau » principe général du droit aux multiples facettes », *Dalloz*, 2006, p. 1190.

- CASTETS-RENARD, Céline. « Brève analyse du règlement général relatif à la protection des données personnes », *Dalloz IP/IT*, 2016, p. 331.

- CHEMTOB-CONCE, Marie-Catherine.

    - « Dossier médical personnel et dossier pharmaceutique ». *Gaz. Pal.*, 2007, n° 174, p. 2.

    - « La protection des données de santé à caractère personnel », *RGDM*, 2004, numéro spécial, p. 111.

- CHEMTOB-CONCE, Marie-Christine. CAILLEUX, Anne. « L'impact des nouvelles dispositions de la loi relative aux recherches impliquant la personne humaine », *Médecine et droit*, 2013, p. 30.

- CONTIS, Maïalen. « La télémédecine : nouveaux enjeux, nouvelles perspectives juridiques », *RDSS*, 2010, n° 2, p.235.

- CORGAS-BERNARD, Cristina. « Responsabilité civile médicale et nouvelles pratiques numériques : l'exemple de la télémédecine », *LPA*, 2014, n° 164, p. 27.

- CORMIER, Maxence. « L'informatisation des archives médicales hospitalières », *RDSS*, 1994, p. 456.

- COYOL, Jérôme. « Réflexion sur la responsabilité médicale à la suite de l'introduction du dossier médical personnel (DMP) », *Médecine et droit*, 2006, p. 85.

- DALEAU, Jeanne. « République numérique : après la consultation publique, la discussion parlementaire », *Dalloz actualités*, 28 janvier 2016

- DAVER, Corinne. « La télémédecine entre intérêts des patients et responsabilité », *Médecine et droit*, 2000, n° 41, p. 21.

- DEBOST, Claire.

    - « La généralisation de la messagerie sécurisée, un pas de plus vers l'échange d'informations personnelles de santé sécurisé », *RDS*, 2014, p. 955.

    - « L'appréhension juridique de la relation de soin au prisme des nouvelles technologies », *Jurisdoctoria*, n° 8, 2012, p. 104.

- DE CLAUSSADE, Jocelyne. « Sécurité juridique et complexité du droit : considérations générales du Conseil d'Etat », *Recueil Dalloz*, 2006, p. 737.

- DE GIVRY, Emmanuel. « Tic et surveillance du salarié : regards de la CNIL », *JCP-S*, octobre 2013, n° 41, p. 24.

- DE LARD, Brigitte. « Hébergement de données et coopération », *Actualités Jurisanté*, 2011, n° 74, p. 6.

- DE LAMBERTERIE, Isabelle. LUCAS, Henri-Jacques. « Informatique, libertés et recherche médicale », *CNRS éd.*, 2001, p. 68.

- DE LAMBERTERIE, Isabelle. «La place du consentement dans la collecte et le traitement des informations sensibles. La situation en France », *RGDM*, n° 13, 2004, p. 62.

- DE MONTCLER, Marie-Christine.
    - « Le droit souple entre dans le prétoire », *AJDA*, 2016, p. 572.
    - « Délai de recours contre les actes de droit souple », AJDA, 2016, p 1481.

- De MONTVALON, Luc. « Droit à la déconnexion : l'arbre qui cache la forêt ? », *Semaine sociale Lamy*, novembre 2016, n° 1743, p. 19.

- DERAEDT, Guillaume. « Carte d'établissement, gestion des identités et des rôles », *Revue hospitalière de France*, 2010, p. 34.

- DESBORDES, Marie. « La télémédecine en psychiatrie du sujet âgé : enjeux et perspectives La télémédecine en psychiatrie du sujet âgé : enjeux et perspectives », *NPG Neurologie - Psychiatrie - Gériatrie*, Volume 15, 2015, p. 270.

- DESMARAIS, Pierre.
    - « La télémédecine, source de nouveaux cas de responsabilité. », *Communication commerce électronique*, n° 9, étude n° 16, septembre 2011.
    - « Quel régime pour la m-health ? », *Communication Commerce électronique*, n° 3, étude 5, 2013.

- DUMESNIL, Chloé, « Informatisation des données et protection du secret : l'exemple des travaux de la commission de confidentialité des informations médicales du CHRU de Lille », *RGDM*, n° 61, décembre 2016, p. 79.

- DUTHEILLET de LAMOTHE, Louis. « Un recours souple pour le droit souple », *AJDA*, 2016, p. 717.

- EVIN, Claude. « le secret médical dans le cadre hospitalier », *recueil Dalloz* [en ligne], 2009, disponible sur [http://bu.dalloz.fr], consulté le 15 mai 2017.

- FANTONI-QUINTON, Sophie. LEBORGNE-INGELAERE, Céline. « L'impact des TIC sur la santé au travail », *JCP-S*, novembre 2013, n° 48, p. 16.

- FLAVIN, Patrick. « De la responsabilité encourue dans le cadre de la télémédecine », *Revue hospitalière de France*, 2010, n° 537, p. 56.

- FERRAUD-CIANDET, Nathalie. « Questions juridiques sur l'e-santé », *LPA*, n°89, p.11.

- FOREST, David. « Pouvoirs de sanction de la CNIL : le réveil soudain de la belle endormie », *Recueil Dalloz*, 2007, p. 94.

- FORGERON, Jean-François. BENEAT, Anne-Lise. « De la santé électronique à l'hôpital numérique », *Gaz. Pal.* , 2009, n° 295, pp. 5-10.

- FORGERON, Jean-François. BELAY, Nathalie. « Les applications de la télémédecine : responsabilités médicales traditionnelles aux responsabilités techniques nouvelles », *Gaz. Pal.*, 2001, n° 289, p. 20.

- FRAYSSINET, Jean. « Le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi modifiée du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », *RLDI*, 2005, n°11, p. 24.

- GAGNON, Marie-Pierre. BRETON, Erik. « L'influence des technologies de l'information et des communications sur le maintien en poste des infirmières », *Santé Publique*, 2013/3 (Vol. 25), p. 126.

- GAURIAU, Bernard. « Les TIC et l'action syndicale », *JCP-S*, octobre 2013, n° 41, p. 18.

- GAVAUDAN, Jérôme. ABEILLE, Jean-François. « Le secret professionnel, le secret médical et l'avocat », *RDSS*, 2011, numéro hors-série, p. 65.

- GAY, Laurence, « Jurisprudence du Conseil constitutionnel », *RFDC*, n° 50, avril-juin 2002, p. 385.

- GENOT-POK, Isabelle. « Des archives publiques aux archives hospitalières : points de droit », *Actualités Jurisanté*, 2010, n° 69, p.4.

- GERVAIS, Jean-Bernard. « L'hôpital, une zone de non droit ? », *Décision santé*, supplément au n° 270, 2010, p. 4.

- GIOCANTI, Dominique. « Les différentes acceptions des termes « dossier médical » et, dans ce contexte, situation du dossier hospitalier », *RGDM*, 2010, n° 37, p. 161.

- GIROT, Clarisse. WOLTON, Elise. « Informatique et libertés ? Pouvoirs de sanctions de la CNIL : rupture et continuité. », *Expertises des systèmes d'information*, 2011, n° 361, p. 295.

- GOUT, Olivier. « Rapport introductif. Notion et enjeux des concours de responsabilités », *Responsabilité civile et assurances*, 2012, n° 2. Disponible sur [http://www.lexisnexis.com], consulté le 15 mai 2017.

- GRIDEL, Jean-Pierre. « L'entreprise et l'utilisation en justice de l'information issue de l'outil informatique mis à la disposition du salarié pour les besoins de son activité professionnelle. En hommage à la haute mémoire du professeur Pierre Catala », *Communication commerce électronique*, n° 7-8, juillet 2016, étude n° 13.

- GRIGUER, Merav. « Quel cadre légal pour l'e-santé ? », *Cahiers de droit de l'entreprise*, n° 5, Septembre 2016, prat. 25.

- GROS Jeannette, « Santé et nouvelles technologies de l'information », *Journal officiel de la République française, avis et rapports du Conseil économique et social*, 2002, p. 4.

- HARDY, Jacques. « Les catégories juridiques à l'épreuve de la réforme administrative. Le Cas des groupements hospitaliers de territoire », *AJDA*, 2017, p. 919

- HERVIEU-BEGUE, Marie. GIROUD, Maurice. BEJOT, Yannick. «Un réseau de télémédecine pour AVC », *Soins Aides-Soignantes*, Volume 14, 2017, p. 13.

- HUNTER, L. RULE, J « Vers un droit de propriété des renseignements personnels », Communication au congrès de l'association canadienne française pour l'avancement de la science, Montréal, mai 1994.

- JEGOUZO, Yves. « L'étude d'impact : formalité ou garantie de la qualité de la loi ? », *AJDA*, 2012, p. 1425.

- JOB, Jean-Marie. « La loi Informatiques et libertés et les données de santé », *RLDI*, n° 34, 2008, p. 87.

- JONAS, Carol. « La loi du 4 mars 2002 et la pratique médicale quotidienne : apports et incertitudes », *Médecine et droit*, 2002 n° 56, p.1.

- KAHN, Axel. « Le secret médical, d'Hippocrate à Internet », *Recueil Dalloz*, 2009, disponible sur [http://bu.dalloz.fr], consulté le 15 mai 2017.

- KELLER, Catherine. MOQUET-ANGER, Marie-Laure. « Les outils juridiques de coopération issus de la loi HPST : des instruments au servie de la restructuration de l'offre hospitalière ? », *RDSS*, 2013, p. 687.

- KHODOSS, Hélène. « L'exploitation des données de santé », *RGDM*, 2004, numéro spécial, p. 65.

- KRZICH, Delphine. « Force normative et efficacité des recommandations de bonne pratique en matière médicale », *RDSS*, 2014, p. 1087.

- LA BŒUF, Dominique. « La télémédecine en France, du concept à la pratique », *Soins*, Volume 61, 2016, p. 28.

- LAIGNEAU, Jean-François. « Sécurité et développement des recherches : de la loi Bertrand à la loi Jardé », *médecine et droit*, 2012, n° 117, p.163.

- LALLET, Alexandre. THIELLAY, Jean-Philippe. « La commission d'accès aux documents administratifs a trente ans », *AJDA*, 208, p. 1415.

- LAMBERTERIE, Isabelle. « Qu'est-ce qu'une donnée de santé ? », *RGDM*, 2004, numéro spécial, p. 11.

- LANDAIS, Claire. LE NICA, Frédéric. « Sécurité juridique : la consécration », *AJDA*, 2006, p. 1028.

- LANTERO, Caroline. « Les hôpitaux et la responsabilité du fait des produits de santé défectueux », *RDA* [en ligne], 2012, n° 4, disponible sur [http://bu.dalloz.fr], consulté le 15 mai 2017.

- LASSERRE, Daniel. « Dossier médical et informatique », *Droit, déontologie et soin*, juin 2005, vol. 5, n° 2, p. 194.

- LAUDE, Anne. « L'encadrement juridique de l'innovation », *Les tribunes de la santé*, 1/2004, n°2, p. 37.

- LE CLAINCHE, Julien. « Pouvoirs a posteriori de la CNIL : les risques de l'excès de prudence », *RDLI*, 2005, n° 11, p. 43.

- LE COZ, Pierre. « Avis de CCNE à propos des questions soulevées par l'informatisation des données de santé », *RGDM*, 2010, n°37, p. 199.

- LEDUC, Fabrice. « Pas de requiem prématuré pour l'arrêt Mercier », *RDC*, 2011, n° 1, p. 345.

- LE GOFFIC, Caroline. « Consentement et confidentialité à l'épreuve de la télémédecine », *RDSS*, 2011, p. 987.

- LEMAIRE, François. « Pourquoi faut-il encore réformer la législation de la recherche biomédicale ? », *Médecine et droit*, 2011, n° 106, p. 28.

- LEPAGE, Agathe. « Loi du 6 août 2004. Réflexions de droit pénal sur la loi du 6 août 2004 relative à la protection des personnes à l'égard des traitements de données à caractère personnel », *Communication commerce électronique*, 2005, n° 2, étude n° 9.

- LEQUILLERIER, Clémentine. « "L'ubérisation" de la santé », *Dalloz IP/IT*, 2017, p. 155.

- LEROYER, Anne-Marie. « Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine », *RTD Civ.*, 2012, p. 384.

- LUCAZEAUX, Gilles. « La justice pénale et les informations médicales», *RGDM*, n° 20, 2006, p. 189.

- LYON-CAEN, Gérard. « Débat autour de l'arrêt Nikon France », *Semaine Sociale Lamy*, [en ligne], nº 1046, 15 octobre 2001, disponible sur [http://lamyline.lamy.fr]

- MALLET-POUJOL, Nathalie.

    - « Appropriation de l'information : l'éternelle chimère », *Recueil Dalloz*, [en ligne], 1997, n° 23, disponible sur [http://bu.dalloz.fr], consulté le 15 mai 2017.

    - « Droit à et droit sur l'information de santé », *RGDM*, 2004, numéro spécial, p. 77.

- MANAOUIL, Cécile. « Le dossier médical personnel (DMP) : « autopsie » d'un projet ambitieux ? », *Médecine et droit*, [en ligne], 2009, disponible [www.sciencedirect.com], consulté le 15 mai 2017.

- MARKUS, Jean-Paul. « Nature juridique des recommandations de bonnes pratiques médicales », *AJDA*, 2006, p 308.

- MARLIAC-NEGRIER, Claire. « La protection des données nominatives informatiques en matière de recherche médicale » Tome 1, *PUAM*, 2001, p. 106.

- MARTIN, Raymond. « Aller et retour de Kelsen à Aristote », *RDT civ.*, 1997, p. 387.

- MARTIN, Sébastien. « Les autorités publiques indépendantes : réflexions autour d'une nouvelle personne publique », *Revue de droit public et de la science politique en France et à l'étranger*, 2013, n° 1, p. 53.

- MARZOUG, Sanaa. « L'hébergement des données de santé à caractère personnel des établissements de santé : quelques repères juridiques », *Actualités JuriSanté*, 2011, n° 74, p. 4.

- MATHIEU, Bertrand. « Les lois de finances au crible de la sécurité juridique», *LPA*, n° 10, 2006, p. 4.

- MATHIEU, Chantal. PERETIE, Marie-Madeleine. PICAULT, Alex. « Le droit à la déconnexion, une chimère ? », *Revue droit du travail Dalloz*, octobre 2016, n° 10, p. 592.

- MATTATIA, Fabrice. « CNIL et tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés ? », *Revue de science criminelle et de droit pénal comparé*, 2009, n° 2, p. 317.

- MAXWELL, Winstaon. TAIEB, Sarah. « L'accountability, symbole d'une influence américaine sur le règlement européen des données personnelles ? », *Dalloz IP/IT*, 2016, p. 123.

- MELLERAY, Fabrice. « L'arrêt KPMG consacre-t-il vraiment le principe de sécurité juridique ? », *AJDA*, 2006, p. 897.

- MILANO, Laure. « Contrôle de constitutionnalité et qualité de la loi », *Revue de droit public*, n° 3, 2006, p. 637.

- MONNIER, Anne. « Le dossier médical personnel : histoire, encadrement juridique et perspectives », *RDSS*, 2009, n° 4, p. 625.

- MORLET-HAÏDARA, Lydia. RAHAL-LÖFSKOG Délia. « La télémédecine et la protection des données de santé par la loi informatique et libertés », *RGDM*, n° 44, 2012, p. 341.

- MORVAN, Patrick. « Le principe de sécurité juridique : l'antidote au poison de l'insécurité juridique ? », *Droit social*, 2006, p. 707.

- OBERDORFF, Henri. « La responsabilité d'un établissement public de santé est distincte de la responsabilité du fait des produits défectueux », *JCP-A*, 2012, n° 10-11, p. 2088.

- PACTEAU, Bernard, « La sécurité juridique, un principe qui nous manque ? », *AJDA*, numéro spécial 1995, p. 151.

- PEIGNE, Jérôme. « Les tribulations de la responsabilité hospitalière du fait des produits de santé défectueux », *RDSS*, 2011, p. 95.

- PERRAY, Romain. « Traitement de données personnelles dans le cadre de recherches médicales : vers un allégement des formalités », *Revue Lamy droit de l'immatériel*, 2007, n° 24, p. 64.

- PERRIER-BONNET, Sabine. « Une consultation de télémédecine dans le cadre d'un réseau plaies et cicatrisation », La Revue de l'Infirmière, Volume 65, 2016, p. 35.

- PIDOUX, Estelle. « La responsabilité médicale au regard de la télétransmission et de la télémédecine », *LPA*, 2000, N° 149, p. 5.

- PORCHY-SIMON, Stéphanie. « Revirement de la Cour de cassation quant à la sanction du défaut d'information du patient », *JCP-G*, 2010, n° 28, p. 788.

- PREUVOT, Perrine. « L'amélioration de l'application des lois : un enjeu dans la relation Parlement-Gouvernement », *Revue de droit public et de la science politique en France et à l'étranger* [en ligne], 2012, n°1, disponible sur [www.lextenso.fr], consulté le 15 mai 2017.

- PY, Bruno. « Conclusions sur les aspects juridique », RGDM, n° 20, 2006, p. 239.

- RAYNOUARD, Arnaud. « Le droit de l'écrit électronique », *LPA*, 2001, n° 65, p. 15.

- REBOUL-MAUPIN, Nadège.
    - « Responsabilité des médecins et Internet », *Gaz. Pal.*, 2002, n° 85, p. 28.
    - « Déontologie et Internet », *Gaz. Pal.*, 2002, n° 85, p. 22.

- REMY, Claire. « Les aspects juridiques de la dématérialisation des documents », *Solutions et logiciels*, 2010, n°12, p. 30.

- RENARD, Isabelle. « Preuve informatique – valeur juridique du document numérique », *Expertises*, 2010, p 215.

- RICHARD, Jacky. « Droit souple : pour une doctrine de recours et d'emploi », *Recueil Dalloz*, 2013, p. 2512.

- ROBIN, Jean-Yves. « L'urgence numérique. Faire de la France un leader de l'e-santé », *L'Harmattan*, 2015, p. 88.

- ROUSSEL, Bruno. « Informatisation des dossiers médicaux en milieu hospitalier : intégrité et opposabilité des données numériques », *Communication commerce électronique*, 2009, n° 6, étude 15.

- SABOURIN, Pierre. « Les autorités administratives indépendantes : une catégorie nouvelle », *AJDA*, 1983, p. 275.

- SAISON-DEMARS, Johanne. « Modernisation du système de santé : une gouvernance hospitalière à géométrie variable ». *RDSS*, 2016, p. 633.

- SAMARCQ, Nicolas. BRIOIS, Sébastien. « Données de santé à caractère personnel : les enjeux de la diffusion des TIC », *Expertises*, 2010, p. 382.

- SARR, Minata. « Droit souple et commerce électronique », *Jurisdoctoria*, 2012, n°8, p. 52.

- SAUTEL, Olivier. « Le dossier médical personnel », *Journal de médecine légale*, 2007, p. 6.

- SAVIN, Patricia. TESSALONIKOS, Arnaud. « Big data, santé et droit : quelle combinaison idéale ? », *Techniques hospitalières*, 2015, n° 753, p. 26.

- SERAICHE, Rhislène. « Petit rappel sur le commencement de preuve par écrit », *Gaz. Pal*., 2012, n° 89, p.12.

- SICARD, Didier. « Quelles limites au secret médical partagé », *recueil Dalloz*, [en ligne] 2009, disponible sur [http://bu.dalloz.fr], consulté le 15 mai 2017.

- STEFANI, François. « Le secret médical à l'épreuve des nouvelles technologies », *Recueil Dalloz*, 2009, n° 39, p. 2636.

- SOULAS DE RUSSEL, Dominique. RAIMBAULT, Philippe. « Nature et racines du principe de sécurité juridique : une mise au point », revue internationale de droit comparé, 2003, n° 1, p. 85.

- THIBIERGE, Catherine. « Réflexion sur les textures du droit », *RTD civ*., 2003, p. 599.

- TIERS, Gonzague. CAPON, Catherine. CLEMENTE, Hélène. « Télémédecine en région Nord-Pas de Calais », *ITBM-RBM*, 2000, 271-4.

- TRUCHET, Didier. « Que dit la loi », *RGDM*, N°20, 2006, p. 67.

- VACARIE, Isabelle. « La finalité des traitements de données de santé », *RGDM*, 2004, numéro spécial, pp. 27-34.

- VARNIER, Frédéric. « La coopération hospitalière au service de la modernisation de notre système de santé », *RDSS*, 2016, n° 4, p. 620.

- VAYR, Jonathan. « Les données de santé, un enjeu pour le futur », *LPA*, septembre 2016, n° 185-186, p. 4.

- VIALLA, François.

    - « Dossier patient, DMP : quelles frontières », *RGDM*, n° 20, 2006, p. 135

- « Secret et DMP », *RDS*, 2005, p. 42.

- VINET, Camille. « Responsabilité de l'hôpital du fait des produits défectueux ? », *AJDA*, 2010, p. 1485.

- VIOUJAS, Vincent. « La télémédecine : entre expérimentations réussies et généralisation au ralenti », *RDSS*, 2015, p. 681.

- VEILLEROT, Guy. « Le dossier hospitalier », *RGDM*, 2010, n° 37, p. 177.

- WALLE, Emmanuelle. « A nouvelles technologies, nouvelles causes de licenciement », *Gaz. Pal.*, 23 avril 2011, n° 113, p. 20.

- WARUSFEL, Bertrand. « Le droit des nouvelles technologies : entre technique et civilisation », La lettre de la rue Saint Guillaume, *Revue des Anciens élèves de Sciences-Po*, n° 127, juin 2002, p. 52.

- ZORN, Caroline. BELLIVIER, Florence. NOIVILLE, Christine. « Gestion et partage des données de santé : un démarrage poussif du contrat », *Revue des contrats* [en ligne], 2009, n° 2, p. 711, disponible sur [http://www.lextenso.fr]. Consulté le 15 mai 2017.

- ZORN, Caroline.
  - « Chronique martienne des données de santé numérisées », *RDS*, 2010, n° 36, p. 331.
  - « Les dossiers médicaux des défunts : des archives publiques non communicables », *Revue Lamy Droit de l'Immatériel*, 2010, n° 56, p. 63.

IV. Avis et délibérations

- CNIL.

    - Délibération n° 2005-003 du 13 janvier 2005 décidant la dispense de déclaration des traitements mis en œuvre par les organismes publics dans le cadre de la dématérialisation des marchés publics, *JORF* n° 55 du 6 mars 2006, p. 3875.

    - Délibération CNIL n°81-094 du 21 juillet 1981 portant adoption d'une recommandation relative aux mesures générales de sécurité des systèmes informatiques.

    - Délibération CNIL n°2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel.

    - Délibération CNIL n° 2007-036 du 20 février 2007 portant avis sur deux projets d'arrêtés relatifs, d'une part, aux spécifications physiques et logiques de la carte d'assurance maladie et aux données y étant contenues et, d'autre part, aux conditions d'émission et de gestion des cartes d'assurance maladie. *JORF* n°65 du 17 mars 2007, p. 4983.

- Comité Consultatif National d'Ethique, « le Dossier médical personnel et l'informatisation des données de santé », avis n° 104, juin 2008.

V. Décisions commentées

- BON, P. *Concl*. et note sous C.E., 5 janvier 2000, Consorts Telle c./AP-HP, n°181899, RFDA, 2000, p. 646.

- BRETON, A., note sous Cass. civ., 20 mai 1936, Dr Nicolas c/ époux Mercier, S. 1937, I, p. 321.

- CHAUVAUX, D. *Concl*. sous C.E., Sect., 5 janvier 2000, Consorts Telle c/ AP-HP, n°181899, *RFDA*, 2000, p. 641.

- CHAVRIER, G. « Création prétorienne d'un régime de responsabilité sans faute du service public hospitalier en cas de défaillance dommageable des produits et appareils de santé », note sous CE, 9 juillet 2003, n° 220437, Assistance publique-Hôpitaux de Paris c./ Mme M.Sera, *JCP-A*, n° 41, 2003, p. 1302.

- DUBOUIS, L. Note sous C.E., 5 janvier 2000, Consorts Telle c./AP-HP, n°181899, *RDSS*, 2000, p. 357.

- DE FORGES, J.-M. Note sous C.E., Ass., 9 avril 1993, Bianchi, n°69336, *RDSS* 1994, p. 108

- DEYGAS, S. Note sous CE, 18 décembre 2002, n° 233618, Mme Duvignères, *Procédures*, 2003, n° 154. AJDA, 2003, p. 487, chron. F. DONNAT et D. CASAS.

- DONNAT, F. CASAS, D. *Chron*. CE, 18 décembre 2002, n° 233618, Mme Duvignères, *AJDA*, 2003, p. 487.

- GUETTIER, C.

    - Note sous C.E., 5 janvier 2000, Consorts Telle c./AP-HP, n°181899, *Revue de droit public*, 2001, p. 4012.

    - Note sous CE, 9 juillet 2003, Assistance publique-Hôpitaux de Paris c/ Mme Marzouk, n° 220437, *JCP-A*, n° 41, 2003, p. 1302.

- LANDAIS, C. LE NICA F. Note sous CE, 24 mars 2006, KPMG et autres, n° 288460 et s, *AJDA*, 2006, p. 1028.

- LOSCHAK, D. Note sous CE, 11 décembre 1970, n° 78880, *Crédit foncier de France, D*. 1971, p. 674.

- MATTER, P. *Concl*. sous Cass. civ., 20 mai 1936, Dr Nicolas c/ époux Mercier, *D*., 1936, p. 88.

- MOQUET-ANGER, M.L. Note sous CE, 24 septembre 2012, n° 339285, *JCP-A*, n° 1, 2013, 2001.

- SARGOS, P. Note sous Cass. civ., 3 juin 2010, n° 0913591, *D.*, 2010, p. 1522.

- VIOUJAS, V. note sous arrêt CAA Marseille, 25 juin 2009, centre hospitalier intercommunal de Toulon-La-Seyne, n° 07MA02024, *RDSS*, 2009, p. 1155.

Index alphabétique

Les numéros renvoient aux paragraphes.

A

Agence Régionale de Santé : 33, 378, 385-389, 546-560, 563, 573, 576 et s., 672, 763, 783, 789, 796.

Agrément : 152, 179 et s., 182-189, 212, 215, 224, 232, 300, 332, 393, 659.

Archives

- ~ hospitalières : 124, 157, 162-168, 174, 193, 207.
- ~ publiques : 124, 156, 158-169, 174-177, 202, 206, 251, 659.

Article 29 (Groupe de l'.) : 65, 67, 104, 645.

ASIP santé : 183, 185-187, 195, 219, 243-245, 277, 306, 312, 325, 341, 346, 355,-356, 361, 410, 478, 501, 503 et s., 518-521, 527-529, 537-540, 545, 558 et s., 576, 619, 763.

Autodétermination informelle : 116-118, 661, 667.

Autorité Administrative Indépendante (AAI) : 81, 83, 93, 634, 713.

C

Carte de Professionnel de Santé (CPS) : 130 et s., 195, 244-247, 250, 407, 484, 504, 515, 531, 544, 758.

Clarté de la loi : 582-584.

Comité d'agrément : 187, 232-235, 659.

Commission d'Accès aux Documents Administratifs (CADA) : 169, 239 et s., 174-177.

Commission Nationale de l'Informatique et des Libertés (CNIL) : 47, 85, 89, 93, 97, 101 et s.,106, 140, 146-152, 171-173, 181-185, 240, 242, 291, 300-305, 325, 358, 379, 391, 458, 693, 713, 782.

Consentement

- ~ aux soins : 21, 427, 431, 434 et s., 437.
- ~ au traitement automatisé des données : 55, 59, 96, 97-98, 103-107, 116, 647-649.
- ~ à l'hébergement des données : 225-232, 658.
- ~ à l'ouverture d'un DMP : 274, 286, 295, 335-338, 341, 346, 360.

Coopération : 48, 219-224, 320, 394-397, 401, 407, 550, 555, 559, 561-568, 571, 574, 576, 662, 679.

D

Data Protection Officer (DPO) : 652.

Décret confidentialité : 130 et s., 242, 245 et s., 248, 616, 618, 620.

Données de santé (définition) : 62-65

Données personnelles (protection des ~) : 48-51, 66, 78, 227, 592, 646 et s., 592, 646 et s., 660 et s.,667, 707, 798.

Dossier (définition)

- ~ Hospitalier : 265.
- ~ Médical Electronique : 269, 271, 281.
- ~ Médical Partagé : 268, 274-282.
- ~ Pharmaceutique : 267.

Droit souple : 623, 631-639, 642, 669, 671, 707.

Droit à l'oubli : 54, 170 et s., 651.

E

Equipe de soins : 126-129, 150, 772.

Etablissement public de santé (définition) : 4.

Responsabilité des ~ : 458, 460, 463.

Evaluation des pratiques professionnelles (EPP) : 789, 791.

F

Formation professionnelle : 727-734, 741.

G

Groupement

- ~ d'Intérêt Economique (GIE) : 224.
- ~ d'Intérêt Public (GIP) : 223, 511-517.
- ~ Hospitalier de Territoire (GHT) : 561-577, 657, 672, 796.

Gouvernance des systèmes d'information hospitaliers : 476-485, 489-500, 504-510, 518, 520-523.

H

Hébergement de données : 179, 212 et s., 215, 218, 222, 659.
Hébergeur de données : 184, 211 et s., 214, 218, 393.
Hôpital (voir établissement de santé)

I

Identifiant National de Santé (INS) : 324, 326, 505, 527 et s.
Intelligibilité de la loi : 582-584, 588.
Interopérabilité : 243, 247, 325, 420, 482, 485, 488, 490 et s., 497, 504 et s., 522-527, 532, 534-541, 544-546, 572, 576 et s., 619 et s., 683.

N

Numéro d'inscription au Répertoire (NIR) : 324-326, 410, 527, 529, 542, 545, 576.

P

Propriété (des données de santé) : 110 et s., 115, 118-124, 605, 667.

R

Recommandations de Bonnes Pratiques (RBP) : 639-641.
Référentiels de sécurité : 181, 242, 620.
Réseaux sociaux : 607 et s., 720, 765.

S

SAFARI (projet) : 44.
Secret

- ~ médical : 150, 175, 207, 251, 288, 331, 346, 475, 790.
- ~ partagé : 126, 129, 132, 150, 153, 235, 346, 430, 772.
- ~ professionnel : 22, 65, 71-73, 78, 99, 108, 125, 128, 145, 150 et s., 173, 234, 288, 331-333, 346, 530, 608, 738, 772, 787, 790 et s. 798.

Sécurité juridique (définition) : 585-589.
Système d'information hospitalier (définition) : 682-683.

T

Tarification à l'activité (T2A) : 629, 681.
Technologies de l'Information et de la Communication (définition) : 2.
Télémédecine : 10 et s., 13, 25-29, 212, 367-399, 402-405, 407, 410, 426-433, 435, 437-442, 445-450, 455, 464-469, 733, 746, 745.
Téléconsultation : 11, 25 et s., 374, 383, 407, 436, 438, 445.
Téléexpertise : 8, 12, 375, 383, 434, 445 et s., 448, 450.
Téléprescription : 371, 407.

V

Vie privée : 21, 22, 37, 44, 46, 48, 56, 86, 333-334, 473, 578, 605-607, 646, 660, 710 et s., 714, 718.

Table des matières

Remerciements 1
Sommaire 1
Principales abréviations 3
Introduction Générale 7
§1. Les multiples possibilités offertes par l'introduction des TIC dans la pratique médicale ... 9
A. Les TIC, nouvel espoir pour les prises en charges difficiles 10
B. Les TIC, outil majeur dans la mise en place d'actions de prévention en santé. 13
§2. Les TIC, des outils sources de risques éthiques et juridiques majeurs 15
A. Les risques pesant sur la vie privée du patient 15
B. Les risques « d'ubérisation » de la médecine : la nouvelle crainte 17
§3. Problématique de la thèse 20
PREMIERE PARTIE LE CADRE JURIDIQUE DE L'UTILISATION DES TIC A L'HÔPITAL, UN CADRE INCOMPLET 23
TITRE 1 TIC ET INFORMATISATION DES DONNEES DE SANTE : UN CADRE PARFOIS INADAPTE 27
Chapitre 1 Le traitement informatisé des données du patient 29
Section 1. La protection des données du patient 30
§1. La législation de droit commun à disposition du droit de la santé 30
A. La loi Informatique et Libertés, pilier de l'encadrement 30
1) La France parmi les précurseurs 30
2) Une protection forte 34
B. La protection spécifique des données de santé 39
1) Les données de santé, des données sensibles 39
2) Des mécanismes de protection propres aux données de santé 43
§2. Une protection à l'efficacité relative 48
A. Le contrôle et la sanction du non-respect de la loi Informatique et Libertés : des mesures disproportionnées ? 48
1) La CNIL, une autorité administrative indépendante dotée d'un pouvoir de contrôle nécessaire 48
2) La limite des sanctions prévues par les textes 51
B. La protection limitée des données de santé 56
1) Les limites de l'interdiction de traitement des données sensibles 56
2) Le consentement mis à mal 60
Conclusion de la Section 63
Section 2. Les modalités de partage des données relatives au patient. 64

§1. Les règles générales 64
A. La délicate question de la propriété des données de santé 65
1) La recherche d'une qualification du droit des individus sur leurs données..... 65
2) Tentative de qualification du droit des professionnels de santé sur le dossier médical .. 68
B. La difficile application des règles relatives au secret partagé 72
1) Le secret partagé, une dérogation au secret professionnel strictement encadrée..... 72
2) Les limites de l'application du secret partagé aux TIC 75
§2. Le cas particulier de la recherche médicale : des règles de protection spécifiques..... 77
A. Le cadre juridique des recherches impliquant la personne humaine..... 77
B. L'encadrement particulier des traitements des données de santé dans le cadre de la recherche 80
1) Les principes applicables aux traitements de données à caractère personnel dans le cadre de la recherche médicale 81
2) Les Méthodologies de Références MR001 et MR003 83
C. Les données de santé utilisées dans le cadre de la recherche, des données moins bien protégées ?..... 85
Conclusion de la section..... 89
Conclusion du chapitre..... 91
Chapitre 2 Les modalités de conservation et de communication des informations relatives aux patients..... 93
Section 1. La conservation des données de santé en tant qu'archives hospitalières 95
§1. Les règles spécifiques aux archives publiques..... 95
A. Les conséquences de la qualification d'archives publiques. 96
1) Définitions légales 96
2) Conséquences juridiques..... 98
a) Les conséquences relatives à la durée de conservation des données..... 98
b) Les conséquences relatives à la suppression des données..... 100
B. Archives publiques, archives hospitalières et secret médical : des règles parfois en opposition..... 103
§2. La conservation à l'ère des TIC : le cadre de l'hébergement des données de santé 106
A. L'hébergement des données de santé : de l'agrément à la certification..... 106
1) Des règles à la mise en place laborieuse..... 107
2) L'agrément des hébergeurs : une procédure critiquée..... 109
a) Points essentiels de la procédure..... 109
b) Une procédure remise en cause 110
c) L'adoption définitive d'une procédure de certification 112
B. La reprise de l'existant : l'éventualité de la numérisation des dossiers papier..... 113

1) Les conditions de la numérisation des dossiers existants 114
a) Les règles applicables en droit commun 115
2) Le devenir des dossiers papier numérisés 119
a) La réponse des Archives de France 119
b) Les apports de la loi de modernisation de notre système de santé 121
Conclusion de la section 122
Section 2. Hébergement et communication des données : un cadre limité 123
§1. L'hébergement des données de santé, un cadre incomplet 123
A. Choix de l'hébergeur et questions en suspens 123
1) L'hypothèse d'un établissement de santé hébergeur de données 124
2) Quelles conditions pour le choix du tiers hébergeur ? 126
a) L'obligation d'un marché public 126
b) Les possibilités de coopération 127
B. Quelle place laissée au respect du droit des patients ? 130
1) La disparition progressive du consentement 130
a) Le consentement, élément initialement essentiel à l'hébergement 130
b) Le consentement : du principe à l'exception 131
c) La disparition du consentement au profit de la non opposition 132
2) Le médecin de l'hébergeur, garant du respect de la confidentialité des données 133
§2. La construction laborieuse du cadre relatif à la communication des données de santé 135
A. La communication des données de santé : des prescriptions difficilement applicables en l'état 135
1) Des questions en suspens 135
2) Des référentiels non parus 137
B. L'utilisation systématique de la carte de professionnel de santé : une utopie abandonnée 139
Conclusion de la section 142
Conclusion du chapitre 143
Conclusion du titre 145
TITRE 2 TIC ET PRISE EN CHARGE MEDICALE : UN CADRE EN EVOLUTION 147
Chapitre 1 La dématérialisation des dossiers médicaux : l'exemple du DMP 149
Section 1. Le DMP, un Dossier médical électronique institutionnel 150
§1. La place incertaine du DMP dans le champ des dossiers médicaux 150
A. Tentative de délimitation du cadre juridique des DME 151
1) Le dossier médical : un dossier aux formes multiples. 151
2) Délimitation des contours du DME 154

B. DMP, DME et autres dossiers médicaux : une articulation indispensable 157
1) Le DMP, un projet novateur 157
2) Le DMP, complément ou concurrent des autres dossiers ?..... 159
§2. Le DMP, un encadrement juridique évoluant avec difficultés 162
A. Les premiers pas du DMP : des orientations incertaines..... 162
1) Origines et principes fondamentaux du DMP 162
2) Des évolutions au gré des critiques..... 165
a) Les apports pratiques 165
b) Les apports sur le fond 166
B. Une rapide remise en question du projet initial 168
1) Un premier bilan négatif 168
a) Le rapport GAGNEUX..... 168
b) Le bilan de la CNIL 169
2) Une première relance mitigée..... 171
3) La loi de modernisation de notre système de santé, un nouveau souffle pour le DMP . 172
Conclusion de la section..... 175
Section 2. Le DMP : les limites d'un projet ambitieux 176
§1. Des ambitions louables mais démesurées 176
A. Un outil plein de promesses 176
1) L'amélioration et la coordination des soins, un enjeu majeur..... 177
2) La sécurité de l'outil, une priorité 178
B. Des lacunes certaines..... 181
1) Le DMP, un outil à géométrie variable..... 181
2) Les droits et devoirs des patients, un manque de clarté 182
§2. Un outil à l'avenir incertain 185
A. Un outil mal perçu..... 186
1) DMP et responsabilité 186
2) La théorie du masquage 189
B. Un projet voué à l'échec ? 191
1) Le coût important du DMP 191
2) Les bémols face à la relance de la loi de modernisation de notre système de santé 193
Conclusion de la section..... 196
Conclusion du chapitre..... 197
Chapitre 2 L'utilisation des TIC dans la prise en charge du patient 199
Section 1. La prise en charge à distance, un cadre naissant 200

§1. La télémédecine, une pratique ancienne récemment consacrée par le législateur 200
A. Un cadre spécifique strictement défini par la loi HPST 201
1) La télémédecine, seule pratique à distance légalement définie 201
a) Définition des différentes pratiques 201
b) Les cinq actes de télémédecine 203
2) Une procédure préalable stricte 204
B. Un cadre lourd, frein au développement de l'activité ? 206
1) Etat des lieux de l'activité en France 207
2) Le poids des procédures préalables 208
a) La contractualisation avec les acteurs 208
b) Les procédures induites par l'activité. 209
3) Pistes d'évolution 213
§2. L'informatisation des prescriptions médicales, un cadre en construction 215
A. La prescription par voie électronique, une possibilité encore limitée 215
1) La prescription par e-mail, une possibilité légalement encadrée 215
2) Les voies de déploiement de la e-prescription 218
a) La note d'orientation du CLIO santé 218
b) Le projet européen EPSOS 219
B. La prescription informatisée, une pratique encouragée par les pouvoirs publics 220
1) L'incitation à l'informatisation du circuit du médicament 220
2) La certification obligatoire des logiciels de prescription médicale 223
Conclusion de section 225
Section 2. Prise en charge médicale et TIC : des règles de responsabilité bousculées 226
§1. Droit des usagers et responsabilité médicale : l'adaptation du droit commun 226
A. Information et consentement du patient : une obligation maintenue et renforcée 226
1) L'obligation classique étendue aux spécificités des TIC 227
2) La mise en œuvre des droits des patients 230
a) La question de la forme de l'information 230
b) La preuve de l'information et du recueil du consentement 232
B. Responsabilité médicale : des règles classiques aux risques d'application multipliés 234
1) La responsabilité médicale, une responsabilité pour faute 234
2) La répartition de la responsabilité entre les différents acteurs de la télémédecine 236
§2. Télémédecine et responsabilité : des règles spécifiques à prendre en considération 239
A. Défaillance des logiciels et responsabilités 240

1) Qualification juridique des logiciels 240
2) Responsabilité du fait des produits défectueux 242
B. Nouveaux acteurs et nouvelles responsabilités 246
Conclusion de section 250
Conclusion du chapitre 251
Conclusion du titre 253
Conclusion de la première partie 255
SECONDE PARTIE LES VOIES DE SECURISATION DE L'UTILISATION DES TIC A L'HOPITAL 257
TITRE 1 L'IMPULSION DE LA SECURISATION AU NIVEAU NATIONAL 259
Chapitre 1 Une gouvernance forte des systèmes d'information en santé, une priorité 261
Section 1. L'éparpillement notable de la gouvernance actuelle 262
§1. Des difficultés pour instaurer une gouvernance stable et efficace 262
A. L'évolution de la gouvernance des systèmes d'information en santé en France 262
1) Les structures de coordination 263
a) La Mission pour l'informatisation du système de santé 263
b) Le Conseil supérieur des systèmes d'information de santé 264
2) Les structures opérationnelles 265
a) Le groupement pour la modernisation du système d'information hospitalier 265
b) La Mission Nationale d'Appui à l'Investissement Hospitalier 267
c) Les GIP DMP et CPS 268
B. Un bilan mitigé 269
1) Les rapports de la Cour des comptes 269
2) Le rapport de l'IGAS 271
C. Les propositions GAGNEUX et FIESHI 272
§2. Un manque de visibilité sur la gouvernance des projets en cours 274
A. Le nouvel organigramme de la gouvernance des SIS 274
1) Une structure de coordination : la délégation à la stratégie des systèmes d'information de santé 274
2) Des structures opérationnelles en appui 276
a) L'ASIP Santé 276
b) L'agence Nationale d'Appui à la Performance 278
B. Les limites de cette nouvelle organisation 279
1) Le schéma de gouvernance choisi par l'Etat 279
a) L'ASIP, une nouvelle venue dans le paysage des agences de l'Etat. 279
b) L'ASIP, un GIP sous tutelle 280

2) Un manque de visibilité des projets en cours 283
Conclusion de la section 285
Section 2. Les défis à relever pour une gouvernance efficace 286
§1. L'interopérabilité des SI, un chantier prioritaire 286
A. Enjeux d'une problématique ancienne 286
1) Périmètre de l'interopérabilité 287
2) Préalables nécessaire à l'interopérabilité 287
a) Une identification unifiée des patients. 287
b) L'identification des professionnels 289
3) La normalisation des systèmes : la condition technique essentielle 290
B. L'interopérabilité, une problématique insoluble ? 291
1) Le cadre d'interopérabilité des SIS 291
2) Les obstacles au développement de l'interopérabilité. 293
§2. La place stratégique des acteurs régionaux dans la gouvernance des SIS 295
A. L'ARS, acteur charnière dans la mise en œuvre des politiques relatives aux SIS. ... 295
1) L'ARS, « bras armé » de l'Etat en matière de politiques de santé. 296
2) L'ARS, acteur essentiel de la stratégie hôpital numérique 298
3) Les maîtrises d'ouvrage régionales, appuis stratégiques aux ARS 300
B. Les GHT, nouveaux acteurs stratégiques pour le SIS. 301
1) Les GHT une forme atypique de coopération 301
a) Spécificité des GHT 302
b) Des questions en suspens. 304
2) La mutualisation des SIS entre établissements de santé 307
Conclusion de la section 311
Conclusion du chapitre 313
Chapitre 2 La refonte du cadre juridique, un effort nécessaire 315
Section 1. Le cadre juridique actuel, source d'insécurité juridique 316
§1. Retour sur la notion de sécurité juridique 316
A. Portées des principes de clarté et d'intelligibilité de la norme 317
1) Définition des principes 317
2) Des composantes d'un concept plus large : celui de sécurité juridique 319
B. Les outils de lutte contre l'insécurité juridique 321
1) Les origines variées de l'insécurité juridique 322
2) Les pistes de sécurisation du droit 324
§2. La complexité du cadre juridique s'appliquant aux TIC en santé 327

A. L'utilisation des TIC à l'hôpital, une pratique évoluant dans des environnements normatifs distincts 327
1) Multiplicité des matières à prendre en compte 328
2) L'empilement législatif et règlementaire relatif aux TIC en santé 332
B. Un cadre juridique source d'incertitudes 334
Conclusion de la section 338
Section 2. Un cadre juridique à repenser 339
§1. Le cadre actuel, frein au développement pérenne des TIC à l'hôpital 339
A. L'encadrement juridique de l'innovation, un équilibre délicat 339
B. Le recours au droit souple, une solution à envisager 343
1) La notion de droit souple. 344
2) Le développement du droit souple pour encadrer les TIC en santé. 346
§2. Le législateur sur la voie de la modernisation du cadre juridique 350
A. Une volonté européenne d'unifier la protection des données personnelles 350
1) Une procédure législative longue et délicate. 350
2) La mise en place d'un cadre rénové 352
a) Le renforcement du droit des personnes 352
b) Un nouveau cadre de contrôle et de sanction 354
C) Des nouvelles formalités 356
B. Une volonté française de moderniser le cadre applicable 357
1) La loi de modernisation de notre système de santé, patch correctif de certains dysfonctionnements 357
2) La loi pour une République numérique 358
a) Les travaux préalables du Conseil d'Etat 358
b) Les enjeux de la loi 360
Conclusion de la section 363
Conclusion du chapitre 365
Conclusion du titre 367
TITRE 2 LES ETABLISSEMENTS DE SANTE, ACTEURS CLES DE LA SECURISATION DE L'UTILISATION DES TIC A L'HÔPITAL 369
Chapitre 1 Les établissements de santé, au cœur de la sécurisation de leurs pratiques 371
Section 1. Les pistes de sécurisation a priori 372
§1. La gestion stratégique de l'informatisation à l'hôpital 372
A. Le Système d'information hospitalier 372
1) Bref rappel historique 372
2) Tentative de définition de la notion de système d'information hospitalier 374

B. Une gestion stratégique indispensable 375
§ 2. L'appui sur des ressources qualifiées 378
A. Le recrutement de compétences spécialisées 378
B. L'appel aux ressources extérieures 382
1) L'aide à la conception du SIH 383
2) L'appui à la maîtrise d'ouvrage 384
Conclusion de la section 386
Section 2. Les pistes de sécurisation *a posteriori* 387
§1. L'utilisation d'outils juridiques 387
A. Le contrôle et la limitation de l'utilisation des TIC 388
1) Le droit à la vie privée dans le cadre professionnel : enjeux et limites 389
a) La messagerie professionnelle 389
b) L'utilisation d'Internet et du matériel informatique à des fins privées 391
2) Les possibilités de régulation et de contrôle offertes à l'employeur 392
B. La mise en place d'une charte informatique 395
§2. L'utilisation d'outils managériaux 399
A. La formation des utilisateurs 400
1) La formation professionnelle, une obligation légale réciproque 400
2) La formation professionnelle, un outil managérial stratégique 403
B. La sanction d'une mauvaise utilisation des TIC 404
1) Le cadre d'exercice du pouvoir disciplinaire 405
2) La sanction d'un mésusage des TIC 406
Conclusion de la section 408
Conclusion du chapitre 409
Chapitre 2 Un exemple de sécurisation réussie : le CHRU de Lille 411
Section 1. Une volonté marquée de sécuriser l'utilisation des TIC en santé 413
§1. Une organisation interne tournée vers la sécurité du SIH 413
A. Présentation de l'organisation du CHRU en matière de SIH 414
1) La gouvernance du SIH 414
2) La gestion stratégique du SIH 416
B. Le développement de projets ambitieux relatifs à la sécurité 417
1) Le projet carte d'établissement 417
2) Le projet Système de Management de la Sécurité du Système d'information (SMSSI) . 418
§2. La diffusion d'une culture de la sécurité informatique 421
A. La sensibilisation des utilisateurs du SIH 421
1) Les formations 421

2) Les actions de communication 422
B. La mise en place de chartes informatiques 423
Conclusion de section 425
Section 2. Une volonté affirmée de protéger les données de santé 426
§1. La création de structures ad'hoc pour gérer la confidentialité des données de santé ... 426
A. La Commission Confidentialité de l'Information Médicale (CCIM) 427
1) Contexte de la création de la CCIM 427
2) Missions et évolution de la CCIM 429
B. Le Comité CNIL 430
§2. Bilan des réalisations de ces structures novatrices 432
A. L'élaboration d'une réglementation interne 432
B. Analyse et sanction des accès indus 434
C. La labellisation de l'action de la CCIM 436
Conclusion de la section 439
Conclusion du chapitre 441
Conclusion du titre 443
Conclusion de la seconde partie 445
Conclusion générale 447
Table des Annexes 451
Annexe I. Schéma de l'organisation en briques fonctionnelles d'un SIH type 452
Annexe II : Présentation et modalités d'obtention du label "droits des usagers" 453

Parcours de santé : usagers, vos droits

Cahier des charges du label et du concours
2016-2017

Mai 2016

..... 453

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES
ET DE LA SANTÉ

STRATÉGIE
NATIONALE
DE SANTÉ

..... 454

I | Le contexte

Le label « Droits des usagers de la santé » a été initié dans le cadre du dispositif « 2011, année des patients et de leurs droits ». Il vise à valoriser des expériences exemplaires et des projets innovants en matière de promotion des droits des usagers. Reconduit en 2015 et étendu au champ médico-social et social, le bilan de la labellisation s'avère très positif :

- une dynamique régionale effective et constante avec 21 régions sur 26 impliquées ;
- une répartition territoriale confortée avec plus de 160 projets examinés par les commissions spécialisées « Droits des usagers » (CSDU) des conférences régionales de la santé et de l'autonomie (CRSA) ;
- un nombre de candidats au concours en augmentation ;
- plus de 60 projets labellisés en région, tous valorisés sur l'espace « Droits des usagers de la santé » du site du ministère chargé de la santé :

www.espace-droits-usagers.sante.gouv.fr

Dans ce contexte, il a été décidé de rééditer l'expérience de labellisation en 2016-2017, en tenant compte d'une part, du retour d'expérience de l'édition 2015, de l'avis de la commission spécialisée « droits des usagers » (CSDU) de la conférence nationale de santé (CNS), des observations formulées par les agences régionales de santé (ARS) et d'autre part, des résultats de l'étude réalisée par l'école des hautes études en santé publique (EHESP) à l'initiative du ministère et relative à la participation des usagers ou de leurs représentants.

En 2015, les projets labellisés concernaient majoritairement les actions d'information, de formation des professionnels de santé intégrant la participation des usagers et de leurs représentants.
Dans une moindre mesure, les projets labellisés portaient sur des initiatives en lien avec la médiation en santé, le traitement des réclamations et des plaintes ou encore l'évolution du système de santé.
L'édition 2016-2017 accompagne voire préfigure la mise en œuvre des lois dites : vieillissement, santé et fin de vie et renforçant les droits des usagers dans la logique de parcours – de santé, de soins, de vie – et intégrant les recommandations de la conférence nationale de santé et la nécessité d'une identification d'un « dénominateur commun » des droits individuels et collectifs qui « traverse » le secteur des soins de ville, le secteur hospitalier et le secteur social et médico-social, tant en établissement qu'à domicile au moyen d'une charte de la personne dans son parcours de santé et des professionnels l'accompagnant.
Elle permet une continuité entre le dispositif de labellisation et la 6ème édition du concours « Droits des usagers de la santé » qui viendra récompenser, les meilleurs projets labellisés, dans la limite de 2 par région. La sélection est faite par les ARS, après avis de la CSDU des CRSA, et en lien, le cas échéant, avec les DRJSCS, puis communiquée au ministère chargé de la santé. Un jury représentant les différentes composantes du système de santé examinera les projets labellisés sélectionnés par les ARS et décernera des prix à 5 lauréats dont les projets auront été jugés particulièrement exemplaires.

A titre d'exemple, le jury du concours 2015 a récompensé 5 lauréats parmi les projets labellisés en région :

-Association Médecins du Monde de Rouen (Haute-Normandie) | Prévention et réduction des risques pour les personnes travailleuses du sexe
-Centre hospitalier d'Argenteuil (Ile-de-France) | Intégration des proches dans la prise en charge du patient en réanimation
-Hôpital local Jean-Baptiste-Caron de Crèvecœur-le-Grand (Picardie) | Accompagnement de la douleur à domicile
-Hospitalité Saint-Thomas-de-Villeneuve de Lamballe (Bretagne) | Développement de la démocratie en santé
-EPSM Lille Métropole (Nord-Pas-de-Calais) | Chronique du tiers exclu

Les 5 projets mettent en avant **des démarches intégrant pleinement la participation des usagers, des patients ou des résidents aux projets** de la simple information à la co-construction des projets en tant que telle.

Par ailleurs, **les initiatives « ouvrant les murs » des établissements de santé, des services de soins ou des structures spécialisées** et permettant, ainsi, d'aller à la rencontre des populations concernées – entre autre à domicile – ont été particulièrement distingués par le jury.

Enfin, l'une des actions promue illustre concrètement la démocratie sanitaire en développant **les actions de type participatif** au sein d'un établissement de santé.

Les 5 projets sont modélisables, transposables : ils s'inscrivent dans la durée, s'attachent à favoriser l'appropriation des droits par tous – y compris par des populations en situation difficile -. Ils ont une visée pédagogique, sont originaux ou comblent un vide : chacun d'entre eux a reçu du ministère un prix de 2 000€.

En 2016-2017 comme en 2015, le label et le concours seront ouverts à tous les acteurs du système de santé qui souhaitent s'engager dans une action innovante autour de la promotion des droits des usagers, et aux collectivités territoriales qui développent, pour certaines, des projets expérimentaux au niveau de leurs territoires.

Concernant les professionnels de santé, le label converge vers les objectifs poursuivis par le conseil national de l'ordre des médecins en faveur du renforcement du respect du droit à l'information et à l'accompagnement des patients, tant par les médecins libéraux qu'hospitaliers et salariés.

II | Le périmètre du label et du concours 2016-2017 « Droits des usagers de la santé »

Les thématiques privilégiées

En 2016-2017 comme en 2015, les axes thématiques s'appuient sur les recommandations issues des rapports sur les droits des usagers de la CNS et sur la

mission confiée à la CNS en vue d'élaborer une charte de la personne dans son parcours personnalisé de santé et des professionnels l'accompagnant.

Six axes thématiques, non exhaustifs, seront particulièrement privilégiés :

- renforcer et préserver l'accès à la santé – y compris à la prévention – pour tous, notamment par **une information adaptée** aux personnes vulnérables (mineures, majeures protégées, en perte d'autonomie, souffrant de troubles psychiques, intellectuellement déficientes etc.), étrangères, placées sous main de justice, etc. ;
- sensibiliser les professionnels de santé au moyen d'**actions de formation** aux droits des usagers ;
- favoriser **la médiation en santé** dans les structures de soins, médico-sociales et à domicile en mobilisant, entre autres, les médiateurs tels que les médiateurs médicaux, les médiateurs non-médicaux, les personnes qualifiées, etc. ;
- faire converger les droits des usagers des structures de soins, sociales et médico-sociales, notamment au travers de **la participation des représentants des usagers et des usagers** (Commission des usagers (CDU), Conseil de la vie sociale (CVS) et de la mise en place de dispositifs expérimentaux adaptés aux parcours (organisation territoriale pour l'exercice des droits impliquant les établissements, conseils généraux, ordres et organisations professionnels, ARS, les conseils territoriaux de santé, etc.) ;
- renforcer **l'effectivité** des droits des usagers par le traitement des réclamations et des plaintes en lien avec les représentants des usagers, quels que soient les destinataires de ces plaintes ou réclamations (établissements, conseils généraux, ordres et organisations professionnels, ARS, les conseils territoriaux de santé, etc.) et par l'analyse systématique des motifs notamment à partir des rapports des CDU ou des CVS et la mise en œuvre de mesures d'amélioration ;
- accompagner **les évolutions du système de santé** dans le respect des droits des usagers (e-santé, télémédecine, maisons et centres de santé, soins de santé transfrontaliers, développement de la chirurgie ambulatoire, etc.).

Ces thématiques, sont indicatives et serviront de guide pour l'attribution du label et des prix du concours.

Les candidats admissibles à la labellisation 2016-2017

Ils relèvent des 4 catégories éligibles au label « Droits des usagers de la santé », en phase avec le champ de compétence et le périmètre d'action des ARS voire des DRJSCS :

- les associations et les fondations exerçant leur activité dans le domaine de la santé et le secteur médico-social comme les associations d'usagers ou les associations et organisations professionnelles ;
- les établissements de santé, sociaux et médico-sociaux ;
- les professionnels de santé exerçant une activité libérale en ville, que ce soit à titre individuel ou dans le cadre d'un regroupement (réseaux de santé, structures de proximité, maison ou centre de santé, etc.) ou de service d'intérêt général dédiés à la prévention (services de PMI, santé scolaire et universitaire, santé au travail) ou encore dans un service de soins à domicile ;

- les institutions et les organismes susceptibles de conduire des actions de promotion des droits : ARS, agences sanitaires, collectivités territoriales, caisses d'assurance maladie, mutuelles, organismes de recherche, etc.

La nature des projets labellisables

Toute action visant à promouvoir les droits individuels et collectifs des usagers est susceptible d'être labellisée, dans la mesure où elle présente **un caractère innovant et reproductible**.

L'implication des usagers dans les projets retenus pour la labellisation est une condition indispensable. La participation des usagers ou leurs représentants varie de l'information, à la co-décision en passant par la concertation et la co-construction.

Les résultats du label et du concours 2015 peuvent être consultés à titre indicatif pour illustrer la nature des projets attendus dans ce cadre.

Des critères de sélection sont proposés infra : ils pourront être adaptés à des spécificités locales.

III | Les modalités de labellisation des projets et leur sélection au concours

L'information sur le dispositif de labellisation

Les modalités de lancement du label au niveau régional – appels à projets, actions médiatiques, etc – sont laissées à l'appréciation de chaque ARS et DRJSCS, sachant que l'ensemble des informations sera disponible prochainement sur l'espace internet « Droits des usagers du système de santé » du ministère chargé de la santé :

www.espace-droits-usagers.sante.gouv.fr

L'analyse et la sélection des projets

Comme en 2015, il est proposé de confier l'attribution du label « Droits des usagers de la santé » aux ARS, après avis des CSDU des CRSA et en lien, le cas échéant, avec les DRJSCS. Les critères de sélection pourront être mis en cohérence avec les priorités des plans stratégiques régionaux de santé en matière de droits des usagers.

Pour être recevables, les initiatives présentées satisferont aux caractéristiques suivantes :

- être modélisables et/ou transposables à l'ensemble du champ d'activité décrit supra ;
- associer les usagers ou leurs représentants, que ceux-ci soient à l'origine du projet ou qu'ils y participent. L'implication de ces derniers s'apprécie de l'information à la co-décision en passant par la concertation et la co-construction ;
- s'inscrire dans la durée ;

- favoriser l'appropriation des droits par tous, y compris par les populations dont la situation rend difficile l'accès à leurs droits ;
- se traduire par des supports informationnels et pédagogiques.

Lire à titre indicatif la grille d'analyse des projets labellisés au concours figurant en annexe I

Le calendrier

Le recueil des candidatures à la labellisation débutera à la réception de l'instruction ministérielle.

Les ARS proposeront les meilleurs projets labellisés admis à concourir au niveau national jusqu'au **10 février 2017** dans la limite de 2 par région. Les projets sélectionnés par les ARS seront accompagnés d'un avis motivé.

Le jury du concours national se réunira le **9 mars 2017** : les résultats seront annoncés au niveau national le **18 avril 2017**.

La valorisation des projets labellisés au niveau national

Les projets labellisés feront l'objet d'une valorisation, notamment par la mise en ligne d'informations au sein de l'espace « Droits des usagers de la santé » du ministère chargé de la santé : cela, au moyen du formulaire ad hoc à renseigner en ligne. L'objectif est de porter à la connaissance du plus grand nombre les projets labellisés ainsi que les initiatives des lauréats du concours afin d'en favoriser la reproductibilité.

Un suivi et une mise à jour seront assurés par les ARS pour les projets labellisés au niveau régional et par le bureau des « Usagers de l'offre de soins » de la direction générale de l'offre de soins (DGOS) pour les lauréats du concours national.

Lire à titre indicatif la grille de suivi des projets labellisés au concours, en annexe II.

Une cérémonie nationale de remise de prix viendra clore la campagne 2016-2017 pour récompenser les initiatives sélectionnées par le jury du concours.

IV | La protection des données à caractère personnel et la publicité des projets primés

Les porteurs des projets labellisés dans le cadre de ce dispositif autorisent le ministère chargé de la santé à divulguer leurs identités. Ils l'autorisent également à diffuser gracieusement, sur le site internet du ministère, le mode opératoire de leurs initiatives, y compris s'il s'agit d'un support vidéo.

Annexe I – Grille d'évaluation des projets labellisés admis à concourir

Nom du participant : **Catégories :** – les associations et les fondations exerçant leur activité dans le domaine de la santé et le secteur médico-social comme les associations d'usagers ou les associations et organisations professionnelles ; – les établissements de santé, sociaux et médico-sociaux ; – les professionnels de santé exerçant une activité libérale en ville, que ce soit à titre individuel ou dans le cadre d'un regroupement (réseaux de santé, structures de proximité, maison ou centre de santé, etc.) ou de service d'intérêt général dédiés à la prévention (services de PMI, santé scolaire et universitaire, santé au travail) ou encore dans un service de soins à domicile ; – les institutions et les organismes susceptibles de conduire des actions de promotion des droits : ARS, agences sanitaires, collectivités territoriales, caisses d'assurance maladie, mutuelles, organismes de recherche, etc. **Thématiques :** – renforcer et préserver l'accès à la santé – y compris à la prévention – pour tous, notamment par **une information adaptée** aux personnes vulnérables (mineures, majeures protégées, en perte d'autonomie, souffrant de troubles psychiques, intellectuellement déficient, étrangères, placées sous main de justice, etc.) ; – sensibiliser les professionnels de santé au moyen **d'actions de formation** aux droits des usagers ; – favoriser la **médiation en santé** dans les structures de soins, médico-sociales et à domicile en mobilisant, entre autres, les médiateurs tels que les médiateurs médicaux, les médiateurs non-médicaux, les personnes qualifiées, etc. ; – faire converger les droits des usagers des structures de soins, sociales et médico-sociales, notamment au travers de **la participation des représentants des usagers et des usagers** (CDU, CVS) et de la mise en place de dispositifs expérimentaux adaptés aux parcours (organisation territoriale pour l'exercice des droits etc.) ; – renforcer **l'effectivité** des droits des usagers par le traitement des réclamations et des plaintes, l'analyse systématique des motifs notamment à partir des rapports des CDU ou des CVS et la mise en œuvre de mesures d'amélioration ; – accompagner **les évolutions du système de santé** dans le respect des droits des usagers (e-santé, télémédecine, maisons et centres de santé, soins de santé transfrontaliers, chirurgie ambulatoire, etc.).	

..... 460

Critères d'éligibilité		
Capacité du projet à être modélisable et/ou transposable à l'ensemble du périmètre de l'offre sanitaire ou médico-sociale		… / 5
Capacité du projet à s'inscrire dans la durée		… / 5
Capacité du projet à favoriser l'appropriation des droits par tous, y compris par les populations dont la situation rend difficile l'accès à leurs droits		… / 2.5
Implication des usagers ou de leurs représentants (information, concertation, co-construction, co-décision).		… / 2.5
Originalité du projet/caractère innovant		… / 2.5
Appréciation générale (sur les supports informationnels, pédagogiques, les réalisations concrètes et mesurables)		… / 2.5
Total note		**… / 20**
Points forts	**Points faibles**	

Intitulé du projet :

Nom du rapporteur :

Appréciation générale sur le projet

Propositions du rapporteur

Annexe II – Grille de suivi des projets labellisés ou lauréats au concours

Année d'obtention du label (prix) :

Intitulé de votre projet :

Bref rappel des objectifs :

Catégorie dans laquelle votre projet concourt :

- **Droits collectifs : oui / non | Droits individuels : oui / non**

- **Thématique (cocher la case correspondante) :**

renforcer et préserver l'accès à la santé – y compris à la prévention – pour tous, notamment par **une information adaptée** aux personnes vulnérables (mineures, majeures protégées, en perte d'autonomie, souffrant de troubles psychiques, intellectuellement déficientes, etc), étrangères, placées sous main de justice, etc. ;

sensibiliser les professionnels de santé au moyen **d'actions de formation** aux droits des usagers ;

favoriser **la médiation en santé** dans les structures de soins, médico-sociales et à domicile en mobilisant, entre autre, les médiateurs tels que les médiateurs médicaux, les médiateurs non-médicaux, les personnes qualifiées, etc. ;

faire converger les droits des usagers des structures de soins, sociales et médico-sociales, notamment au travers de **la participation des représentants des usagers et des usagers** (CDU, CVS) et de la mise en place de dispositifs expérimentaux adaptés aux parcours (organisation territoriale pour l'exercice des droits) ;

renforcer **l'effectivité** des droits des usagers par le traitement des réclamations et des plaintes, l'analyse systématique des motifs notamment à partir des rapports des CDU ou des CVS et la mise en œuvre de mesures d'amélioration ;

accompagner **les évolutions du système de santé** dans le respect des droits des usagers (e-santé, télémédecine, maisons et centres de santé, soins de santé transfrontaliers, chirurgie ambulatoire, etc.).

Autre (précisez) :

- **Catégorie (cocher la case correspondante) :**

association, fondation des domaines de la santé et médico-social ;

établissement de santé ou établissement médico-social ;

professionnel de santé exerçant une activité libérale à titre individuel ou regroupé, dans un service d'intérêt général dédié à la prévention, dans un service de soins à domicile ;

institution ou organisme susceptible de conduire des actions de promotion des droits : ARS, agence sanitaire, collectivité territoriale, caisse d'assurance maladie, mutuelle, organisme de recherche, etc.

Capacité de modélisation et/ou de transposition à l'ensemble du périmètre de l'offre sanitaire ou médico-sociale de votre projet	*Le projet a-t-il donné lieu à transposition dans une autre structure ?* *Avez-vous été contacté pour avoir des informations sur votre projet ?* *Si oui, quelles suites ont été données ?*
Capacité du projet à s'inscrire dans la durée	*Le projet se poursuit-il ? si oui, va-t-il évoluer ?* *Si non, pour quelle raison n'est-il pas poursuivi ?*
Capacité du projet à favoriser l'appropriation des droits par tous, y compris par les populations dont la situation rend difficile l'accès à leurs droits	*Avez-vous pu mesurer une meilleure appropriation des droits ?* *Si oui, comment et auprès de quel public ?*
Implication des usagers ou de leurs représentants (information, concertation, co-construction, co-décision).	*Les usagers sont-ils toujours partie prenante de votre projet ? si oui, dans quelle mesure ?* *Si non, pour quelle raison ?*
Originalité du projet/caractère innovant	*Votre projet vous semble-t-il encore original/ innovant ? si oui, dans quelle mesure, si non, pour quelle raison ?* *Imaginez-vous adapter votre projet pour qu'il soit à nouveau original/innovant ?*
Appréciation générale (sur les supports informationnels, pédagogiques, les réalisations concrètes et mesurables)	*Vos supports sont-ils toujours adaptés, pensez-vous les faires évoluer, si oui, comment ?* *si non, pourquoi ?*
L'attribution du label (prix) droits des usagers de la santé a-t-il été une aide dans le déploiement de votre projet ?	*Dans quelles circonstances avez-vous eu besoin de vous prévaloir de l'attribution du label ou du prix pour mener à bien votre projet ? quels ont été les effets positifs ou négatifs de l'attribution du label (prix) droits des usagers de la santé ?*
Points forts	**Points faibles**
Quels sont les points forts que vous retenez de votre expérience ? constatez-vous des points forts que vous n'aviez pas envisagés initialement ? si oui, lesquels ?	*Quelles sont les difficultés que vous avez rencontrées ? comment les avez-vous surmontées ?*

11

..... 463
Annexe III : Documents de communication de la CCIM..... 464

Commission Confidentialité de l'Information Médicale

Etre acteur de sa santé

La confidentialité, c'est aussi notre métier !

La CCIM, c'est quoi ?

C'est une **commission** crée en 2011, composée de **représentants de divers services ou instances** du CHRU de Lille (COSI, DIM, DRN, SIAM, CME, DAJ, SCQSS, CSIRMT, CGS), du correspondant Informatique et Liberté, et pilotée par le Dr Theis (médecin responsable de l'information médicale et chef de service du DIM).

Quelles sont ses missions ?

Elle a **deux missions principales** :

- analyser les questions portant sur la confidentialité des données médicales
- définir puis mettre en place les procédures nécessaires pour en garantir le respect.

Semaine sécurité patient
Commission Confidentialité de l'Information Médicale
CCIM@chru-lille.fr

..... 464
Annexe IV : Questionnaire d'évaluation des pratiques professionnelles de la CCIM ... 470
..... 470

B) Accès au dossier médical informatisé du patient :

8) Par votre fonction, êtes-vous amenés à consulter des dossiers médicaux informatisés de patients ? **OUI / NON** *(si NON, renvoi à la question 13)*

9) Dans quelle(s) circonstance(s) vous arrive-t-il d'aller voir des dossiers médicaux informatisés de patients que vous n'avez pas pris en charge ?
   - O Pour aller consulter votre dossier personnel
   - O Pour consulter le dossier d'un membre de votre famille pris en charge au CHRUL
   - O Pour un proche qui vous a demandé des renseignements sur quelqu'un de sa famille pris en charge au CHRUL
   - O Par curiosité
   - O Pour se renseigner sur un personnel du CHRUL
   - O Pour inclure des patients dans une recherche
   - O Pour répondre à un avis médical
   - O Pour l'activité de tarification
   - O Pour la maintenance d'un logiciel
   - O Pour anticiper une prise en charge d'un patient dans le service
   - O Je ne le fais jamais
   - O Autre, précisez : *Question ouverte*

10) Selon vous, est-il permis de consulter le dossier médical informatisé d'un patient que vous n'avez pas pris en charge ? **OUI / NON**

11) Si vous utilisez Sillage, utilisez-vous « la demande d'accès étendu » dans Sillage ? *(si « jamais » ou « je n'utilise pas sillage » ou « non concerné », renvoi à la question 13)*
   - O Non concerné car mon profil me donne accès à toutes UF
   - O Jamais
   - O Au moins une fois par jour
   - O Au moins une fois par mois
   - O Au moins une fois par trimestre
   - O Au moins une fois par an
   - O Je ne sais pas ce qu'est l'accès étendu dans Sillage
   - O Je n'utilise pas Sillage

12) Dans quel cas utilisez-vous l'accès étendu dans Sillage ? *Question ouverte*

C) Connaissance des règlementations sur la confidentialité :

13) Lors de votre arrivée au CHRU de Lille, avez-vous eu des informations sur le comportement à adopter concernant le secret professionnel? **OUI / NON**

14) Avez-vous déjà vu ou lu des documents du CHRU de Lille sur le comportement à adopter par rapport au secret professionnel? **OUI / NON** *(si NON, renvoi à la question 16)*

15) Si OUI, lesquels ? *Réponse ouverte*

16) Saviez-vous que, dès que vous allez consulter un dossier patient informatisé, votre connexion est tracée et qu'il est possible de savoir quand, à quelle heure, et quelle(s) action(s) vous avez effectuée(s)? **OUI / NON**

17) Vous faites-vous soigner au CHRU de Lille ? **OUI / NON**

Contact : Joséphine Beharel, élève juriste
Josephine.BEHAREL@CHRU-LILLE.FR

18) Avez-vous déjà pensé à vous faire soigner dans un autre établissement parce que vos collègues pourraient consulter votre dossier médical informatisé ? **OUI / NON**

19) Selon vous, en cas de non-respect du secret professionnel, quel est le montant maximum de l'amende encourue ? *Liste déroulante* *(jusqu'à 1 000€, jusqu'à 5 000€, jusqu'à 10 000€, jusqu'à 15 000€)*

20) Selon vous, en cas de non-respect du secret professionnel, quelle est la durée maximale de la peine d'emprisonnement encourue ? *Liste déroulante* (aucune, jusqu'à 1 mois, jusqu'à 4 mois, jusqu'à 8 mois, jusqu'à 12 mois, jusqu'à 18 mois)

D) Communication des données médicales patients :

21) Emportez-vous des fichiers de données médicales informatisées de patients et/ou des dossiers médicaux papier à l'extérieur de l'établissement ? **OUI / NON / NON CONCERNE** *(non concerné : car pas d'accès aux données patients) (non et non concerné, renvoi à la question 23)*

22) Si OUI, pourquoi ? : *Question ouverte*

23) Avez-vous déjà communiqué des données médicales non cryptées de patients :
- O par mail
- O par les réseaux sociaux
- O par le partage collectif (ex : dropbox)
- O je n'ai jamais communiqué de données médicales de patients

24) Avez-vous déjà lu ou vu des affiches CNIL du CHRU de Lille ? **OUI / NON**

25) Est-ce que ces affiches se trouvent dans votre service ? **OUI / NON**

E) Questions générales :

Age : *Liste déroulante* ans

Depuis combien d'années travaillez-vous au CHRU de Lille ? *Liste déroulante* années

Personnel soignant/ Personnel non soignant ? *Liste déroulante*

Pôle/ Service/ Métier ? *Liste déroulante*

Question facultative : Dans le cadre d'une campagne de communication sur la confidentialité, quel serait le meilleur moyen pour vous, de communiquer des informations afin que celles-ci soient connues et comprises par tout le personnel du CHRU ?

Question ouverte

Contact : Joséphine Beharel, élève juriste
Josephine.BEHAREL@CHRU-LILLE.FR
V8 12/06

MERCI DE VOTRE PARTICIPATION

« Parce que les professionnels du CHRU de Lille sont aussi des patients comme les autres… ».

En tant que personnel du CHRU de Lille, vous avez des droits mais aussi des devoirs.

Vos droits :

- Seul le personnel hospitalier vous prenant en charge au CHRU de Lille peut avoir accès à votre dossier médical informatisé ; excepté les cas de dérogation, expressément prévus par la loi (article L1110-4 Code de la Santé Publique)
- Si vous avez des doutes sur une personne qui aurait pu consulter votre dossier médical informatisé, vous pouvez faire part de votre crainte à votre cadre Supérieur de Santé ou directement à la Délégation des Affaires Juridiques (DAJ).

Vos devoirs :

- Il est strictement interdit de consulter le dossier médical informatisé d'un patient que vous n'avez pas pris en charge.

Pour information :

- Lorsque vous vous connectez à un dossier patient informatisé, cette connexion est tracée et identifiable.
- En cas de connexion irrégulière, cette trace peut constituer un commencement de preuve en cas de plainte.
- En cas de consultation irrégulière d'un dossier patient informatisé vous encourez une peine d'un an d'emprisonnement et une amende de 15 000 euros.
- http://intrachru/intranet-gapi/SSI/

Pour toutes questions supplémentaires, vous pouvez contacter la CCIM par mail CCIM@CHRU-LILLE.FR

La Commission Confidentialité de l'Information Médicale (CCIM) est une commission qui a été mise en place en 2011 dans le but d'analyser les questions portant sur la confidentialité des données médicales, puis de définir et de mettre en place les procédures pour en garantir le respect. Cette commission est pilotée par le Dr Theis, médecin responsable de l'information médicale. Elle est composée de représentants du SIAM (Secteur d'Information et des Archives Médicales), de la CME (Commission Médicale d'Etablissement), de la sous-commission qualité de la coordination générale des soins, du DRN (Département des Ressources Numériques), de la DAJ (Délégation des Affaires Juridiques), du COSI (Comité Opérationnel du Système d'Information), du DIM (Département de l'Information Médicale), ainsi que le CIL (Correspondant Informatique et Libertés) du CHRU.

Contact : Joséphine Beharel, élève juriste
Josephine.BEHAREL@CHRU-LILLE.FR
V8 12/06

Page **4** sur **4**

..... 473

Bibliographie 475

I. Ouvrages, manuels et thèses 476

A. Ouvrages et manuels généraux 476
B. Ouvrages spéciaux 476
C. Contribution à un ouvrage 477
D. Thèses 477
II. Rapports et études 479
III. Articles 484
IV. Avis et délibérations 497
V. Décisions commentées 498
Index alphabétique 501
Table des matières 505

L'utilisation des technologies de l'information et de la communication à l'hôpital.

L'utilisation des TIC à l'hôpital prend une place de plus en plus importante et son développement ne cesse de croître. Le cadre juridique applicable se révèle cependant complexe à appréhender, composé à la fois de textes de droit commun et de textes plus spécifiques, le tout formant un ensemble pas toujours cohérent. Pour accompagner au mieux l'utilisation des TIC à l'hôpital, le législateur doit trouver le juste équilibre entre cadre propice pour le développement de ces pratiques, protection des droits fondamentaux et sécurisation des pratiques. Or, à l'heure actuelle, le cadre juridique applicable à l'utilisation des TIC à l'hôpital ne permet pas d'assurer cet équilibre délicat. Les pouvoirs publics ont donc un rôle stratégique à jouer dans la sécurisation de l'utilisation des TIC à l'hôpital. Une impulsion nationale doit être donnée en la matière, afin d'assurer la cohérence des projets développés, au travers d'une gouvernance forte. Le cadre juridique doit, quant à lui, être rénové afin d'accompagner l'innovation dans le numérique en santé et assurer la sécurité juridique nécessaire à la bonne utilisation des TIC. Dans ce contexte, les hôpitaux ont un rôle essentiel à jouer afin de sécuriser leurs pratiques.

Mots clefs français : TIC – hôpital - télémédecine – dossier médical électronique - données de santé – données personnelles - e-santé

The use of information and communication technologies in hospitals

The use of ICT has become increasingly important in hospitals. However, the legal framework structuring its use is very complex to grasp. Indeed, it is made up of general laws as well as specific ones and makes this framework sometimes unconsistent. To provide an optimal legal framework for the ICT to expand safely, the legislator needs to strike the right balance between protecting fundamental rights and securing practices. As the current legal framework does not provide this delicate balance, public authorities have a strategic role to play to ensure a secure use of ICT within hospitals. To guarantee the development of consistent projects, a strong governance has to set up a national leadership. The legal framework needs to be rehabilitated to support digital innovation in Healthcare and to ensure a legal protection required for an appropriate use of ICT. Hospitals have then a key role to play in securing their practices.

Keywords : ICT – hospitals – telemedecine – electronic medical record – health data – personal data - eHealth

Unité de recherche/Research unit : Centre Droits et perspectives du droit – CRDP - EA n°4487, http://crdp.univ-lille2.fr/

Ecole doctorale/Doctoral school : Ecole doctorale des sciences juridiques, politiques et de gestion, n° 74, 1 place Déliot, 59000 Lille, ecodoc.univ-lille2.fr, http://edoctorale74.univ-lille2.fr/

Université/University : Université Lille 2, Droit et Santé, 42 rue Paul Duez, 59000 Lille, http://www.univ-lille2.fr/