PRES Université Lille Nord de France

Thèse délivrée par

L'Université Lille 2 – Droit et Santé

N° attribué par la bibliothèque

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

THÈSE

Pour obtenir le grade de Docteur en Droit

Présentée et soutenue publiquement par

ETIEN-GNOAN N'Da Brigitte

Le 18 Décembre 2014

L'encadrement juridique de la gestion électronique des données médicales

JURY

Directeur de thèse: M. le Professeur LAVENUE Jean-Jacques, Université Lille 2

Membres du jury: Mme. la Professeure ANDREU MARTINEZ Belen, Université de Murcie, Espagne (Rapporteur)

M. GILLES William, Maître de conférences, Université Paris 1

M. le Professeur HARDY Jacques, Université Lille 2

M. le Professeur TRUDEL Pierre, Université Montréal, Canada (Rapporteur)

REMERCIEMENTS

Aboutir à la soutenance de cette thèse n'a été possible qu'avec le soutien des parents, amis et encadreurs.

La disponibilité, les conseils et le soutien de mon Directeur de thèse, Monsieur le Professeur LAVENUE Jean-Jacques, ont été des plus précieux pour la réalisation de cette œuvre. Je lui suis infiniment reconnaissante et lui souhaite une santé de fer et tout le bonheur possible.

Ma reconnaissance va, aussi à l'endroit des membres du jury qui ont bien voulu accorder de leur temps, si chargé, à l'appréciation de mon travail.

Je voudrais également remercier l'école doctorale pour l'encadrement et particulièrement mesdames RANCHY-DESRUMEAUX et MENU pour leur disponibilité et leur aide.

A mes parents Joséphine et Philippe, à mon époux, Ambroise et mes filles Eliora et Kerène, je réitère mon affection et ma gratitude. Toutes leurs attentions, tous leurs conseils et leur compréhension m'ont été d'un très grand soutien.

Je remercie ma famille et mes amis de Côte d'Ivoire, de France et du Québec pour leurs encouragements, leur compréhension et leur aide.

Je rends grâce à Dieu pour tous les bienfaits reçus, notamment, pour l'accomplissement de ce projet professionnel et personnel si cher à mon cœur.

SOMMAIRE

Sommaire

TABLE DES SIGLES ET ABREVIATIONS

I. SIGLES ET ACRONYMES

AAPC: Avis d'appel public à la concurrence

ACPM: Association canadienne pour la protection médicale

ACS : Aide à l'acquisition d'une complémentaire santé

ADICAP : Association pour le Développement de l'Informatique en Cytologie et en Anatomie Pathologiques

AFCDP : Association française des correspondants à la protection des données à caractère personne

AFHADS : Association française des hébergeurs agréés de données de santé

AFNOR : Association française de normalisation

AFSSAPS : Agence française de sécurité sanitaire des produits de santé

AFUL : Association francophone pour l'utilisation des logiciels libres

AGIRA : Association pour la gestion des informations sur les risques en assurance

ALD : Affection longue durée.

AMC : Association médicale canadienne

AMC : Assurance maladie complémentaire

AMM : Association médicale mondiale

AN : Assemblée nationale

ANAES : Agence nationale d'accréditation et d'évaluation en santé

ANAP : Agence nationale d'appui à la performance des établissements de santé et médico-sociaux

ANR : Agence nationale de la recherche

ANSI: American national standards Institute

ANSM : Agence nationale de sécurité du médicament et des produits de santé

AP-HP, Assistance Publique hôpitaux de Paris

ARH : Agence régionale d'hospitalisation

ARS : Agence régionale de santé

ASHQ : Agents des services hospitaliers qualifiés

ASIP SANTÉ : Agence des systèmes d'information partagée de santé

ATIH : Agence technique de l'information sur l'hospitalisation

BCR: Binding corporate rules

BPCO: Broncho- pneumopathie chronique obstruante

BSI : British Standard Institute

CADA : Commission d'accès aux documents administratifs

CALLIOPE: Call for InterOperability in Europe

CATEL : Club des acteurs de la télésanté

CCNE : Comité consultatif national d'éthique

CCPPRB : Comités consultatifs de protection des personnes dans la recherche biomédicale

CCTIRS : Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé.

CE : Conseil de l'Europe

CEE : Communauté économique européenne

CEN : Comité européen de normalisation

CENELEC : Comité européen de normalisation en électronique et en électrotechnique.

CEPD : Contrôleur européen de la protection des données

CGIET : Conseil général de l'industrie, de l'énergie et des technologies

CGTI : Conseil général des technologies de l'information

CHRU : Centre hospitalier universitaire

CIL : Correspondant informatique et libertés

CIS : Code identifiant des spécialités

CISI : Comité interministériel pour la société de l'information

CI-SIS : Cadre d'Interopérabilité des Systèmes d'Information de Santé

CMU : Couverture maladie universelle

CNAMTS : Caisse nationale de l'assurance maladie des travailleurs salariés

CNAVTS : Caisse nationale d'assurance vieillesse pour les travailleurs salariés

CNDA : Centre national de dépôt et d'agrément

CNIL : Commission nationale informatique et libertés

CNISAS : Commission de normalisation de l'informatique de santé et de l'action sociale.

CNOM : Conseil national de l'Ordre des médecins

CNOP : Conseil national de l'Ordre des pharmaciens

CNRS : Centre national de recherche scientifique

CNSA : Caisse nationale de solidarité pour l'autonomie

CNUCID : Commission des nations unies pour le droit commercial international

CPE : carte professionnelle d'établissement

CPME : Comité permanant des médecins européens

CPP : Comités de protection des personnes

CPS : Carte de professionnel de santé

CRO : Contract Research Organisation

CURAPP : Centre universitaire de recherches administratives et politiques de Picardie

DADVSI : Droits d'auteurs et droits voisins dans la société de l'information

DCC : Dossier communicant de cancérologie

DDASS : Direction départementale des affaires sanitaires et sociales

DG Info : Direction générale société de l'information et médias

DGCIS : Direction générale de la compétitivité de l'industrie et des services

DGME : Direction générale de la modernisation de l'État

DGOS : Direction générale de l'offre de soins

DHOS : Direction de l'hospitalisation et de l'organisation de soins

DIN : Deutsches Institut für Normung

DME : Dossier médical électronique

DMP : Dossier médical personnel

DMSP : Dossier médico-social partagé

DNDR : Dotation nationale de développement des réseaux

DP : Dossier pharmaceutique

DSE : Dossier santé électronique

DSQ : Dossier santé du Québec

DSSIS : Délégation à la stratégie des systèmes d'information de santé

EDESS : Échange de données dans l'espace sanitaire et sociale

EDISANTE : Échange de données informatisées dans le secteur de la santé

EDVIGE : Exploitation documentaire et valorisation de l'information générale

EPSOS: Smart Open Service for European Patients

ETSI : Institut européen des normes de télécommunication.

FAQSV : Fonds d'aide à la qualité des soins de ville

FCC : Fichier central des chèques

FIEEC : Fédération industrielle représentant les entreprises des industries électriques, électroniques et de communication

FNI : Fédération Nationale des Infirmiers

G 29 : Groupe de travail de l'article 29

GAMIN : Gestion automatisée de la médecine infantile

GHS groupes homogènes de séjours

GIE : Groupement d'intérêt économique

GIP : Groupement d'intérêt public

GIP SPSI : Groupement d'intérêt public santé-protection social international

GMSIH : Groupement pour la modernisation du système d'information hospitalier

HADOPI : Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet

HAS : Haute autorité de santé

HL7 : Health level seven

HPST : Hôpital patients santé et territoires

HR5 : Historique de remboursement version 5

HTML: Hypertext Markup Language

IAS ECC: Identification-authentification-signature european-citizen-card

ICCS: Institute of Communication and Computer Systems

IGAS : Inspection générale des affaires sociales

IGF : Inspection générale des finances

IHE : Integrating the healthcare entreprise

INCA : Institut national du cancer

INRIA : Institut National de Recherche en Informatique et en Automatique

INS : Identifiant national de santé

INSEE : Institut national de la statistique et des études économiques

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

IRM : Imagerie par résonance magnétique

ISO : Organisation internationale de normalisation

ITU : Unité internationale des télécommunications

JUDEX : Système judiciaire de documentation et d'exploitation

LESISS : Les Entreprises des Systèmes d'Information Sanitaires et Sociaux

LGC : Logiciel de gestion de cabinet

LGO : Logiciel de gestion d'officine

MAINH : Mission nationale d'appui à l'investissement hospitalier

MDM : Master data management

MEAH : Mission d'expertise et d'audit hospitalier

MOAR : Maîtrises d'ouvrage régionales

MSAP : Mise sous accord préalable de prescripteurs

NAS : Nomenclature des acteurs de santé

NIR : Numéro d'inscription au répertoire

NPO : National Patient Overview

NTIC : Nouvelles technologie de l'information et de la communication

OCDE : Organisation de coopération et de développement économique

OIT : Organisation internationale du travail

OMS : Organisation mondiale de la santé

ONU : Organisation des Nations unies

PAGSI : Programme d'action gouvernementale pour la société de l'information

PERNNS : Pôle d’expertise et de référence nationale de nomenclatures de santé.

PGSSI-S : Politique générale de sécurité des systèmes d'information de santé

PHAST : Association de Pharmaciens Hospitaliers

PIAHDS : Procédure d'agrément des hébergeurs de données de santé

PIB : Produit intérieur brut

PIN : Personal identification number

PMSI : Projet de médicalisation des systèmes d'information

PPS : Programme personnalisé de soins

PRISM : Programme américain de surveillance électronique

PSAD : Prestataires de services de santé à domicile

RAMQ : Régie de l’assurance maladie du Québec

RASS : Référentiel des acteurs santé sociaux

RCP : Réunion de concertation pluridisciplinaires

RNIPP : Répertoire national identification des personnes physiques

RNR : Répertoire national des référentiels

ROR : Répertoire opérationnel des ressources

RPPS : Répertoire partagé des professionnels de santé.

RSA : Résumés de sortie anonyme

RSS : Résumé de sortie standardisée

RSSI : Responsable de la sécurité des systèmes d'information

RUM : Résumé d'unité médicale

SAFARI : Système automatisé des fichiers administratifs et des répertoires des individus

SAMU : Service d'aide médicale urgente

SDB : Syndicat des Biologistes

SESAM-VITALE : Système électronique de saisie de l'assurance-maladie associée à la carte vitale

SFIL : Société Française d'Informatique de Laboratoire

SIH : Système d'information hospitalière

SIL : Système d'information pour laboratoire

SIS : Système d'information de santé

SISA : Société interprofessionnelle de soins ambulatoires

SNOMED : Systemized nomenclature of medecine

STIC : Système de traitement des infractions constatées

SVR AB : Sjukvårdsrådginvningen, en abrégé, l'équivalent de l'ASIP santé en Suède

T2A : Tarification à l'activité

TAJ : Traitement des antécédents judiciaires

TIC : Technologie de l'information et de communication

URCAM : Unions régionales des caisses d'assurance-maladie

II. ABRÉVIATIONS DE RÉFÉRENCES EN MATIÈRE JURIDIQUE

ADSP : Actualité et dossier en santé publique

C. Comptes : Cour des Comptes

C.A : cour d'appel

Cass. civ. : Cour de cassation, chambre civile

Cass. Com. : Cour de cassation, chambre commerciale

Cass.crim.: Cour de cassation, chambre criminelle

CE : Conseil d'État

CEDH : Cour européenne des droits de l'homme

CGCT : Code Général des Collectivités Territoriales

CJCE : Cour de justice des communautés européennes

CJUE : Cour de justice de l'Union européenne

Cons. Const : Conseil Constitutionnel

Cons : Considérant

CSP : Code de la santé publique

CSS : Code de la sécurité sociale

DIT : Droit de l'informatique et des télécoms

DOG : Diario oficial de Galicia (journal officiel de Galice)

IFSA : Institut français des sciences administratives

JCP : Semaine juridique

JOAN : Journal officiel de l'Assemblée nationale

JOCE : Journal officiel des communautés européennes

JORF : Journal officiel de la république française

JOUE : Journal officiel de l'Union européenne

LGDJ : Librairie générale de droit et de jurisprudence

PUF : Presse universitaire de France

R.D.P.C : Revue de droit pénal et de criminologie

RDA : Revue de droit d'Assas

RLDI : Revue Lamy droit de l'immatériel

SFS : Svensk för fattningssamling (code suédois des lois)

T. confl. : Tribunal de conflits

TGI : Tribunal de grande instance

INTRODUCTION

Au cours des deux dernières décennies, la France s'est engagée dans une réforme de son système de santé fondée sur le concept de « la santé électronique » dans le double objectif d'améliorer la qualité des soins et de maîtriser les dépenses de santé. La santé électronique, intégration des technologies de l'information et de la communication dans le domaine de la santé, implique une informatisation généralisée du système de santé (A).

L'informatisation du système de santé implique une gestion électronique accrue de données médicales qui nécessite un encadrement juridique strict.

Au plan international, la régulation de la politique de santé des États est assurée par les instances comme l'OCDE[1], l'OMS[2] et la Commission européenne. Néanmoins, la France a mis en place un cadre institutionnel interne qui lui est propre. Les compétences en matière de politique de santé et de régulation du système de soins sont partagées entre l'État (Parlement, gouvernement et administrations ministérielles) ; les organismes d'assurance maladie obligatoire et les collectivités territoriales (les agences régionales de santé (ARS). Votant les principales lois qui guident le projet d'informatisation du système de santé, le Parlement est en amont de l'organisation. La mise en application de ce projet est assurée par le gouvernement à travers les règlements qu'il prend et les maîtres d'ouvrage qu'il nomme. Une autorité indépendante de régulation supervise toutes les actions en veillant à ce qu'elles respectent les normes de la loi informatique et libertés.

La nécessité de la prise de tant de mesures de contrôle réside dans la singularité qui caractérise la gestion électronique des données médicales. Que renferme l'expression « gestion électronique des données médicales » et quelle en est sa spécificité ? Une analyse préalable de ces notions s'imposera pour la clarté de la suite de cette étude (B).

A. L'informatisation du système de santé

L'informatisation du système de santé qui passe nécessairement par la gestion électronique de données médicales s'inscrit, en France, dans le cadre de l'évolution de l'administration électronique avec la collaboration de partenaires socio-économiques des secteurs public et privé sous le contrôle de la CNIL.

[1] Organisation de coopération et de développement économique.

[2] Organisation mondiale de la santé.

1. De l'administration électronique à la santé électronique

L'implication de l'État dans le système de santé français tel que nous le connaissons aujourd'hui date de la fin du XIXe siècle, lorsque, succédant à l'église et au pouvoir royal dans la gestion administrative des hôpitaux, l'État doit veiller à la protection de la santé publique. Il crée les premières institutions et met en place des législations dont la loi du 15 février 1902 définissant le premier cadre d'action pour les communes et les départements. Le ministère de la santé est créé en 1920 et le code de la santé publique est promulgué sous le régime de Vichy[3].

Les années 70 ont été marquées par l'essor des systèmes macro-informatiques dans les grandes organisations, notamment les administrations publiques en Europe et en Amérique du Nord. L'ordinateur était présenté comme un instrument de renforcement de l'efficacité des administrations publiques dans leurs relations avec les usagers dans le cadre de l'exercice de leurs fonctions de contrôle, dans les matières fiscales et policières. Cependant, de nombreux travaux relatifs au développement de l'informatique dans l'administration soulignent les risques que fait peser cette technique sur les libertés publiques. En France par exemple, les administrés manifestaient une crainte vis-à-vis de cet outil qui représentait pour eux l'instrument par lequel l'administration investirait progressivement la sphère privée. « *On parle d'une nouvelle sorcellerie qui va mettre l'homme à nu et l'exposera sans défense à la vue de tous*[4] », reprenait madame GALLOUEDEC-GENUYS, Françoise.

Cette psychose a été nourrie par un article de Philippe BOUCHER paru le 21 mars 1974 au journal le Monde. Intitulé Safari ou la chasse aux Français, cet article dénonçait le détournement de finalité de données personnelles des 52 millions de Français par le ministère de l'intérieur au moyen d'un ordinateur Iris-80. SAFARI ou système automatisé des fichiers administratifs et des répertoires des individus, avait été créé dans le but de mieux repérer les personnes en facilitant l'interconnexion des fichiers administratifs à partir de l'identifiant unique que constitue leur numéro de sécurité sociale. Des interventions comme l'avertissement adressé à l'Académie des sciences morales et politiques du Procureur général TOUFFAIT[5] dans son discours du 9 avril 1973 suscitaient déjà un climat d'inquiétude. Il

[3] Pour plus de détails sur l'historique du système de santé en France, lire *Le livre de présentation du système de santé en France*. Chapitre 1. Décembre 2013. www.gipspsi.org. Consulté le 20 février 2014.

[4] GALLOUEDEC-GENUYS, Françoise. *Le secret des fichiers*. p. 9. IFSA. CUJAS. 1976

[5] M. Adolphe TOUFFAIT fut Procureur général près la Cour de Cassation de 1968 à 1976.

l'exprimait en ces termes : « *la dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques*[6] ». En France, ce fut l'élément générateur[7] de la loi informatique et libertés de 1978. D'autres États ont suivi la France dans ce mouvement et plusieurs mesures législatives ont été adoptées par des pays occidentaux pour protéger les citoyens contre les abus dont ils pourraient être victimes de la part des administrations publiques exploitant systématiquement leurs données personnelles.

Les années 80 ont servi à rétablir la confiance entre les usagers et l'administration publique dont les mots d'ordre étaient : la transparence administrative, la simplification, la télématique administrative, les droits des usagers dans leurs relations avec les administrations, etc. Dans cette dynamique, l'État va amorcer un processus de modernisation visant à modifier les relations entre administrations et administrés et encadré par plusieurs lois. La transparence était ainsi assurée à travers les lois du 17 juillet 1978 sur la liberté d'accès aux documents administratifs[8] ; du 6 janvier 1978 sur l'informatique, les fichiers et les libertés[9] ; et celle du 3 janvier 1979 sur les archives[10].

Poursuivant ce processus, le gouvernement français a engagé, dès 1997, à travers le programme PAGSI [11], une promotion de l'usage des technologies de l'information et de la

---

[6] Extrait de l'article Safari ou la chasse aux Français de Philippe BOUCHER paru le 21 Mars 1974 au journal "Le Monde".

[7] Suite aux réactions des Français, le premier ministre interdit aux services de procéder sans son autorisation à de nouvelles interconnexions et demanda, par décret du 8 novembre 1974, au Garde des Sceaux de constituer une Commission chargée de « *proposer au gouvernement dans un délai de six mois, des mesures tendant à garantir que le développement de l'informatique dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques* ». La Commission rendit un rapport le 27 juin 1975 par le biais de Bernard TRICOT. Le projet de loi élaboré sur la base de ce rapport a abouti à l'adoption de la loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés. TRICOT, Bernard. *Rapport de la Commission informatique et libertés: (décret 74-938 du 8 novembre 1974).* Paris: La Documentation française, 1975. Volume 1. p. 7.

[8] Loi n° 78-553 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.

[9] Loi n° 78-17 du 6 janvier 1978 relatif à l'informatique, aux fichiers et aux libertés. JORF du 7 janvier 1978. p. 227.

[10] Loi n° 79-18 du 3 janvier 1979 sur les archives. JORF du 5 janvier 1979. p. 43.

[11] Annoncé par le premier ministre Lionel JOSPIN en août 1997, un premier projet : programme PAGSI (*programme d'action gouvernementale pour la société de l'information*) a été adopté par le premier Comité interministériel pour la société de l'information (CISI) le 16 janvier 1998. Il visait une généralisation des sites Internet publics et la mise en ligne des formulaires administratifs (espace public numérique). BRAUN, Gérard. *Rapport sur l'administration électronique au service du citoyen*. 6 juillet 2004. N° 402. www.senat.fr.

communication dans les services rendus par les administrations publiques. Désignée sous le vocable « e- administration ou e-gouvernement » ou encore « administration électronique », cette méthode a pour finalité première l'amélioration des services rendus au public.

En novembre 2001, le gouvernement a procédé à la généralisation des téléservices après la mise en ligne des documents administratifs et des textes publics. « *L'État se donne pour objectif que soient proposées en ligne, d'ici à 2005, l'ensemble des démarches administratives des particuliers, des associations et des entreprises, ainsi que les paiements fiscaux et sociaux. Il s'agit de faire progressivement en sorte que chaque usager bénéficie des technologies de l'information et de la communication dans les transactions avec les services publics et puisse notamment :*

- accéder simplement et rapidement à toutes les informations et à une aide personnalisée sur les services publics et ses démarches administratives. Un téléservice ne doit donc jamais être plus complexe à utiliser que son équivalent « papier » ;

- effectuer en ligne et de manière sûre toutes ses démarches avec les services publics sauf celles qui, par nature, exigent un déplacement. Cela inclut notamment les échanges eux-mêmes, mais également le suivi de ses dossiers, la définition de calendrier prévisionnel personnalisé, la relance par courrier électronique, etc. ;

- accéder à ses démarches passées et stocker en ligne, à son gré et en toute sécurité les résultats dématérialisés issus de ces dernières ;

- exercer en ligne son droit d'accès et, le cas échéant, de modifier des informations le concernant détenues ou échangées par les administrations, notamment aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[12]. »

Le 12 novembre 2002, le premier ministre Jean-Pierre RAFFARIN présentait un programme succédant au PAGSI, dénommé programme gouvernemental RE/SO 2007[13] (pour une république numérique dans la société de l'information). Celui-ci comprend trois volets dont une intervention directe de l'État en tant qu'acteur de la société de l'information ayant

[12] TRUCHE, Pierre. FAUGERE, Jean-Paul. FLICHY, Patrice. *Rapport sur la mise en place du site « mon.service-public.fr »*. Février 2002. p.13 - 14. www.ladocumentationfrançaise.fr. Consulté le 20 février 2014.

[13] Ce plan vise à construire et favoriser une République numérique, fidèle à la devise française "liberté, égalité et fraternité". Dans cet esprit, il doit permettre de "donner un nouvel élan à la société de l'information" en agissant pour un développement efficace de ses infrastructures (équipement, modalités d'accès à internet, cadre législatif, etc.) et de ses usages. Il s'agit également de simplifier les règles en vigueur sur internet, de restaurer la confiance des usagers, notamment et de clarifier les responsabilités des différents acteurs de la société de l'information. RAFFARIN, Jean-Pierre. *Discours du 12 novembre 2002 relatif au plan RE/SO 2007*. http://archives.internet.gouv.fr. Consulté le 20 février 2014.

vocation à l'exemplarité. Dans cette optique, l'État compte, entre autres, utiliser tous les apports des technologies de l'information et de la communication dans le domaine de la santé[14]. « *Ce développement s'orientera vers l'amélioration des pratiques médicales, de la prise en charge et du suivi des patients. Le gouvernement souhaite favoriser le haut débit pour les réseaux d'expertise et impulser le dossier médical partagé*[15].»

Depuis les années 80, l'informatique était déjà implantée dans les cabinets privés et les centres hospitaliers par la numérisation des données nominatives des usagers, à partir du projet de médicalisation des systèmes d'information (PMSI[16]). La modernisation passant notamment par l'informatisation des systèmes d'information de santé est une des options qu'a privilégiées le gouvernement français. Divers projets d'incitation à l'utilisation des TIC ont été menés par le gouvernement des années 80 à nos jours, qui influencent énormément le fonctionnement du système de santé français dans sa recherche de solutions pour une meilleure qualité de soins et la réduction des dépenses de santé[17].

La loi informatique et libertés du 6 janvier 1978 ayant jeté les bases en autorisant exceptionnellement les traitements automatisés des données de santé lorsque ceux-ci *« sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, de la gestion des services de santé et mis en œuvre par un membre*

---

[14] BRAUN, Gérard. *Rapport sur l'administration électronique au service du citoyen*. 6 juillet 2004. N° 402. www.senat.fr.

[15] RAFFARIN, Jean-Pierre. *Discours du 12 novembre 2002 relatif au plan RE/SO 2007*. http://archives.internet.gouv.fr. Consulté le 20 février 2014.

[16] Le programme de médicalisation des systèmes d'information est un dispositif faisant partie de la réforme du système de santé français ayant pour but la réduction des inégalités de ressources entre les établissements de santé (ordonnance du 24 avril 1996) sur la réforme de l'hospitalisation. Le programme débute en France en 1982 avec la circulaire n° 16 du 18 novembre 1982. Son objectif était de définir l'activité des établissements et de calculer l'allocation budgétaire qui en découlait. Il a été mis en place par Jean de KERVASDOUE, responsable de la direction des hôpitaux. En 1996, Alain JUPPÉ a confirmé ce projet par ordonnance n° 96-346 du 24 avril 1996 portant réforme de l'hospitalisation publique et privée.

[17] L'ensemble des études internationales (Union européenne, OCDE, l'OMS…) confirme que la France dispose de l'un des systèmes de santé les plus performants au monde. Avec le développement de l'assurance maladie, ce système est accessible à toute la population, grâce à la combinaison entre les régimes d'assurance maladie obligatoire, les régimes complémentaires et les dispositifs de solidarité comme la couverture maladie universelle (CMU) ou l'aide à l'acquisition d'une complémentaire santé (ACS). Ce système a en revanche un coût : la France consacre aux dépenses de santé environ 12 % de son PIB en 2012, ce qui la classe au second rang mondial derrière les États-Unis qui ont consacré près de 18 % de leur PIB à la santé en 2011. Selon la dernière étude de l'OCDE, portant sur l'année 2011 la moyenne des pays de l'OCDE se situe à 9,3 %. Par ailleurs, la dépense moyenne de santé par habitant (ajustée sur la base de la parité du pouvoir d'achat moyen des monnaies) se situe à 4118 $ en France, compte 3322 $ pour l'ensemble des pays de l'OCDE en 2011. GIP SPSI (groupement d'intérêt public santé-protection social international). *Le livre de présentation du système de santé en France*. Décembre 2013. p. 108. www.gipspsi.org. Consulté le 20 février 2014.

d'une profession de santé, ou par une personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévu par l'article 226-13 du code pénal » l'État a, par la suite, entrepris plusieurs réformes allant dans ce sens. Après l'informatisation des hôpitaux publics[18] et le traitement informatique des dossiers médicaux économiques et épidémiologiques de l'immunodéficience humaine dans les centres d'information et de soins de l'immunodéficience humaine et autres établissements hospitaliers[19] et le recueil et le traitement des données d'activité médicale[20], la réforme la plus marquante fut celle relative à la maîtrise médicalisée des dépenses de santé[21].

L'ordonnance du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de santé imposait, à compter du « *31 décembre 1998 au plus tard, aux professionnels, organismes ou établissements dispensant des actes ou des prestations remboursables par l'assurance maladie (...), d'émettre, de signer, de recevoir et de traiter des feuilles de soins électroniques ou documents assimilés conformes à la réglementation* ». C'est la base légale de Sesam-vitale dans l'ensemble des régimes d'assurance maladie. Conçu au début des années 80 comme outil devant permettre aux caisses primaires du régime général d'assurance maladie de faire face au flux croissant des demandes de remboursement pour les actes et prescriptions délivrés hors hospitalisation, le projet Sesam-vitale a vu ses objectifs confortés avec l'apparition d'une démarche « de maîtrise médicalisée des dépenses de santé ». La loi du 4 janvier 1993, en prescrivant le codage des actes, des prestations et des pathologies, a renforcé l'intérêt pour ce projet: seules, la saisie à la source par les professionnels de santé eux-mêmes et la

[18] Circulaire n° 275 du 6 janvier 1989 relative à l'informatisation des hôpitaux publics. NOR : SPSH8910005C (non paru au journal officiel).

[19] Arrêté du 27 novembre 1991 autorisant le traitement informatique des dossiers médicaux économiques et épidémiologiques de l'immunodéficience humaine dans les centres d'information et de soins de l'immunodéficience humaine et autres établissements hospitaliers. JORF du 17 janvier 1992 p. 822, référence à la loi 91-748 du 31 juillet 1991 portant réforme hospitalière (JORF n° 179 du 2 août 1991).

[20] Arrêté du 20 septembre 1994 relatif au recueil et au traitement de données d'activité médicale et de coût, visée 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 (tous les articles de cet arrêté ont été abrogés le 11 février 2004 par arrêté 2003-12-36, article 9). JORF n° 242 du 18 octobre 1994. p. 14761. NOR: SPSH9402990A.

[21] L'ordonnance du 24 avril 1996 (article 8.1) relative à la maîtrise médicalisée des dépense de santé. JORF n° 98 du 25 avril 1996. p. 6311. NOR: TASX9600042R.

transmission électronique des données au service des caisses habilités à les recevoir peuvent garantir la fiabilité, la sécurité et la confidentialité nécessaire[22].

En 2004, la loi n° 2004-810 du 13 août 2004[23] relative à l'assurance maladie, créait le dossier médical personnel « *afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie*[24] *»*. Prévu pour être opérationnel dès juillet 2007, le déploiement du dossier médical peinait à se réaliser. Le gouvernement a alors entrepris une relance du projet en même temps que la promotion de la télésanté à travers le plan hôpital (2007[25], puis 2012[26]). Cette nouvelle réforme a été traduite par la loi[27] portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires du 21 juillet 2009. Cette loi, dite loi Bachelot est « *un projet d'organisation sanitaire et non de financement. A terme, elle doit permettre de mettre en place une offre de soins graduée et de qualité, accessible à tous, satisfaisant à l'ensemble des besoins de santé*[28]». L'article 50 de ce texte a transposé les dispositions relatives au dossier médical

---

[22] COMITE CENTRAL D'ENQUETE SUR LE COÛT ET LE RENDEMENT DES SERVICES PUBLICS. *Conclusions sur Sesam-Vitale. Sesam-Vitale au-delà de l'informatique, un projet au service de la population*. p.1/8. www.ladocumentationfrançaise.fr. Consulté le 27 mai 2014.

[23] JORF n° 190 du 17 août 2004. p. 14598 texte n° 2.

[24] Article 3 de la loi du 13 août 2004.

[25] Le plan hôpital 2007, lancé en 2002 et concrétisé par l'ordonnance du 4 septembre 2003 portant simplification de l'organisation et du fonctionnement du système de santé ainsi que des procédures de création d'établissements ou de services sociaux ou médico-sociaux soumis à autorisation, est un programme constitué d'une série de mesures visant à moderniser l'offre de soins en réduisant l'augmentation des dépenses de santé. Ces mesures consistent en une nouvelle gouvernance hospitalière et une tarification à l'activité. Le 13 février 2007 le plan hôpital 2007 qui éprouvait des difficultés dans sa mise en œuvre a été remplacé par le plan hôpital 2012.

[26] « *Lancé dès le mois de juin 2007, le plan Hôpital 2012 s'inscrit dans la continuité du volet investissement du plan Hôpital 2007 et a pour objet de maintenir durant la période 2007-2012 un niveau d'investissement équivalent à celui de la période précédente et nécessaire à la réalisation des schémas régionaux d'organisation des soins de troisième génération, au développement des systèmes d'informations et à certaines mises aux normes de sécurité»*. Ministère de la santé. *Présentation des opérations retenues au titre du plan hôpital 2012*. Dossier de presse, 10 février 2010. p.1. http://www.sante.gouv.fr.

[27] Loi n° 2009-879 du 21 juillet 2009. JORF n° 0167 du 22 juillet 2009. P. 12184. Texte n° 1. NOR: SASX082264L.

[28] Agence régionale de santé Aquitaine. *« Hôpital, patients, santé, territoires » le droit à la croisée de nombreuses attentes*. Septembre 2009. www.ars.aquitaine.sante.fr.

« La loi acte le principe général de complémentarité et de coopération entre acteurs du système de santé. Elle propose, en 4 grands titres, une réorganisation globale du système de soins, en traitant prioritairement les questions de la lutte contre les déserts médicaux, du décloisonnement entre les soins ambulatoires, les soins hospitaliers et le secteur médico-social, de la performance des hôpitaux, de l'attractivité des métiers de la santé, de la santé des jeunes et d'une manière générale, de la coordination du système de santé. Tout cela étant rendue possible par la création des agences régionales de santé (ARS) ». Ministère du travail, de l'emploi et de la santé. Plaquette HPST *Une ambition nécessaire pour préserver le système de santé*. www.sante.gouv.fr.

personnel et au dossier pharmaceutique (articles L 161-36-1 à L. 161-36-4-3) dans le code de la sécurité sociale et l'article 78 a modifié le code de la santé publique en y insérant le concept de la « télémédecine » (article L 6316-1).
Le plan hôpital 2012, à la suite du plan 2007, devait permettre de passer d'une phase d'expérimentation à celle d'un développement généralisé de l'hôpital numérique. Le gouvernement entendait amener les établissements de santé à s'orienter vers plus de maturité informatique pour une amélioration significative de la qualité et de la sécurité des soins. Pour augmenter ses chances d'atteindre ses objectifs, il a lancé, en 2011, un autre plan appelé « programme hôpital numérique[29] » visant les mêmes objectifs, mais avec un pilotage plus percutant.

L'ensemble des projets qui jalonnent l'informatisation du système de santé est rigoureusement régulé par la Commission informatique et libertés (CNIL).

2. La régulation par la CNIL

La CNIL, Commission nationale de l'informatique et des libertés a été créée par la loi du 6 janvier 1978 dite loi informatique et libertés. Autorité administrative indépendante, elle est chargée de veiller à la protection des données personnelles. L'article 11 de la loi informatique et libertés précise que ses missions consistent à informer toutes les personnes concernées et tous les responsables du traitement de leurs droits et obligations et à veiller à ce que le traitement de données à caractère personnel soit mis en œuvre conformément aux dispositions de la loi. La CNIL joue aussi un rôle d'alerte et de conseil car elle a pour mission de veiller à ce que le développement de nouvelles technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

[29] Le programme hôpital numérique, lancé en novembre 2011 par la direction générale de l'offre de soins (DGOS) définit un plan de développement et de modernisation des systèmes d'information hospitalier et a pour but de fixer des priorités et des objectifs en 6 ans (2012-2017) en mobilisant tous les acteurs concernés et en accompagnant les établissements de santé dans la transformation par les technologies de l'information et de la communication. Une équipe projet pilotée par la DGOS et associant la délégation à la stratégie des systèmes d'information de santé (DSSIS), l'agence nationale d'appui à la performance des établissements de santé et médico-sociaux (ANAP) et l'agence des systèmes d'information partagée de santé (Asip santé) a élaboré et suit ce programme.
Le site internet du ministère des affaires sociales et de la santé dédié au programme hôpital numérique donne plus de détails sur la stratégie de ce programme. http//www.sante.gouv.fr/le-programme-hopital-numerique.html.

La CNIL dispose de pouvoirs de contrôle et de sanction. Elle autorise le traitement automatisé des données mentionnées à l'article 25 (notamment les données qui sont relatives à la santé), donne un avis sur les traitements mentionnés aux articles 26 (traitement relatif à la sécurité de l'État et infractions pénales) et 27 et reçoit les déclarations relatives aux autres traitements[30]. Les traitements de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention ainsi que ceux ayant pour fin la recherche dans le domaine de la santé sont donc soumis à l'autorisation de la CNIL[31]. Les décisions de la CNIL prononçant une sanction peuvent faire l'objet d'un recours de pleine juridiction devant le Conseil d'État[32].

Pour l'accomplissement de ses missions, la Commission dispose également d'un pouvoir réglementaire. Elle élabore des recommandations[33], des dispenses de déclaration[34], un règlement intérieur[35], des normes simplifiées[36], des autorisations uniques[37], des actes

[30] Article 11 de la loi informatique et libertés.

[31] Articles 54 et 64 de la loi informatique et libertés.

[32] Le pouvoir réglementaire des autorités administratives indépendantes est subordonné et second car il ne règle que des mesures de détail. Il revient au pouvoir réglementaire national de définir les éléments essentiels. Les sanctions prononcées par les autorités administratives indépendantes n'ont pas un caractère juridictionnel. Elles demeurent des décisions administratives soumises au respect des principes fondamentaux tels que la non rétroactivité des sanctions pénales et la nécessité ou la proportionnalité des peines. GELARD, Patrice. *Rapport sur les autorités administratives indépendantes : évaluation d'un objet juridique mal identifié (tome 1).* 15 juin 2006.www.senat.fr.

[33] Article 11, 4° de la loi informatique et libertés : «… *Pour l'accomplissement de ses missions, la Commission peut procéder par voie de recommandation.* »

[34] Article 24-II de la loi informatique et libertés modifiée : « *la Commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et les catégories de personnes concernées, sont dispensées de déclaration.* »

[35] Article 13-II de la loi informatique et libertés modifiée : « *la Commission établit un règlement intérieur. Ce règlement fixe les règles relatives à l'organisation et au fonctionnement de la Commission. Il précise notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la Commission.* »

[36] Article 24 de la loi informatique et libertés. Pour le fichier au traitement de données personnelles les plus courants, c'est-à-dire ceux qui ne portent pas atteinte à la vie privée et aux libertés, la CNIL peut adopter des décisions qui les encadrent.

[37] Certains fichiers ou des traitements de données personnelles sensibles ou à risque qui visent une même finalité et des catégories de données et de destinataires identiques, sont autorisés par la CNIL au travers des décisions cadres, appelées autorisations uniques. Par exemple, la CNIL a rendu, le 30 janvier 2014 une autorisation unique portant autorisation unique de traitement de données à caractère personnel mis en œuvre par les prestataires de santé à domicile pour la téléobservance en application de l'arrêté du 22 octobre 2013 relatif aux dispositifs médicaux à pression positive continue. *Autorisation unique n° AU-033 - Délibération n° 2014-046 du 30 janvier 2014*. www.cnil.fr.

réglementaires uniques[38] et des avis sur actes réglementaires uniques[39]. Certes, les recommandations de la CNIL n'ont pas force normative[40] mais elles contribuent considérablement à l'élaboration des règles en vigueur en la matière.

En matière de santé, la procédure d'autorisation préalable de la CNIL imposée aux responsables des traitements de données personnelles de santé constitue une garantie de protection pour les usagers. En effet, compte tenu de leur caractère sensible, la CNIL est plus rigoureuse sur l'adoption de mesures sécuritaires physiques et logiques qui sont prises par le responsable des traitements en fonction de l'utilisation qui est faite de l'ordinateur, de sa configuration, de l'existence d'une connexion à Internet. Par exemple, le seul déploiement du dossier médical personnel a fait l'objet de plusieurs délibérations[41] de la CNIL depuis 2006.
Le souci majeur de la Commission réside dans la recherche des garanties en matière de protection des personnes à l'égard de la gestion électronique des données médicales et de leur sécurité.

[38] Article 26 - IV de la loi informatique et libertés. La CNIL peut autoriser par acte réglementaire unique les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

[39] Article 26 - IV et 27 - III de la loi informatique et libertés modifiée. La CNIL donne un avis motivé par acte réglementaire unique pour des traitements de données à caractère personnel mis en œuvre pour le compte de l'État ou d'une personne morale de droit public ou de droit privé gérant un service public et qui portent notamment sur le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou sur des données biométriques.

[40] La Cour d'Appel de Paris l'a rappelé dans sa décision du 27 janvier 2005. « *Considérant que la recommandation de la CNIL du 1er juillet 2003 ne constitue pas une décision administrative normative ; que si par son caractère très complet, elle représente, à l'évidence, un guide particulièrement utile pour tout ceux qui envisagent de mettre en œuvre le vote électronique et doivent établir un cahier des charges pour fixer les relations contractuelles avec le prestataire de services chargés d'assurer la gestion technique des opérations électorales, aucune disposition légale ne permet de considérer que les règles contenues dans cette recommandation s'imposaient à l'ordre* ». Cour d' appel de Paris, 1ère chambre, section F. Arrêt du 27 janvier 2005. M. Y. L...c/Ordre des avocats. Gazette du palais n° 33 du 2 février 2005. p. 4-14.

[41] Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel. Délibération n° 2006-082 du 21 mars 2006 portant avis sur la demande d'agrément présentée par le GIE Santeos, candidat à l'hébergement du dossier médical personnel dans le cadre de son expérimentation. Délibération 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 n° 2006-080 du 21 mars 2006 portant avis sur la demande d'agrément présentée par la société France Telecom candidate à l'hébergement du dossier médical personnel dans le cadre de son expérimentation. A la même date, cinq autres avis ont été donnés sur le même sujet sur la base de la recherche des garanties présentées par les candidats pour la confidentialité et la sécurité des données.

B. Les notions

Une analyse sémantique des mots clés de cette étude est nécessaire pour la compréhension des textes qui nous serviront de fondement. La démarche consistera à définir d'une part l'expression « gestion électronique de données » et d'autre part, celle de « données médicales ».

1. La gestion électronique de données

La gestion électronique de documents, connue, généralement sous l'acronyme GED ou EMD pour "electronic document management" en anglais, désigne un procédé informatisé visant à organiser et gérer des informations et des documents électroniques au sein d'une organisation ou encore des logiciels permettant la gestion de ces contenus documentaires. Mais, pris dans ce sens, cette expression ne prend pas totalement en compte toutes les actions que recouvre la gestion électronique telle que nous voulons l'employer dans le cadre de cette étude.

Le substantif « gestion », synonyme du « maniement » selon le dictionnaire Robert, renvoie dans le langage informatique au contrôle du fonctionnement d'une entité notamment des informations ou des périphériques. Le maniement d'informations consiste dans leur collecte, leur manipulation, leur conservation et leur échange. L'adjectif « électronique » associé ramène à une gestion par support informatique. En effet, en l'absence de définition du terme « électronique » dans la législation européenne, celle donnée par la loi uniforme canadienne peut nous éclairer. « Électronique », qualifie ce qui est « *créé, transmis ou mis en mémoire sous forme numérique ou sous une autre forme intangible par des moyens électroniques, magnétiques ou optiques ou par d'autres moyens capables de créer, d'enregistrer, de transmettre ou de mettre en mémoire de façon similaire à ceux-ci*[42] ».
Ainsi présentée, l'expression « gestion électronique » se rapproche de ce que les législations européenne et française dénomment « traitement automatisé ». Et c'est dans ce sens que cette expression doit être comprise dans le contexte de cette analyse.

[42] Article 1 de la loi uniforme canadienne sur le commerce électronique. Août 1999. http://www.ulcc.ca/fr/us/index.cfm?sec=1&sub=lul. Consulté le 9 mars 2014.

Aux termes de l'article 2c de la convention du Conseil de l'Europe du 28 janvier 1981, un « *"traitement automatisé" s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement de données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, installation ou diffusion*. »

La proposition de règlement européen[43] adopté en mars 2014 ne définit pas le « traitement automatisé » de données mais le « traitement de données » en y incluant les procédés automatisés. On entend par « *traitement de données à caractère personnel » : toutes opérations ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que l'effacement ou la destruction* ». La proposition reprend, en cela, les termes de l'article 2b de la directive européenne 95/46/CE à laquelle elle doit succéder. Ces dispositions étendent le « traitement » à un champ plus vaste que celui délimité par la convention de 1981 même si les « *applications à ces données d'opérations logiques et/ou arithmétiques* » peuvent sous-entendre plusieurs types d'opérations non énumérées.

Quant à la loi informatique et libertés, telle que modifiée par la loi[44] du 6 août 2004, elle dispose en son article 2 : « *constitue un traitement de données à caractère personnel tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction»*. Alors que sa version initiale

[43] Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection de données). Article 4. (3). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 22 mai 2014.

[44] 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 relatif à l'informatique, aux fichiers et aux libertés. JORF n° 182 du 17 août 2004. p. 14 063. Texte n° 2. NOR: JUSX0100026L.

définissait le « traitement automatisé de données[45] », à la faveur de la transposition de la directive européenne 95/46/CE, la loi informatique et libertés, après la modification de 2004 précise seulement ce qu'est un « traitement de données ». Cette définition proposée par la loi informatique et libertés en vigueur, couvre un large choix de procédés utilisés pour le traitement ou la gestion des données. Le support du traitement peut donc être papier, électronique, optique ou autre. Dans le cadre de cette étude, la gestion est électronique ; le procédé utilisé entre donc dans le champ d'application de cette définition.

La gestion électronique des données crée un lien juridique entre le responsable de traitement, le destinataire et la personne concernée. Subsidiairement, le lien peut être quadripartite avec l'intervention d'un hébergeur. « Le responsable de traitement », « le destinataire » et « la personne concernée » sont définis par la législation européenne.

Le responsable du traitement est « *la personne physique ou morale, l'autorité publique, le service au tout autre organisme qui, seule ou conjointement avec d'autres, détermine les finalités, les conditions et les moyens de traitement de données à caractère personnel. Lorsque les finalités, les conditions et les moyens du traitement sont déterminés par le droit de l'Union, ou la législation d'un État membre, le responsable du traitement peut être désigné, ou les critères spécifiques applicables pour le désigner peuvent être fixés, par le droit de l'Union ou par la législation d'un État membre*[46] ». La loi informatique et libertés est plus succincte quant à la définition du responsable de traitement. C'est, « *sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ces traitements, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens*[47] ».

Le destinataire est : « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers ; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une*

[45] Article 5 de la loi du 6 janvier 1978 : « *Est dénommé traitement automatisé d'informations nominatives au sens de la présente loi tout ensemble d'opérations réalisées par des moyens automatiques, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives.* »

[46] Article 2, d) de la directive européenne 95/46/CE.

[47] Article 3 de la loi informatique et libertés.

mission d'enquête particulière ne sont toutefois pas considérés comme des destinataires[48] ». A cette définition, la loi informatique et libertés apporte une précision en indiquant que le destinataire doit être une personne « *autre que la personne concernée, le responsable de traitement, le sous-traitant*[49] *et les personnes qui, à raison de leurs fonctions sont chargées de traiter les données*[50] *».*

La personne concernée est, selon la directive européenne 95/46/CE, « *une personne physique identifiée ou identifiable* ». Cette définition déduite de celle des « données à caractère personnel » manque de précision. C'est probablement ce qu'a essayé d'améliorer la proposition de règlement européen en donnant une version beaucoup plus élaborée. Aux termes de ce dernier texte, la personne concernée est « *une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par tout autre personne physique ou morale, notamment par référence à un numéro d'identification, à 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*[51] *».* La loi informatique et libertés est beaucoup plus concise à ce sujet. Il s'agit de « *celle à laquelle se rapportent les données qui font l'objet du traitement*[52] *».*

L'hébergeur n'est pas défini par la loi informatique et libertés, mais la directive européenne sur le commerce électronique présente l'activité d'hébergement comme la « *fourniture d'un service de la société de l'information consistant à stocker des informations fournies par le destinataire du service*[53] ». L'Asip santé en donne plus de précisions. Elle « *recouvre plusieurs réalités : elle peut consister en une application associant traitement et archivage des données. Il peut s'agir d'un simple archivage ou de la fourniture d'un site de*

---

[48] Article 2, g) de la directive européenne 95/46/CE.

[49] « *Le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ». Article 2, e) de la directive européenne 95/46/CE.

[50] Article 3 de la loi informatique et libertés.

[51] Article 4 de la proposition de règlement européen.

[52] Article 2 de la loi informatique et libertés.

[53] Article 14 de la directive européenne sur le commerce électronique. *Directive 2000/35/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« directive sur le commerce électronique »). JOCE n° L 178 du 17 juillet 2000. P. 0001 - 0016. http//eur-lex.europa.eu.

sauvegarde. Participe à l'hébergement tout opérateur intervenant dans cette chaîne de valeurs ». L'hébergeur est donc le prestataire technique offrant de tels services. En matière de gestion électronique des données médicales, l'hébergeur joue un rôle très important en ce sens qu'il doive garantir leur confidentialité, leur sécurité et leur pérennité lorsqu'elles lui sont confiées. Une telle extension de leur responsabilité par rapport aux autres hébergeurs de données se justifie par la sensibilité qui caractérise ces données médicales.

Finalement, au sens de cette étude, la gestion électronique des données s'entend de la collecte, l'enregistrement, la conservation, l'accès, l'utilisation, le partage, l'échange, la gestion administrative, la responsabilité éventuelle des gestionnaires des systèmes, l'évaluation et le suivi et la conception des systèmes et réseaux d'information.

2. Les données médicales

L'expression « *données médicales* » n'était définie par aucune loi française ni aucun texte international jusqu'à la proposition de règlement européen adopté fin 2013 précitée. Seule la recommandation R(97) 5 du Conseil de l'Europe essayait d'en donner en indiquant que « *l'expression "données médicales" se réfère à toutes les données à caractère personnel relatives à la santé d'une personne. Elle se réfère également aux données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques*[54] ». Quant à l'expression « données génétiques », elle se réfère à *toutes les données, quel qu'en soit le type, qui concernent les caractères héréditaires d'un individu ou qui sont en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés*. Elle se réfère également à *toute donnée portant sur l'échange de toute information génétique (gènes) concernant un individu ou une lignée génétique, en rapport avec les aspects, quel qu'ils soient, de la santé ou d'une maladie*, qu'elle constitue ou non un caractère identifiable. La lignée génétique est constituée par des similitudes génétiques résultant d'une procréation et partagée par deux ou plusieurs individus[55]. » Les données génétiques sont donc une catégorie particulière de données médicales que la recommandation sépare des autres données relatives à la santé[56].

[54] Recommandation R(97) 5 du Conseil de l'Europe. I. Définitions.

[55] Idem.

[56] La spécificité de la donnée génétique réside dans le fait qu'elle ait « *une double nature : elle peut soit être primaire et s'entendre alors d'un ensemble de messages génétiques contenus dans le génome, soit être dérivée, et*

En somme, selon la Recommandation, les données médicales sont composées de deux types d'information : les données à caractère personnel relatives à la santé et les données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques. Le texte définit les données génétiques mais ne donne pas plus de détails sur les autres composantes des données médicales. Or, il semble difficile de distinguer des données « relatives à la santé » des données « ayant un lien manifeste et étroit avec la santé ». Pour notre part, les données relatives à la santé seraient celles reconnues par tous comme étant des renseignements utilisés universellement dans le domaine médical pour décrire l'état de santé d'un individu (résultats d'analyses médicales, traitements, antécédents médicaux, etc.). Les données ayant un lien manifeste et étroit avec la santé seraient des informations qui directement ou non pourraient permettre d'avoir des pistes de réflexion sur l'état de santé d'un individu. En d'autres termes, ce serait plus des indices que des informations directement liées à la santé (lieu de vie, origines raciales, etc.). L'avis[57] du groupe européen d'éthique relatif à l'utilisation des données personnelles de santé de 1999 pourrait nous éclairer dans ce sens du fait des détails qu'il donne du contenu des données personnelles de santé. « *Les données personnelles de santé englobent un large éventail d'informations qui toutes touchent à la vie privée de la personne concernée. Elles incluent non seulement les données médicales de base : historique des interventions médicales subies par l'intéressé, médicaments qui lui ont été prescrits, résultats d'analyses divers (biologiques, radiologiques, etc.), 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 : admission dans les établissements de santé et décharges établies lors de ces admissions, données opérationnelles de routine, conditions d'assurance de la personne et autre données financières.* »

Dans un avis sur les données de santé informatisées, la conférence nationale de la santé abonde dans le même sens en définissant les données de santé comme « *les informations sur l'état de santé et les maladies d'un individu ou d'une population donnée mais aussi sur les*

---

signifier ici l'information qui dérive de la reconnaissance d'un génome d'un individu permettant, ainsi d'être renseigné sur sa santé et son identité. À ces deux facettes correspondent deux régimes de protection. Le droit au respect protège l'information génétique humaine comme un élément du corps humain. Le droit au secret protège quant à lui l'information génétique dérivée au même titre que les informations personnelles sensibles ». DE LAMBERTERIE, Isabelle. *Informatique, Libertés et recherche médicale.* p. 74.

[57] Groupe européen d'éthique. Avis n° 13 du 30 juillet 1999 relatif aux aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information. p. 3 - 4. http://ec.europa.eu/bepa/european-group-ethics/docs/avis13_fr.pdf. Consulté le 22 mai 2014.

éléments qui peuvent déterminer l'état de santé et les maladies (facteurs de risques médicaux, biologiques ou génétiques, comportements de santé, consommation des soins, positions sociales, conditions de travail, conditions de vie, environnement physique de l'habitat…)[58] **».**

La proposition de règlement européen employant l'expression « *donnée concernant la santé* » propose la définition suivante « *toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne*[59] ». C'est une des innovations que ce texte apporte à la législation européenne comme l'explique l'exposé des motifs de cette proposition[60]. A la forme conditionnelle, elle propose le contenu des données médicales dans son considérant 26. « *Les données à caractère personnel concernant la santé devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée ; les informations relatives à l'enregistrement du patient pour la prestation de services de santé, les informations relatives aux patients ou à l'éligibilité du patient à des soins de santé ; un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destiné à l'identifier de manière univoque à des fins médicales ; toute information relative au patient recueillie dans le cadre de la prestation de services de santé audit patient ; des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques ; l'identification d'une personne en tant que prestataire de soins de santé au patient ; ou toute information concernant par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro.* »

---

[58] Conférence nationale de la santé . Assemblée plénière. *Avis sur les données de santé informatisées*. 19 octobre 2010. P. 3. http://www.sante.gouv.fr/IMG/pdf/Avis_donnees_sante_19102010.pdf. Consulté le 12 mai 2014.

[59] Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection de données). Article 4. 12. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 27 mai 2014.
Dans sa décision du 12 mars 2014, le Parlement européen a amendé l'article 4 en proposant d'employer l'expression " toutes données à caractère personnel relative à la santé" en lieu et place de "toute information relative à la santé". Parlement européen. *Résolution législative sur la proposition de règlement*. 12 mars 2014. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR. Consulté le 11 septembre 2014.

[60] Point 3.4: Explication détaillée de la proposition. p. 8.

En France, sans définir les données médicales, la législation en donne un contenu sous diverses appellations. La loi[61] informatique et libertés les présente comme « *des données à caractère personnel qui sont relatives à la santé des personnes* » dont la collecte ou le traitement est, en principe, interdit. A titre d'exemple, sont cités les diagnostics médicaux, les données relatives à l'administration de soins ou de traitements, la gestion des services de santé ou les données recueillies pour des raisons de recherche dans le domaine de la santé dont le traitement n'est admis que dans la mesure ou sa finalité l'exige.

Le code de la santé publique emploie les expressions « *données de santé à caractère personnel* », « *informations médicales* » et « *des informations concernant sa santé* » dans les dispositions prises en vue de garantir leur confidentialité et leur sécurité. L'article L 1111-8 cite « *les informations recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins* ». Quant à l'article L 1110-4, il fait référence aux « *données concernant une personne prise en charge par un professionnel de santé, un établissement de santé, un réseau de santé ou tout autre organisme participant à la prévention et aux soins* ». Et l'article L 1111-7 utilisant l'expression « *informations concernant sa santé* » en donne quelques exemples : «*résultats d'examens, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mises en œuvre, feuilles de soins, 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.* »

La jurisprudence[62] de la Cour de justice des communautés européennes (CJCE) en a fait une large interprétation en 2003, en incluant dans la notion de « données relatives à la santé » les informations concernant les aspects, tant physiques que psychiques, de la santé d'une personne. Dès lors, « *l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie constitue une donnée à caractère personnel relative à la santé au sens de l'article*[63] *8 § 1 de la directive 95/46* ».

---

[61] Article 8.

[62] CJCE. Affaire C- 101/01. Arrêt. Luxembourg, le 6 novembre 2003. http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=205847. Consulté le 30 mai 2014

[63] L'article 8 de la directive intitulé « *traitement portant sur des catégories particulières de données* », prévoit : «*Les États membres interdisent le traitement des données à caractère personnel qui révèle l'origine raciale ou éthique ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle*».

Si la lecture de ces dispositions relève une légère différence dans le contenu des données médicales, elles ont en commun de les présenter comme des données personnelles ou encore « données à caractère personnel » caractérisées par une certaine sensibilité qui justifie les mesures particulières prises pour assurer leur sécurité.

Aux termes de l'article 2 de la loi informatique et libertés, constitue « *une donnée à caractère personnel 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peuvent avoir accès le responsable du traitement ou toute autre personne* ». Une donnée médicale est donc une donnée relative à sa santé pouvant permettre d'identifier un individu. Elle fait partie de celles qui sont régies par la section de la loi informatique et libertés relative aux dispositions propres à certaines catégories de données[64]. Ce sont des données que la doctrine a qualifié de « données sensibles ». Elles ne sont pas définies par le droit positif. Le dictionnaire Robert qualifie de « *sensible* » l'état de ce qui est très délicat, qui requiert une attention, des précautions particulières à cause des réactions possibles. Dans la même logique, l'on remarque que ces données font l'objet de restrictions particulières quant à leur traitement tant par la convention du Conseil de l'Europe de 1981 que par la directive européenne de 1995. Elles bénéficient d'une protection renforcée par le droit positif. Ces données sont dites sensibles car leurs traitements comportent des risques beaucoup plus considérables que ceux des autres données à caractère personnel dans la mesure où cela engage d'autres droits fondamentaux notamment la liberté d'opinion, la liberté de conscience, ou peut occasionner d'éventuelles discriminations. Ainsi, les données médicales sont-elles préservées pour protéger l'individu contre toute discrimination[65] due à son état de santé. Tous les textes précités s'accordent sur le fait que ces données, par nature, particulièrement sensibles et vulnérables du point de vue des droits fondamentaux et de la vie privée méritent une protection spécifique ; c'est pourquoi elles ne devraient pas faire l'objet d'un traitement, à

[64] Ce sont « *des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou éthiques, 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* ». Article 8, I. Cette liste, dont le cadre a été fixé depuis la convention du Conseil de l'Europe de 1981 a été reprise par l'article 8 paragraphe 1 de la directive européenne 95/46/CE du 24 octobre 1995.

[65] L'exemple le plus fréquent est celui de la possibilité du régime d'une demande de souscription d'un contrat d'assurance ou celui du contrat de travail.

moins que la personne concernée n'y consente expressément ou que la loi ne le permette pour des questions d'intérêt général.

En réalité, la société actuelle multiplie les traitements automatisés de données médicales pour des raisons économiques. Or, en l'état actuel de la législation française (et plus encore au niveau international), il existe plusieurs questions non encore élucidées pour garantir la protection des données sensibles. Vu l'évolution technologique qui aggrave de jour en jour les problèmes de sécurité informatique, des intérêts se trouvent alors opposés. Faut-il privilégier les avantages économiques malgré les risques d'abus que comporte la gestion électronique de données de santé ou faut-il renoncer à cette évolution en faveur de la protection de la vie privée ? Quel encadrement juridique faudrait-il adopter pour garantir davantage la protection des droits et libertés des individus dans la gestion électronique des données médicales devenues indispensables dans l'évolution actuelle de la société ? En somme, quelle est l'opportunité de la gestion électronique des données médicales lorsque celles-ci sont ainsi exposées à des abus ?

Pour répondre à cette préoccupation il convient de présenter l'organisation juridique mise en place par le gouvernement français qui a le mérite d'être l'une des mieux encadrée au monde en la matière. Elle sera présentée sous deux axes principaux : d'une part, le cadre juridique du traitement automatisé des données médicales (première partie) et d'autre part, le cadre juridique du partage des données médicales (deuxième partie).

Première partie : LE CADRE JURIDIQUE DU TRAITEMENT AUTOMATISE DES DONNEES MEDICALES

Le droit positif impose certaines règles aux responsables de traitement automatisé de données personnelles. La plupart d'entre elles sont communes à toutes les données personnelles (Chapitre 1) tandis que quelques unes sont propres aux données médicales (Chapitre 2).

CHAPITRE I: LE CADRE JURIDIQUE COMMUN DU TRAITEMENT AUTOMATISE DES DONNEES PERSONNELLES

Les règles communes aux traitements concernent autant la procédure à suivre pour les effectuer en toute légalité (paragraphe 1) que les principes généraux qui les régissent (paragraphe 2).

Section 1 : Les formalités préalables à la mise en œuvre des traitements

Le traitement automatisé d'informations, qu'elles soient directement ou indirectement nominatives doit respecter certaines formalités pour avoir une valeur légale. La loi informatique et libertés ayant pour vocation majeure de veiller au respect des libertés individuelles a consacré son chapitre IV à celles-ci. Le législateur y prévoit une procédure de déclaration (Paragraphe 1) et une procédure d'autorisation (Paragraphe 2).

Paragraphe 1 : La procédure de déclaration

Le régime de droit commun en la matière prévoit que les traitements automatisés de données à caractère personnel font, au préalable, l'objet de déclaration auprès de la CNIL (A). Cette procédure peut être très allégée au point de dispenser certains traitements de déclaration préalable (B).

A.La déclaration auprès de la CNIL

La déclaration est une requête adressée à la CNIL par voie postale ou par voie électronique. La déclaration peut être « ordinaire, stricte » (a) ou simplifiée (b).

1. La déclaration «ordinaire»

Nous qualifions cette déclaration d'« ordinaire », « de stricte » pour la distinguer de la déclaration simplifiée prévue par l'article 24, I. C'est celle qui se fait dans le strict respect des règles de forme en la matière sans aucune forme de facilité ou lourdeur supplémentaire.

Aux termes de l'alinéa 1er de l'article 22 de loi informatique et libertés, *« A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.»*

L'article 25 est relatif au traitement des données à caractère politique, philosophique, des données concernant la santé et à la vie sexuelle ; les données génétiques ; les infractions ; l'exclusion d'un droit ; les interconnexions ; le NIR ; les difficultés sociales ; la biométrie. L'article 26 fait référence aux traitements portant sur la sûreté de l'État, la sécurité publique et les infractions pénales. Et, l'article 27 porte sur les traitements publics, le NIR, la biométrie, ceux faits pour le compte de l'État, le recensement et les téléservices. Enfin, le deuxième alinéa de l'article 36 est consacré à la conservation d'archives.

La restriction opérée par l'alinéa 1er de l'article 22 concernant les articles sus- cités semble signifier que les traitements qui doivent faire l'objet de déclaration sont ceux qui ne portent pas sur des informations très « sensibles » c'est-à-dire celles qui ne sont pas liées à l'intimité même de l'individu ou à des questions d'intérêt national. Ce sont les traitements dont le degré de « dangerosité » est relatif. La directive de 1995[66] s'attache également à ce critère de « dangerosité » pour les libertés en prévoyant une procédure de notification à l'autorité de contrôle préalablement à la mise en œuvre de tout traitement. C'est probablement, celle-ci qui a inspiré le législateur en 2004 [67]: au lieu de continuer de

[66] Article 18, 1. de la 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 : *« Les États membres prévoient que le responsable du traitement, ou le cas échéant son représentant, doit adresser une notification à l'autorité de contrôle visée à l'article 28 préalablement à la mise en œuvre d'un traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées ».*

[67] Loi informatique et libertés modifiée en 2004.

distinguer[68] les formalités réservées aux fichiers dits « publics » de celles de fichiers du secteur privé, il a finalement adopté une procédure presqu'unitaire[69]. En effet, avec l'évolution de la micro-informatique et d'Internet, on s'est rendu compte que les risques d'atteinte aux libertés sont pratiquement les mêmes quel que soit le secteur d'activité.

L'article 23 de la loi informatique et libertés précise les conditions d'exécution de la déclaration. Celle-ci comporte l'engagement que le traitement satisfait aux exigences de la loi et peut être adressée à la CNIL par voie électronique. Il est ensuite, délivré, sans délai, un récépissé sous un format papier ou par voie électronique. Le demandeur pourra mettre en œuvre le traitement dès réception de ce récépissé. Ce qui ne l'exonère d'aucune de ses responsabilités. Lorsque les traitements relèvent d'un même organisme et ont des finalités identiques ou liées entre elles, ils peuvent faire l'objet d'une déclaration unique. Dans ce cas, les informations requises en application de l'article 30 précité ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

Même si tout cela ne semble pas bien compliquer, le législateur a prévu une modalité de déclaration simplifiée.

2. La déclaration simplifiée

La déclaration simplifiée est énoncée par l'article 24, I[70]. Cette procédure est prévue pour les catégories de traitement dont les risques d'atteintes aux libertés et à la vie privée paraissent moins graves. Tout comme pour la déclaration dite « ordinaire » la directive de 1995 prévoit, pour certains traitements, une notification simplifiée à l'autorité de contrôle.
La déclaration simplifiée peut être effectuée si le traitement considéré est strictement conforme aux normes prévues par la CNIL pour les traitements les plus courants. Cette

[68] Les articles 15 et 16 de la version initiale (6 janvier 1978) de la loi informatique et libertés prévoyaient que les traitements du secteur public sont décidés par un acte réglementaire pris après avis motivé de la CNIL alors que ceux effectués par les personnes autre que l'État font l'objet de déclaration préalable auprès de la CNIL.

[69] Il ne faut pas omettre que les traitements cités par les articles 26 et 27 portant essentiellement sur des fichiers publics restent soumis à autorisation, à des formalités plus lourdes que la simple déclaration.

[70] Pour les catégories les plus courantes de traitements de données à caractère personnel, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés, la Commission nationale de l'informatique et des libertés établit et publie, après avoir reçu le cas échéant les propositions formulées par les représentants des organismes publics et privés représentatifs, des normes destinées à simplifier l'obligation de déclaration.

déclaration simplifiée de conformité peut également être envoyée à la CNIL par voie électronique.

Pour mettre en œuvre cette procédure simpliste de l'obligation de déclaration, la CNIL, après réception des propositions formulées par les représentants des organismes publics et privés représentatifs, établit et publie un ensemble de normes simplifiées en guise de référence. Celles-ci sont accessibles sur le site[71] de la Commission. Ainsi, par exemple, la norme 41 correspond aux instruments financiers, la 43 à la gestion de l'état civil dans les communes et la norme simplifiée 53 est prévue pour la gestion des laboratoires d'analyses et de biologie médicale par les biologistes.

Ces normes précisent[72] :

1° Les finalités des traitements faisant l'objet d'une déclaration simplifiée ;

2° Les données à caractère personnel ou catégories de données à caractère personnel traitées ;

3° La ou les catégories de personnes concernées ;

4° Les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;

5° La durée de conservation des données à caractère personnel.

Comme pour la déclaration ordinaire, la loi autorise le responsable du traitement à effectuer une déclaration unique en tenant compte des finalités, des destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées lorsque celui-ci a plusieurs traitements à déclarer qui relèvent d'un même organisme et ont des finalités identiques ou liées entre elles .

Mais le législateur accorde à certains traitements une dispense de déclaration.

B. Les dispenses de déclaration

Nées de la modification, en 2004, de la loi de 1978, les dispenses de déclaration sont des exonérations légales de formalités préalables qui sont prévues dans différents cas : soit du fait de la nomination d'un correspondant informatique et libertés (1), soit du fait de la nature relativement inoffensive de certains traitements pour la vie privée et les libertés (2).

[71] http://www.cnil.fr/en-savoir-plus/deliberations/normes-simplifiees/

[72] Article 24, I de la loi informatique et libertés

1. La dispense du fait de la nomination d'un correspondant informatique et libertés

L'article 22, III de la loi informatique et libertés prévoit que « *les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel (…) sont dispensés des formalités prévues aux articles 23* (déclaration) *et 24* (déclaration simplifiée), *sauf lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne est envisagé* ». Qu'est-ce qu'un correspondant informatique et libertés et quelles sont ses attributions au point de permettre que les traitements effectués par l'entreprise qui en a désigné un soient exonérés de déclaration préalable?

a. Le statut du correspondant informatique et libertés

La loi n'a pas donné de définition mais a décrit ses attributions. Le correspondant à la protection des données à caractère personnel, communément appelé correspondant informatique et libertés (CIL) exerce une fonction née, en France, de la modification du 6 Août 2004 de la loi du 6 janvier 1978. Celle-ci existe dans d'autres pays comme l'Allemagne (*Datenschutzbeauftragte* (préposé à la protection des données), créé dans les années 1970[73]), les Pays-Bas (*functionaris gegevensbescherming* (délégué à la protection des données)*[74]*), la

[73] Le premier préposé à la protection des données d'Allemagne a été nommé par l'État de Hesse en 1971. Le 7 octobre 1970, le Land de Hesse a été le premier État à voter une loi sur la protection des données. Loi du Land de Hesse (RFA) du 7 octobre 1970 in Gesetz-und verordnungsblatt für das Land Hesse, Teil I Nr 41, Wiesbaden, 12.X.1970. Texte français in: GBF Niblett, L'information numérique et la protection des libertés individuelles, Paris, OCDE. 1971, pp. 51 - 56. in BERLEUR, Jacques. *Vingt ans de lois relatives à l'informatique. Quels acquis ? Quels défis ? En tout cas, encore un long chemin…* in journal de réflexion sur l'informatique n° 17. 1991. P. 41. http://www.anthologieprivacy.be/sites/anthology/files/Vingt_ans_de_lois_relatives_%C3%A0_l%27informatique._Quels_acquis%3F_Quels_d%C3%A9fis%3F_En_tout_cas%2C_encore_un_long_chemin_....pdf. Consulté le 28mars 2014.
Les attributions du préposé à la protection des données personnelles en Allemagne sont actuellement régies par les paragraphes 4f et 4g de la loi fédérale sur la protection des données (BDBS) du 27 janvier 1977. La dernière version de cette loi, modifiée en août 2009 est entrée en vigueur en septembre 2009 et en avril 2010. Federal Data Protection Act. Federal law. Gazette I, p. 2814. Http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile. Consulté le 28 mars 2014.

[74] Les fonctions de délégué à la protection des données aux Pays-Bas sont régies par les articles 62 à 64 de la *Wet Bescherming personsgegevens* du 6 juillet 2000. http://maxius.nl/wet-bescherming-persoonsgegevens. Consulté le 11 août 2013

Suède (*personuppgiftsombud*[75] *(*délégué à la protection des données*)* et le Luxembourg (chargé de la protection des données)[76]. Elle tire sa véritable origine de la transposition de la directive 95/46 qui prévoit la désignation d'un détaché à la protection des données personnelles à son article 18, 2 comme condition requise pour qu'un État autorise une simplification ou une dérogation de l'obligation de notification. Ce correspondant à la protection des données à caractère personnel est différent du correspondant de presse désigné par les organes de presse écrite ou audiovisuelle à des fins journalistiques (article 67 de la loi informatique et libertés et article 56 du décret du 20 octobre 2005 pour l'application de la loi informatique et libertés).

La désignation du correspondant est facultative mais, une fois faite, elle doit être notifiée[77] à la Commission nationale de l'informatique et des libertés, après les organes représentatifs du personnel, dans les formes prescrites[78] par le décret. Cela permet à la CNIL de se rassurer d'avoir une personne avisée qui garde constamment un regard sur la gestion des données personnelles. Il sert, alors, d'intermédiaire, de médiateur, entre l'organisme, les personnes dont les données sont traitées et elle. Le correspondant peut être un collaborateur du responsable du traitement (mais pas le responsable des traitements ni son représentant légal) ou un agent extérieur[79] à l'organisme responsable des traitements. Il devient un

[75] La fonction de délégué à la protection des données en Suède est régie par les articles 37 à 40 de la loi personuppgiftslag du 29 avril 1998: 204 modifiée par 2010:1969 entrée en vigueur le 1er avril 2011. http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/?bet=1998:204. Consulté le 23 janvier 2013.

[76] Les attributions du chargé de la protection des données au Luxembourg sont régies par l'article 40 de la loi du 2 août 2002 modifiée. http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod _fr.pdf#zoom= 125,0,0& page mode=none et le règlement grand-ducal du 27 novembre 2004. Mémorial A n° 200 du 20.12.2004. http://www.legilux.public.lu/leg/a/archives/2004/0200/a200.pdf . Consulté le 28 mars 2014.

[77] Article 43 du décret 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.

[78] Article 45 du décret 2005-1309 précité : « La désignation d'un correspondant à la protection des données à caractère personnel est, préalablement à sa notification à la Commission nationale de l'informatique et des libertés, portée à la connaissance de l'instance représentative du personnel compétente par le responsable des traitements, par lettre remise contre signature ».

[79] Article 44 du décret 2005-1309 précité : « Lorsque plus de cinquante personnes sont chargées de la mise en œuvre ou ont directement accès aux traitements ou catégories de traitements automatisés pour lesquels le responsable entend désigner un correspondant à la protection des données à caractère personnel, seul peut être désigné un correspondant exclusivement attaché au service de la personne, de l'autorité publique ou de l'organisme, ou appartenant au service, qui met en œuvre ces traitements.
Par dérogation au premier alinéa :
a) Lorsque le responsable des traitements est une société qui contrôle ou qui est contrôlée au sens de l'article L. 233-3 du code de commerce, le correspondant peut être désigné parmi les personnes au service de la société qui contrôle, ou de l'une des sociétés contrôlées par cette dernière ;

personnage central dans la gestion des données personnelles au sein de l'organisme public ou privé ou l'association ou toute administration qui le désigne. Le correspondant veille au respect des droits personnels des usagers, des clients et des salariés, fait donc office de conseil et aide à l'application de la loi en la matière. C'est un interlocuteur qualifié[80] ayant des compétences en matière de protection des données personnelles dont la présence permet d'alléger les formalités déclaratives. En revanche, sa désignation n'exonère pas des demandes d'avis et d'autorisation dans les domaines où la loi les requiert obligatoirement[81] et la dispense n'est limitée qu'aux traitements qui n'engagent pas de transfert de données personnelles hors des frontières de l'Union Européenne.

Menant son activité en toute autonomie vis-à-vis du responsable du traitement, les missions du correspondant sont précisées par le décret d'application du 20 Octobre 2005[82].

---

b) Lorsque le responsable des traitements est membre d'un groupement d'intérêt économique au sens du titre V du livre deuxième du code de commerce, le correspondant peut être désigné parmi les personnes au service dudit groupement;
c) Lorsque le responsable des traitements fait partie d'un organisme professionnel ou d'un organisme regroupant des responsables de traitements d'un même secteur d'activités, il peut désigner un correspondant mandaté à cette fin par cet organisme. »

[80] La loi prévoit que le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Aucun agrément n'est prévu et aucune exigence de diplôme n'est fixée. Néanmoins, le correspondant doit disposer de compétences adaptées à la taille et à l'activité du responsable de traitement. Ces compétences et qualifications doivent porter tant sur la législation relative à la protection des données à caractère personnel que sur l'informatique et les nouvelles technologies, sans oublier le domaine d'activité propre du responsable des traitements. Ainsi, si la connaissance de la loi Informatique et Libertés est essentielle, les connaissances du correspondant devront aussi porter sur les législation particulières au secteur d'activités du responsable de traitement (par exemple en matière de commerce électronique, de santé ou du travail..), sur les règles spécifiques aux conditions de recueil et de traitement de certaines données (données couvertes par exemple par le secret médical, le secret bancaire...). En informatique, une connaissance du vocabulaire et des métiers de l'informatique parait également nécessaire, de même que des différents modes de traitement des données. Les connaissances du correspondant porteront par exemple sur les systèmes de gestion et d'exploitation de bases de données, les types de logiciels et modes de stockage de données, les types de fichiers, ainsi que sur les éléments d'une politique de confidentialité et de sécurité (chiffrement des données, signature électronique, biométrie,...). Elles doivent lui permettre de suivre le déploiement des projets informatiques et de Conseiller utilement le responsable de traitement.
Extrait du *guide du correspondant informatique et libertés* de la CNIL. Janvier 2006. p.8 http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Guide_correspondants.pdf. Consulté le 19 mai 2014.

[81] Article 25 à 27 de la loi informatique et libertés

[82] 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°247 du 22 octobre 2005 page 16769 texte n° 31

b. Les missions du correspondant informatique et libertés

L'article 22, III présente ce personnage comme *« un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations… »*. Comment exerce-t-il cette fonction, quelles sont ses missions et quelles tâches accomplit-il concrètement ?

Le correspondant exerce directement ses fonctions auprès du responsable des traitements mais ne reçoit aucune instruction pour l'exercice de ses missions et ne peut recevoir de sanction de sa part du fait de l'accomplissement de celles-ci. En outre, il ne peut exercer, au sein de l'établissement, aucune autre fonction susceptible d'être à l'origine d'un éventuel conflit d'intérêts. Il en serait ainsi, notamment, d'une fonction qui, de fait ou de droit l'emmènerait à décider de la finalité des traitements, de l'objectif poursuivi ou des moyens à mettre en œuvre pour les interrompre.

Si sa présence dispense l'organisme de déclaration, en interne, le responsable est tenu de l'informer, de l'impliquer totalement dans la gestion des données personnelles en lui dévoilant tous les fichiers à traiter et en suivant ses conseils. Cela l'oblige donc, à prendre les dispositions adéquates pour assurer le respect des droits et obligations depuis le choix du système d'information qui servira au traitement jusqu'à la dernière mesures de sécurité prise dans le cadre des traitements des informations personnelles.

Dès lors, les missions du correspondant consistent, dans les 3 mois suivant sa désignation, à établir une liste[83] des traitements pour lesquels il a été nommé et à la laisser disponible pour la CNIL et les personnes qui en font la demande. Celle-ci doit être tenue régulièrement à jour. Il établit un bilan annuel de ses activités qu'il présente au responsable des traitements et tient à la disposition de la CNIL.

[83] Article 48 du décret 2005-1309 «(…) La liste précise, pour chacun des traitements automatisés :
1° Les nom et adresse du responsable du traitement et, le cas échéant, de son représentant ;
2° La ou les finalités de traitement ;
3° Le ou les services chargés de le mettre en œuvre ;
4° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès et de rectification ainsi que leurs coordonnées ;
5° Une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ;
6° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;
7° La durée de conservation des données traitées. »

Le correspondant, en tant que conseil, médiateur et gardien de la loi informatique et libertés peut, ainsi, faire des recommandations quant aux modalités de traitement et recevoir, transmettre les requêtes des personnes dont les données sont traitées aux services en charge. Par la suite, il apporte ses conseils aux requérants et veille à ce que les droits d'information, d'accès et d'opposition soient respectés par sa contribution à l'élaboration et à la diffusion des notes d'information et des affiches. Le correspondant élabore et contrôle l'application des codes de conduite spécifiques en vue de sensibiliser le personnel aux dispositions de la loi (à partir d'une charte sur l'utilisation de moyens informatiques et sur la sécurité ou d'un règlement intérieur). Son champ d'activité peut être étendu à l'établissement de listes de l'ensemble des traitements mis en œuvre par l'organisme (traitements automatisés ou non, traitements soumis à autorisation ou avis, traitements exonérés par la loi ou par la CNIL) y compris les traitements non dispensés de déclaration.

Lorsqu'il constate des difficultés dans l'application de la loi, le correspondant y attire l'attention du responsable des traitements et lui propose des solutions pour y remédier mais en cas de recommandation infructueuse, il en informe la CNIL. De même, la Commission est-elle saisie lorsque le correspondant rencontre des difficultés sérieuses pour exercer correctement ses missions alors même que le responsable en est informé ou en est l'instigateur ; la CNIL adresse une injonction[84] au responsable qu'il est tenu de respecter sous peine de sanction.

La fonction du correspondant peut prendre fin[85] de différentes manières : soit par démission, soit à l'expiration du contrat le nommant, soit à la demande du responsable des traitements ou de la CNIL. Mais, dans tous les cas où la CNIL n'est pas l'initiateur, cette décision doit lui être notifiée et motivée avant de prendre effet tout comme en cas de remplacement du correspondant.

Le correspondant se révèle être un personnage de plus en plus indispensable dans le domaine de la protection des données personnelles en administration, vue la montée constante de l'insécurité numérique. En revanche, il a été constaté que ceux qui exercent actuellement la fonction manquent de moyens pour mener à bien leurs missions. C'est d'ailleurs ce qui a amené Aurélie GOYER[86], après une étude[87] menée sur la question, à préconiser de

[84] Article 55 du décret d'application 2005-1309.

[85] Articles 52 à 54 du décret d'application 2005-1309 sus-cité.

[86] Aurélie GOYER est Chargée d'affaires juridiques du Conservatoire national des arts et métiers (Cnam) et diplômée du Mastère Spécialisé « Management et Protection des données à caractère personnel » de l'ISEP.

« *permettre à la fonction de se professionnaliser, en s'appuyant sur trois éléments : le renforcement des pouvoirs de contrôle de la CNIL, la prise de conscience de l'intérêt de préserver le patrimoine informationnel de l'entreprise, et l'intérêt grandissant de l'opinion publique pour la protection de la vie privée des citoyens* ». Mais tout espoir n'est pas perdu car la CNIL a, à son niveau, pris des mesures visant à promouvoir la fonction en prenant une décision[88] et une délibération[89] tendant à permettre aux correspondants d'acquérir un site web. D'un autre côté, une proposition de loi[90] des sénateurs ESCOFFIER et DETRAIGNE du 6 novembre 2009 va dans ce sens. En effet, visant à mieux garantir le droit à la vie privée à l'heure du numérique, cette proposition rend la profession de correspondant informatique et libertés obligatoire pour les entreprises publiques ou privées dans lesquels plus de 100 employés peuvent avoir à traiter des données à caractère personnel qui sont en principe, soumis à une procédure d'autorisation. Cette proposition, a été adoptée[91] par le Sénat le 23 mars 2010 et une fois promulguée, celle-ci permettra de valoriser davantage la fonction et les moyens suivront probablement.

En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation de la Commission nationale informatique et libertés.

Dans le cadre de son cursus qui prépare à la fonction de correspondant informatique et libertés, elle a soutenu sa thèse professionnelle sur la thématique : « Donne-t-on aux CIL les moyens de remplir leurs missions ? » http://www.globalsecuritymag.fr/Donne-t-on-au-Correspondant,20100208,15876.html. Consulté le 12 mai 2011.

[87] GOYER, Aurélie. *Donne-t-on aux CIL les moyens de remplir leurs missions ?* http://www.formationcontinue-isep.fr/informatiqueetlibertes/informatique-et-libertes-theses. Consulté le 28 mars 2014.

[88] Décision du 30 avril 2009 du président de la CNIL relative à la mise en œuvre par le service des correspondants informatique et libertés d'un site web dédié aux correspondants à la protection des données à caractère personnel JORF n°0142 du 21 juin 2009. Texte n° 48 NOR : CNIA0900010S

[89] Délibération n° 2009-213 sur la création par la Commission nationale de l'informatique et des libertés d'un site web dédié aux correspondants à la protection des données à caractère personnel (demande d'avis n° 1358690) JORF n°0142 du 21 juin 2009 page texte n° 49 NOR: CNIA0900009X

[90] Titre II, article 3 de la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique. Cette proposition crée un chapitre IV bis à la loi informatique et libertés relatif au correspondant informatique et libertés : *« Art. 31-1. - Lorsqu'une autorité publique ou un organisme privé recourt à un traitement de données à caractère personnel et que plus de cinquante personnes y ont directement accès ou sont chargées de sa mise en œuvre, ladite autorité ou ledit organisme désigne un correspondant « informatique et libertés »*. http://www.senat.fr/leg/ppl09-093.html. Consulté le 19 mai 2014.

[91] Sénat. Article 3 insérant un chapitre IV bis à la loi informatique et libertés. *Texte n° 81 (2009-2010) adopté par le Sénat le 23 mars 2010*. http://www.senat.fr/leg/tas09-081.html. Consulté le 19 mai 2014.

En l'absence d'un correspondant informatique et libertés, une entreprise peut également être exonérée de la procédure de déclaration en raison de la nature ou de la finalité du traitement qui est envisagé.

2. Dispense du fait de la nature ou de la finalité du traitement et des personnes impliquées

Certains traitements exonérés de déclaration sont expressément cités par le texte de la loi informatique et libertés mais d'autres sont laissés à l'appréciation de la CNIL.

a. Les dispenses expresses de la loi

Selon l'article 22, II, deux catégories de données sont concernées par cette dispense : d'une part, « *les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime* ». A ce niveau, la CNIL a déjà pris des décisions de confirmation notamment, au sujet des fichiers des démarcheurs bancaires ou financiers[92]. En effet, ayant été saisie par la banque de France en vue de se prévaloir d'une exonération de déclaration pour la tenue d'un fichier des démarcheurs, la CNIL a décidé de l'y autoriser. La Commission a considéré que la finalité du fichier des démarcheurs est bien de tenir un registre qui, en vertu de dispositions du code monétaire et financier, est bien exclusivement destiné *« à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime »*.

D'autre part, sont concernés par la dispense légale, « *les traitements mentionnés au 3° du II de l'article 8 »* c'est-à-dire les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical.
Mais, la dispense de déclaration n'est reconnue à cette dernière catégorie de traitements qu'à certaines conditions : d'abord, si les traitements effectués portent seulement sur les données

[92] CNIL. *Un exemple de registre exclusivement destiné à l'information du public : le fichier des démarcheurs financiers.* 25 mars 2005. www.cnil.fr/.../un-exemple-de-registre-exclusivement-destine-a-linformation-du-public-le-fichier-des-demarcheu/ Consulté le 10 octobre 2009.

sensibles qui correspondent à l'objet de ladite association ou dudit organisme. C'est dire que les traitements portant sur des données sensibles n'entrant pas dans le cadre de l'objet d'une association ou d'un organisme à but non lucratif ne bénéficient pas d'une telle dispense. Cette précision est faite par la dispense de déclaration n° 8[93] abrogée et remplacée par la délibération de 2010-229, qui, bien que se rapportant aux traitements automatisés des données à caractère personnel mis en œuvre par des organismes à but non lucratif ne s'applique pas aux traitements susmentionnés[94]. Cette dispense, réaffirme, en son article 3, l'interdiction de principe de traitement des données *qui font apparaître, directement ou indirectement, les origines raciales ou ethniques les opinions politiques, philosophique ou religieuse ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* telle que dispose l'article 8, I de la loi informatique et libertés.

La seconde condition est qu'il faut que les traitements 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. Enfin, les traitements ne doivent porter que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément. La forme syntaxique des dispositions de l'article 8 donne d'interpréter ces trois exigences comme des conditions cumulatives qu'il n'est pas nécessaire d'appliquer aux traitements[95] visés par l'article 3 de la délibération 2010-229 de la CNIL dès lors qu'ils répondent aux finalités[96] prescrites par l'article 2. Ceux-ci sont considérés par la

---

[93] CNIL. Délibération n° 2006-130 du 9 mai 2006 (décision de dispense de déclaration n° 8) abrogée et remplacée par la délibération n° 2010-229 du 10 juin 2010 dispensant de déclaration les traitements automatisés de données à caractère personnel mis en œuvre par des organismes à but non lucratif.

[94] « *Cette décision ne s'applique pas aux traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dans les conditions définies à l'article 8-II de la loi du 6 janvier 1978 modifiée qui, en application de l'article 22-II de la loi du 6 janvier 78 modifiée, sont dispensés de toute formalité déclarative préalable auprès de la CNIL* ». CNIL. Délibération n° 2006-130 du 9 mai 2006 (décision de dispense de déclaration n° 8).

[95] « *Les données traitées pour la réalisation des finalités décrites à l'article 2 sont:*
- l'identité : nom, prénoms, sexe, date de naissance, adresse, numéro de téléphone (fixe et mobile) et de télécopie, adresse de courrier électronique ;
- les informations relatives à la gestion administrative de l'organisme : état des cotisations, position vis-à-vis de l'association, informations strictement liées à l'objet statutaire de l'organisme, identité bancaire pour la gestion des dons ;
- données de connexion (date, heure, adresse internet protocole de l'ordinateur du visiteur, page consultée) à des seules fins statistiques d'estimation de la fréquentation du site ».

[96] « *Les traitements doivent avoir pour seules finalités :*
- l'enregistrement et la mise à jour des informations individuelles nécessaires à la gestion administrative des membres et donateurs, en particulier la gestion des cotisations, conformément aux dispositions statutaires qui régissent les intéressés ;

CNIL comme des traitements courants et faisant partie de ceux que la loi informatique et libertés lui reconnaît le pouvoir de dispenser de formalités de déclaration.

b. Les dispenses décidées par la CNIL

« La Commission peut définir, parmi les catégories de traitements mentionnés au I, celles qui, compte tenu de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées, sont dispensées de déclaration »[97].

Il ressort de cette disposition que la détermination des traitements dont la déclaration n'est pas nécessaire est une compétence qui peut être exercée par la CNIL après analyse de la situation particulière de chaque traitement. En dehors des règles générales exigeant de minimiser les risques d'atteinte à la vie privée et aux libertés, la Commission s'assure que dans chaque cas d'espèce, les traitements se feront dans le strict respect de ses délibérations. C'est ce qui explique que chaque type de traitement aie fait l'objet de délibération spécifique par la CNIL. Dès lors, si le traitement mis en œuvre n'entre pas dans le cadre des délibérations de la CNIL, le responsable doit absolument se soumettre à la procédure de déclaration.
La liste des traitements dispensés de déclaration est disponible sur le site internet[98] de la CNIL.

La dispense concerne uniquement les *« traitements mentionnés au I »* c'est-à-dire *« les catégories les plus courantes de traitements de données à caractère personnel, dont la mise*

- d'établir, pour répondre à des besoins de gestion, les états statistiques ou des listes de membres ou de contacts, notamment en vue d'adresser bulletins, convocations, journaux. Lorsque ces listes sont sélectives, les critères retenus doivent être objectifs et se fonder uniquement sur des caractéristiques qui correspondent à l'objet statutaire de l'organisme ;
- d'établir des annuaires de membres, y compris lorsque ces annuaires sont mises à la disposition du public sur les réseaux Internet. Le traitement peut avoir également pour finalité la tenue d'annuaire d'anciens élèves ou d'étudiants ;
- d'effectuer par tout moyen de communication des opérations relatives à des actions de prospection auprès des membres donateurs et prospects.
Dans le cas où est utilisé un service de communication au public en ligne (sites Internet), un traitement des données de connexion à des fins purement statistiques peut être effectué. »

[97] Article 24, II de la loi informatique et libertés.

[98] Liste des traitements dispensés de déclaration : http://www.cnil.fr/en-savoir-plus/deliberations/dispenses-de-declaration/. Consulté le 10 octobre 2009.

en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés ». Mais, alors, la question se pose de savoir comment peut-on affirmer sans risque de se tromper, qu'un traitement n'est pas susceptible de porter atteinte à la vie privée et aux libertés ? Sachant qu'en matière informatique, tout comme dans plusieurs autres domaines, le risque zéro n'existe pas, nous estimons que les notions utilisées par le législateur présentent elles-mêmes des risques. Elles paraissent radicales et semblent minimiser le danger encouru par les données personnelles, quel que soit leur degré de sensibilité, dès qu'elles sont recueillies. Il serait peut-être plus prudent d'employer les termes « traitement dont la mise en œuvre est susceptible de porter une atteinte moins grave ». Cela donnerait ainsi, place à une certaine marge de risque et ferait transparaître une certaine conscience de la faillibilité des systèmes d'information même si l'on compte mettre tout en œuvre pour assurer la protection des droits des personnes.

La CNIL se fonde sur certains critères pour décider de dispenser certains traitements de déclaration. Ceux-ci sont relatifs à leurs finalités, aux destinataires ou catégories de destinataires, aux données à caractère personnel traitées, à la durée de conservation de celles-ci et aux catégories de personnes concernées. La Commission veille ainsi au strict respect des principes émis par la loi informatique et libertés en ses articles 6 et 7 comme conditions de licéité des traitements des données à caractère personnel. Ainsi, par exemple, concernant les traitements destinés à la gestion de la rémunération par les personnes morales du secteur privé (délibération n° 2004-097[99] du 9 décembre 2004), les motifs des absences ne doivent pas être conservés au delà du temps nécessaire à l'élaboration des bulletins de paie. De même, dans le cadre de la dématérialisation du contrôle de légalité par les collectivités locales et le représentant de l'État (délibération n° 2006-056[100] du 2 mars 2006), ne peuvent être collectées et traitées que les catégories de données à caractère personnel strictement nécessaires à la rédaction et la transmission des actes visés au code général des collectivités territoriales qui sont soumis au contrôle de légalité ou qui peuvent être évoqués dans ce cadre par le représentant de l'État. Ou encore, s'agissant des traitements mis en œuvre dans le cadre de plans de continuité d'activités relative à une pandémie grippale (délibération n° 2009-476[101] du 10 septembre 2009), ne peuvent, dans la limite de leurs attributions respectives, être

[99] JORF n°4 du 6 janvier 2005 p. 287. Texte n° 54, norme d'exonération n° 02

[100] JORF n°102 du 30 avril 2006. Texte n° 17, norme d'exonération n° 05

[101] JORF n°0222 du 25 septembre 2009 page texte n° 55, norme d'exonération n° 14

destinataires de tout ou partie des informations que les personnes habilitées des services chargés de la gestion du personnel et, le cas échéant, les personnes habilitées en charge de la cellule de crise mise en place au sein de l'organisme.

Toutefois, d'autres traitements peuvent être soumis à une procédure plus rigoureuse ; ils doivent requérir une autorisation avant d'être effectués.

Paragraphe 2 : La procédure d'autorisation

Antérieurement[102] limitée à l'utilisation du répertoire nationale d'identification des personnes physiques en vue d'effectuer des traitements nominatifs, la procédure d'autorisation est actuellement régie par les articles 25 à 29 de la loi informatique et libertés et s'étend à plusieurs traitements.

L'autorisation est requise pour les traitements *« susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées*[103] ». Lorsque l'on traite des données pour le compte de toute personne autre que l'État (A), l'autorité compétente pour délivrer cette permission est différente de celle qui se prononce lorsque l'État est responsable de l'opération et que les fichiers sont particulièrement « sensibles » (B).

A. Les traitements pour le compte de personnes autres que l'État

Aux termes de l'article 25 de la loi informatique et libertés, sont soumis à autorisation de la CNIL, tous les traitements de données personnelles autres que ceux mentionnés aux articles 26 et 27 c'est-à-dire ceux qui sont d'une certaine sensibilité par rapport à l'intérêt

[102] Sous la loi informatique et libertés, article 18, version du 6 janvier 1978.

[103] Article 20,1. de la directive 95 / 46 / CE du 24 octobre 1995 du Parlement européen et du Conseil 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

général et sont faits pour le compte de l'État (ils feront l'objet du prochain point de notre analyse).

L'article 25 établit une liste des traitements soumis à l'autorisation de la CNIL. Il s'agit:

- Des traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 c'est-à-dire: 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[104] 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 légales prescrites; les traitements nécessaires à la recherche dans le domaine de la santé selon les modalités requises pour les traitements de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention .

Si 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 l'individu sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la loi, la CNIL peut autoriser, compte tenu de leur finalité, certaines catégories de traitements sans tenir compte des dispositions particulières des chapitres IX et X relatifs au domaine de la santé. La CNIL peut, également autoriser le traitement automatisé ou non des données sensibles sans tenir compte de l'interdiction si cela est justifié par l'intérêt public.

- Des 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 ;
- Des traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;
- Des traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, 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 ;

[104] Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques**.** JORF du 8 juin 1951 p. 6013.

- Des 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 ou de l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;
- Des 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 ;
- Des traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ou des données biométriques nécessaires au contrôle de l'identité des personnes.

Tout comme pour les procédures de déclaration, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission. Dans ce cas, le responsable de chaque traitement adresse à la Commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

Lorsqu'une demande d'autorisation lui est soumise, la CNIL se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Si elle ne se prononce pas dans ces délais, la demande d'autorisation est réputée rejetée.

B. Les traitements pour le compte de l'État portant sur des fichiers de souveraineté ou des données d'identification

L'autorisation est requise pour la gestion électronique des données personnelles pour le compte de l'État dans deux hypothèses : soit pour le traitement des fichiers de souveraineté, soit pour celui des données d'identification.

1. Les traitements portant sur des fichiers de souveraineté

L'autorisation accordée pour les traitements effectués pour le compte de l'État à la particularité d'émaner d'une autre autorité administrative que la CNIL mais après avis de celle-ci.

S'agissant des fichiers dits de souveraineté, régis par l'article 26 de la loi informatique et libertés, ils sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la CNIL. Il s'agit des traitements « *qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.*»

On constate que pour les fichiers dits de souveraineté, l'avis de la CNIL n'est requis que comme une simple formalité. Le ministre compétent peut ne pas le suivre mais l'avis de la CNIL est publié pour faire mention des réserves qu'elle aurait pu émettre. La Commission voit réduire ses prérogatives qui sous la loi de 1978 consistaient en un avis conforme que l'autorité administrative ne pouvait outrepasser sans un décret pris en Conseil d'État[105]. Il en est de même pour tous les traitements soumis à autorisation. Cet état de fait a été relevé avant l'adoption de la loi modifiant le texte du 6 janvier 1978. En effet, analysant en 2004, la procédure d'autorisation, lors de la seconde lecture du projet de loi, M. Frédéric DUTOIT[106] déplorait la situation. *«Pourront donc être mis en œuvre, malgré un avis défavorable de la CNIL, les fichiers de police, de justice, les fichiers comportant le numéro de sécurité sociale, mais également les interconnexions de fichiers nécessaires à l'établissement ou au recouvrement de l'impôt, autrement dit des fichiers concernant la totalité ou la quasi-totalité de la population française. Cette nouvelle disposition constitue un recul pour les libertés*

[105] Article 15 de la loi du 6 janvier 1978 « *Hormis les cas où ils doivent être autorisés par la loi, les traitements automatisés d'informations nominatives opérés pour le compte de l'État, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés. Si l'avis de la Commission est défavorable, il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'État ou, s'agissant d'une collectivité territoriale, en vertu d'une décision de son organe délibérant approuvée par décret pris sur avis conforme du Conseil d'État* ».

[106] Ancien député, président des élus communistes, républicains et citoyens de Marseille sous la 12ème législature.

individuelles des citoyens et affaiblit la CNIL[107]*»*, aussi gardienne de l'identité humaine, des droits de l'homme, de la vie privée et des libertés en France.

Quand les fichiers de souveraineté portent sur des traitements prévus au I de l'article 8 précité (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), c'est le Conseil d'État qui a la charge de l'autorisation. Il prend alors un décret autorisant le traitement qui comporte également la publication de l'avis motivé de la CNIL.

Toutefois, pour certains des traitements prévus par l'article 26, il peut être décidé une dispense de publication de l'acte réglementaire les autorisant. Cela se fait également, par décret en Conseil d'État. Ce décret publie la dispense de publication de l'acte réglementaire et le sens de l'avis émis par la CNIL.

Il faut noter que la loi ne donne aucune précision ni sur les types de traitements particulièrement visés dans ce groupe par cette mesure exceptionnelle, ni les raisons d'un tel choix. Qu'en est-il des traitements portant sur des fichiers d'identification ?

2. Les traitements portant sur des fichiers d'identification

L'article 27 prévoit une autorisation émanant du Conseil d'État, après avis motivé et publié de la CNIL pour les traitements de données à caractère personnel portant sur le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public. Cette mesure concerne également les traitements de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. La CNIL a, notamment, le 19 juillet 2012 pris une délibération[108] portant avis sur un projet de décret du ministre des affaires sociales et de la santé relative à la

[107] Compte rendu officiel analytique de l'Assemblée nationale session ordinaire 2003 2004, 82ème jour de séance, 205ème séance, jeudi 29 avril 2004. Disponible sur : http://www.assemblee-nationale.fr/12/cra/2003-2004/205.asp. Consulté le 26 mai 2014.

[108] CNIL. Délibération n° 2012-261 du 19 juillet 2012 portant avis sur le projet de décret du ministre des affaires sociales et de la santé relative à la mise en œuvre de services en santé par les organismes de gestion des régimes obligatoires de base d'assurance maladie. RU- 028. www.cnil.fr.

mise en œuvre de services en santé par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie. La Commission a jugé pertinentes, au regard de la finalité poursuivie, les données qui allaient être susceptibles de traitement dans le cadre de cet décret. Il s'agit de données relatives : « *aux coordonnées, aux données d'identification dont le NIR du bénéficiaire éligible au service et le cas échéant, des ses ouvrants droit ou de ses ayants droits; aux informations relatives au bénéficiaire éligible ou adhérent au service proposé notamment des informations relatives au droit à l'assurance maladie, à la vie personnelle et professionnelle ; aux données de santé de la personne éligible ou adhérente au service ; aux données d'identification des professionnels de santé intervenant dans les programmes*. » L'avis favorable donné par la CNIL a conduit à la prise du décret[109] n° 2012-1249 du 9 novembre 2012 autorisant la création de traitement de données à caractère personnel pour la mise en œuvre de programmes de prévention et d'accompagnement en santé des assurés sociaux.

L'article 27 prévoit également des traitements qui peuvent être autorisés par arrêté, ou par décision de l'organe délibérant chargé de leur organisation, pris après avis motivé et publié de la CNIL si le traitement est mis en œuvre pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public. C'est notamment, le cas :

- Des traitements mis en œuvre par l'État ou les personnes morales de droit public ou d'une personne morale de droit privé gérant un service public qui requièrent une consultation du répertoire national d'identification des personnes physiques sans inclure le numéro d'inscription à ce répertoire ;
- Des traitements portant sur le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes :

a) qui ne comportent aucune des données mentionnées au I de l'article 8 *(*les données à caractère politique, philosophique (…) relatives à la santé et vie sexuelle) ou à l'article 9 (les infractions) ;

b) qui ne donnent pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents ;

[109] Décret n° 2012-1249 du 9 novembre 2012 autorisant la création de traitement de données à caractère personnel pour la mise en œuvre de programmes de prévention et d'accompagnement en santé des assurés sociaux. JORF n° 0263 du 11 novembre 2012. texte n° 1. NOR: AFSS1233684D.

c) et qui sont mis en œuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques ;

- Des traitements relatifs au recensement de la population, en métropole et dans les collectivités situées outre-mer ;
- Des traitements mis en œuvre par l'État ou les personnes morales mentionnées au I aux fins de mettre à la disposition des usagers de l'administration un ou plusieurs téléservices de l'administration électronique, si ces traitements portent sur des données parmi lesquelles figurent le numéro d'inscription des personnes au répertoire national d'identification ou tout autre identifiant des personnes physiques.

Au niveau de cette catégorie de traitements, se trouve encore une zone d'ombre quant à l'autorité administrative qui prend l'arrêté. Est-ce le ministre en charge du domaine concerné comme pour les fichiers dits de souveraineté ou est-ce une autre autorité administrative ? La loi ne donne pas de précision. Nous supposons qu'il s'agit également du ministre compétent mais sans certitude, uniquement parce que cela paraît plus probable que ce soit le ministre et non un maire ou un préfet qui autorise un traitement qui touche un répertoire national. Le législateur n'a probablement pas jugé utile de donner ce détail estimant que cela serait évident. Pourtant une précision ne serait peut-être pas de trop dans la mesure où cela permettrait d'éviter toute confusion ou toute mauvaise interprétation.

Pour cette procédure d'autorisation, la loi permet également aux responsables des traitements de bénéficier d'un acte réglementaire unique pour plusieurs traitements s'il y a des points communs quant aux finalités, aux destinataires, aux catégories de traitements, etc… Dans ce cas, le responsable de chaque traitement adresse à la Commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation. Ainsi, dans l'affaire[110] HYPERCOSMOS, la CNIL a mis en demeure, en janvier 2014 la SAS HYPERCOSMOS, entre autres, pour avoir mis en œuvre un dispositif d'accès biométriques sans utilisation de supports individuels sans remplir les formalités légales requises. La société estimait qu'en déclarant que le traitement de données à caractère personnel auprès des services de la Commission et en joignant à sa lettre une copie du récépissé de déclaration d'engagement de

[110] CNIL. Décision n° 2014-001 du 15 janvier 2014 mettant en demeure la SAS HYPERCOSMOS qui exploite l'enseigne « E.LECLERC » à Saint Médard JALLES (N°MDM 131052). http://www.cnil.fr/fileadmin/documents/approfondir/D2014-001_MED_hypercosmos.pdf. Consulté le 31 mars 2007.

conformité à la norme simplifiée n° 42 avait accompli les formalités. Mais ce fut l'occasion pour la CNIL de rappeler les modalités de mise en œuvre de la formalité d'engagement de conformité. En effet, « *la mise en œuvre d'un dispositif biométriques n'était pas couverte par la norme simplifiée n° 42, laquelle correspond à la mise en œuvre de badges sur les lieux de travail pour la gestion de contrôle d'accès aux locaux, des horaires et de la restauration* ». En outre, « *l'utilisation de tels systèmes doit faire l'objet d'une demande d'autorisation à la CNIL, conformément aux dispositions de l'article 25 I° 8 de la loi du 6 janvier 1978 modifiée ou, le cas échéant d'un engagement de conformité à l'autorisation unique n°008 relative à la mise en œuvre du dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur support, détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail* ».

Les articles 28 et 29 précisent les conditions de demande d'avis de la CNIL et la forme des actes réglementaires d'autorisation. Lorsqu'elle est saisie d'une demande d'avis, la CNIL dispose de deux mois à compter de la date de réception de la demande pour se prononcer. Ce délai peut être renouvelé une fois sur décision motivée du Président. Si la CNIL ne se prononce pas au de-là de ce délai de deux mois sa réponse est réputée favorable.

Les actes réglementaires autorisant les traitements comportent les mentions suivantes la dénomination et la finalité de traitements ; le service auprès duquel s'exerce le droit d'accès ; les catégories de données à caractère personnel enregistrées ; les destinataires ou catégories de destinataires habilités à recevoir communication desdites données et le cas échéant, les dérogations[111] à l'obligation d'information relatives aux fichiers dits de souveraineté.

Que ce soit la déclaration ou la demande d'autorisation, elles doivent comporter des mentions, portant essentiellement sur l'identité du responsable du traitement, le type de traitement, les destinataires, la durée et la ou les finalité(s) de ladite opération. L'article 30[112] de la loi informatique et libertés en donne les détails.

[111] V de l'article 32 de la loi informatique et libertés.

[112] I. - Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent :

1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre État membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;

2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions ;

3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;

En dehors des règles de forme sus-citées les traitements de données à caractère personnel respectent en commun certains principes généraux.

Section 2 : Les principes généraux encadrant le traitement automatisé des données personnelles

Ces principes sont fondés sur deux principales valeurs : certaines sont d'ordre constitutionnels (Paragraphe 1) alors que d'autres prennent leur source dans les règlements européens et la loi informatique et libertés (paragraphe 2).

Paragraphe 1 : Les principes d'ordre constitutionnel

Le traitement de données personnelles doit se faire dans le respect de certains principes de valeur constitutionnelle. Il s'agit du respect de la vie privée (A) et de la sauvegarde de l'ordre public (B).

4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5° La durée de conservation des informations traitées ;

6° Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ;

9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;

10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5.

.

A.Le respect de la vie privée

Toutes les autorités nationales et internationales en charge de la régulation des traitements automatisés des données personnelles, conscientes que l'informatique a fait de la vie privée un des problèmes majeurs de notre ère, se sont déjà penché sur la question de la vie privée à travers les textes qu'elles édictent. Le fondement du droit au respect de la vie privée émerge des droits fondamentaux[113] que sont le droit à la vie, le droit à l'inviolabilité de sa personne, droit de ne pas pouvoir publier certaines informations sur sa vie privée, mais également le droit à la liberté et le droit à la propriété. Selon l'article 3 de la déclaration universelle des droits de l'homme, « *tout individu a droit à la vie, à la liberté et à la sûreté de sa personne* ». Cependant, ni le code civil, ni aucun autre texte législatif ou réglementaire ne définit la vie privée. Le législateur français a seulement précisé à l'article 9 du code civil, *« chacun a droit au respect de sa vie privée ».*

En l'absence de définition légale, on pourrait se référer à la jurisprudence qui n'en a pas donné non plus mais est constante en la matière. Elle a entrepris d'en déterminer le contenu. La vie privée inclut l'état de santé[114], la vie sentimentale, l'image[115], la pratique religieuse, les relations familiales et, plus généralement, tout ce qui relève du comportement intime[116] d'un individu.

La doctrine qui n'en dit pas autre chose est abondante sur le sujet[117]. RIVERO, fut l'un des auteurs les plus inspirés par la problématique de la vie privée. Pour lui, « *le droit, de*

[113] MICHEL, L. *Secret médical et dossier informatisé.* Louvin médical n° 120. Belgique 2001. p. S131.

[114] CEDH 10 octobre 2006, *L.L. c. France*, [en ligne], n° 7508/02. Disponible sur : Consulté le 1 juin 2014.

[115] Cour de cassation, 1ère chambre civile, 12 juillet 2001**,** n° 98-21.337. Dalloz, n° 17, 25 avril 2002, p. 1380-1383 BIGOT, Christophe (droit à l'image), Cass. civ. 1ère, 24 Septembre 2009. *Société Jacky Boy Music c. M Salvado*r. n° 08-11.112. Bull 2009, n° 184, p. 166. JurisData: 2009-049655.

[116]Cour de Cassation Chambre civile 1, 7 février 2006, N° de pourvoi : 04-10941. http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007051655. Consulté le 31 mars 2014.

[117] « *Pour M. RAVANAS, " la vie privée est pour l'individu une sphère secrète de la vie où il a le pouvoir d'écarter les tiers ". Ce pouvoir est considéré par le consentement donné ou refusé par l'individu concerné. La vie privée était également définie par Platon comme la part de l'être humain inaccessible à autrui sans le consentement de l'intéressé. Cette idée sera reprise par le doyen CARBONNIER selon lesquels elle représente " une sphère secrète de vie d'où il « l'individu) a le pouvoir d'écarter les tiers". De son côté, l'Américain NIZER professait que le right of privacy était le droit de l'individu à une vie retirée et anonyme (1939). Enfin J. RIVERO donnera sa définition de la vie privée en la classant dans cette "sphère de chaque existence dans laquelle nul ne puisse s'immiscer sans y être convié". Cette conception, reprise par les différents auteurs cités, vise à préserver le secret la tranquillité de la personne. Cette dernière dispose alors librement de la maîtrise du secret qu'elle peut révéler à sa guise.*

longue date, reconnaît à l'individu une certaine sphère d'activité dont il est libre de refuser l'accès à autrui : c'est sa vie privée. À cette idée se rattachent, traditionnellement, la protection du domicile, qui est, par excellence, le siège de la vie privée, le secret de la correspondance et des conversations téléphoniques, le secret professionnel imposé à ceux que leurs fonctions appellent à pénétrer dans la vie privée des autres. Mais, plus récemment, la loi du 17 juillet 1970 a posé en termes généraux le principe du droit de chacun à l'intimité de sa vie privée, et a ajouté, aux protections précédentes, des protections nouvelles notamment contre les indiscrétions de presse facilitée par les techniques modernes d'espionnage à domicile : micros, photo clandestine qui portent atteinte aux droits de chacun sur son image, etc. »[118]. La vie privée est donc une notion subjective dans la mesure où même si elle est "la chose la mieux partagée, chaque individu peut en avoir une conception propre justifiée par différents facteurs, notamment sa culture. Cela peut expliquer la diversité de ses acceptions au niveau de la doctrine et la difficulté des législateurs à en donner une définition.

Même si le droit positif ne définit pas « la vie privée », il reconnaît au droit au respect de la vie privée une valeur fondamentale. En affirmant son attachement à la déclaration des droits de l'homme et du citoyen de 1789, le préambule de la Constitution française adhère à tous les droits qui y sont proclamés, notamment, les *« droits naturels et imprescriptibles de l'homme »* [119] parmi lesquels l'on compte le droit à la vie privée, une liberté. Le Conseil Constitutionnel a réaffirmé encore, dans une décision[120] datant du 10 juin 2009 que *« la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le respect de la vie privée »*.

D'autres auteurs ont préféré définir la vie privée en l'opposant à la vie publique. Ainsi pour R. Badinter, "la vie privée c'est tout ce qui n'est pas de la vie publique". Ce serait donc cette partie de la vie qui n'est pas consacrée à une activité publique où les tiers n'ont en principe pas accès, afin d'assurer à la personne le secret et la tranquillité auxquels elle a droit. M. KAYSER classe alors le droit au respect de la vie privée dans cette catégorie ayant "pour fin d'assurer la paix et la tranquillité de cette part de la vie de toute personne qui n'est pas consacrée à la vie publique. » MARLIAC. La protection des données nominatives informatiques. p. 669.

[118] RIVERO, Jean. *Les Libertés publiques*, 1991, p 33.

[119] Aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression* »

[120] Conseil Constitutionnel, *loi favorisant la diffusion et la protection de la création sur Internet*. 10 juin 2009. Décision n° 2009-580 DC. JORF du 13 juin 2009. p. 9675. Recueil, p. 107. http://www.Conseil-constitutionnel.fr/decision/2009/2009-580-dc/decision-n-2009-580-dc-du-10-juin-2009.42666.html. Consulté le 31 mars 2014.

La valeur constitutionnelle du droit au respect de la vie privée a jusque là été admise mais cela n'est pas inscrit littéralement dans la Constitution française. C'est une situation que les défenseurs des droits et libertés individuels tiennent à changer. Ainsi, à la suite du Président de la CNIL qui a manifesté en 2008[121], son désir de voir le préambule de la Constitution garantir particulièrement la protection des données personnelles, la sénatrice Anne-Marie ESCOFFIER a proposé à la ministre de la justice, Rachida DATI d'inscrire le droit au respect de la vie privée dans la Constitution. Mais la réponse[122] a été négative car, selon la Ministre, pour différentes raisons[123], la valeur constitutionnelle du droit à la vie privée n'a plus besoin d'être précisée. L'inscription de ce droit dans la Constitution aurait pu rassurer davantage les citoyens, mais il n'est plus à démontrer que le bloc de constitutionnalité semble unanime à ce sujet car même les traités internationaux reconnaissent au droit à la vie privée une valeur fondamentale. De plus, l'absence de la mention expresse du droit au respect de la vie privée dans la Constitution française est fortement compensée par une jurisprudence abondante du Conseil Constitutionnel.

---

[121] A ce propos, lors de la présentation du 28ème rapport annuel de la Commission nationale de l'informatique et des libertés (CNIL), le vendredi 16 mai 2008, son président Alex Türk a plaidé pour que le préambule de la Constitution, qui rappelle les droits fondamentaux, garantisse la protection des données personnelles. (www.lemonde.fr avec AFP, 16 Mai 2008.) Ainsi, la France pourrait conforter sa position sur ce sujet avec l'appui d'autres pays européens (13 pays) qui ont consacré dans leur loi fondamentale le droit au respect de la vie privée voire le droit à la protection des données personnelles. Il s'agit, notamment de l'Allemagne, de l'Autriche, de l'Espagne, de la Grèce, de la Hongrie, des Pays-Bas, du Portugal, de la Suède etc...

[122] Anne-Marie ESCOFFIER a soumis à la ministre de la Justice la question de l'opportunité d'inscrire le droit au respect de la vie privée dans notre Constitution, s'appuyant sur un récent rapport d'information du Sénat qui fait état de l'apparition de nouvelles "mémoires numériques" ayant pour effet principal ou incident de collecter des données permettant de suivre un individu dans l'espace et le temps. Dans sa réponse en date du 14 janvier 2010, la Ministre de la Justice rappelle les engagements internationaux auxquels la France est partie, en vertu desquels nul ne peut faire l'objet d'immixtions arbitraires dans sa vie privée. En outre, depuis 1995, le droit au respect de la vie privée est un principe à valeur constitutionnelle : le Conseil constitutionnel a consacré ce droit en considérant que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen impliquait le respect de la vie privée. Le Conseil constitutionnel donne à ce principe une acception très large, en jugeant que la législation relative à l'informatique, aux fichiers et aux libertés contient des dispositions protectrices de la liberté individuelle et que y déroger pourrait être de nature à porter atteinte à la "liberté individuelle", qui est constitutionnellement protégée. Dès lors, selon la ministre, la réaffirmation expresse, dans la Constitution, du droit au respect de la vie privée et à la protection des données personnelles serait dépourvue de portée pratique, au regard des impératifs auxquels est d'ores et déjà soumis le législateur par le double effet de la jurisprudence constitutionnelle et des traités internationaux. En revanche, il appartient au législateur d'adapter le dispositif juridique de protection des données à caractère personnel à l'évolution des technologies modernes. BRETON, Pascal. *Réponse ministérielle relative à l'inscription du droit au respect de la vie privée dans la Constitution*. http www.legalnews.fr, 18 janvier 2010. id réf. de l'article: 226777.

[123] Ces raisons sont précisées dans la réponse ministérielle. Voir note précédente: « *les engagements internationaux auxquels la France est partie, en vertu desquels nul ne peut faire l'objet d'immixtions arbitraires dans sa vie privée; depuis 1995, le droit au respect de la vie privée est un principe à valeur constitutionnelle : le Conseil constitutionnel a consacré ce droit en considérant que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen impliquait le respect de la vie privée*».

1. Le droit à la vie privée dans les traités internationaux

Le droit au respect de la vie privée est une notion moderne qui a été expressément énoncée pour la première fois dans la déclaration universelle des droits de l'homme. Il y est proclamé que « *nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation*. *Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* »[124].

Suivant la logique de la déclaration, des traités internationaux ont repris ce principe. Les premiers sont restés aussi généraux que la déclaration universelle ; c'est le cas du Pacte international relatif aux droits civils et politiques de 1966 et la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950. Mais les plus récents (surtout les conventions européennes) se sont penchés sur des sujets bien plus spécifiques, notamment celui de la vie privée dans le traitement automatisé des données personnelles. Il s'agit par exemple de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981 et la charte européenne des droits fondamentaux de 2000.

a. Les premiers traités internationaux

i. Le pacte international relatif aux droits civils et politiques du 16 novembre 1966

Le pacte international relatif aux droits civils et politiques du 16 novembre 1966[125], entré en vigueur le 23 mars 1976 et ratifié le 4 novembre 1980[126] par la France a d'abord fait

[124]Article 12 de la Déclaration universelle des droits de l'homme du 10 décembre 1948 http://www.claiming humanrights.org/udhr_article_12.html?&L=1#at13. Consulté le 31 mars 2014

[125] Par décret présidentiel en date du 9 janvier 1981, il a été décidé de la publication de ce pacte au journal officiel de la République française. Le décret n° 81-76 du 29 janvier 1981 portant publication du pacte international relatif aux droits civils et politiques ouverts à la signature à New York le 19 décembre 1966. JORF du 1er février 1981. P. 398. http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO= 19810201&numTexte=&pageDebut=00398&pageFin= . Consulté le 31 mars 2014.

allusion au droit à la vie privée en des termes bien spécifiques : « *Tous sont égaux devant les tribunaux et les cours de justice. Toute personne a droit à ce que sa cause soit entendue équitablement et publiquement par un tribunal compétent, indépendant et impartial, établi par la loi, qui décidera soit du bien-fondé de toute accusation en matière pénale dirigée contre elle, soit des contestations sur ses droits et obligations de caractère civil. Le huis clos peut être prononcé pendant la totalité ou une partie du procès soit dans l'intérêt des bonnes mœurs, de l'ordre public ou de la sécurité nationale dans une société démocratique, soit lorsque l'intérêt de la vie privée des parties en cause l'exige, soit encore dans la mesure où le tribunal l'estimera absolument nécessaire lorsqu'en raison des circonstances particulières de l'affaire la publicité nuirait aux intérêts de la justice; cependant, tout jugement rendu en matière pénale ou civile sera public, sauf si l'intérêt de mineurs exige qu'il en soit autrement ou si le procès porte sur des différends matrimoniaux ou sur la tutelle des enfants*[127] *»*. Puis, il a repris en des termes proches de ceux de la déclaration universelle des droits de l'homme le principe du droit à la vie privée : *« nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation*[128] *»*.

ii. La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950

La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950[129] qui a été ratifiée le 3 mai 1974[130] par la France quant à

---

[126] Voir la fiche retraçant l'état des signatures et ratification du pacte sur le site internet de l'ONU. https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=fr. Consulté le 31 mars 2014.
La loi n° 80-460 du 25 juin 1980 autorisant l'adhésion de la République française au pacte international relatif aux droits civils et politiques, ouvert à la signature le 19 décembre 1966 à New-York. JORF du 26 juin 1980. P.1569. Disponible sur : http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO= 19800626 &numTexte=& pageDebut=01569&pageFin=. Consulté le 31 mars 2014.

[127] Article 14.1

[128] Article 17.1 du Pacte international relatif aux droits civils et politiques du 16 novembre 1966, entré en vigueur le 23 mars 1976 et ratifié le 4 novembre 1980 par la France

[129] La convention, dans sa version de 1950 est accessible sur le lien suivant : http://www.echr.coe.int/ Documents/Collection_Convention_1950_ENG.pdf.
Sa version actuelle est accessible sur le lien suivant : http://conventions.coe.int/Treaty/FR/Treaties/Html/005.htm. ou http://www.echr.coe.int/Documents/Convention_FRA.pdf. Consulté le 31 mars 2014.

elle, dispose que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance*[131]. » Se fondant sur cette disposition, la Cour européenne des droits de l'homme a rendu de nombreux arrêts[132] confirmant ainsi l'importance de ce principe fondamental que constitue le droit à la vie privée. Toutefois, l'alinéa[133] 2 disposant : « *il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui »*, force est de constater que l'article 8 prévoit une restriction. La Cour européenne des droits de l'homme (CEDH) a attiré l'attention sur les risques de vulnérabilité des données à caractère personnel surtout avec le développement actuel de l'informatique et des technologies de l'information. Par exemple, concernant l'affaire Z c. Finlande[134] du 25 février 1997 la Cour a, dans un avis, relevé que la protection de la confidentialité des données médicales peut parfois s'effacer devant la nécessité d'enquêter sur des infractions pénales, d'en poursuivre les auteurs et de protéger l'intérêt public; ce qui ne serait pas conforme avec les garanties prévues à l'article 8.1.

Le décret portant publication de la convention au journal officiel de la république française a été pris le 3 mai 1974. Décret n° 74-360 du 3 mai 1974 portant publication de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales signée à Rome le 4 novembre 1950 et de ses protocoles additionnels. JORF du 4 mai 1974. P. 4750. http://legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19740504 &numTexte=&pageDebut=04750&pageFin=. Consulté le 31 mars 2014.

[130] La loi autorisant la ratification de cette convention a été promulguée le 31 décembre 1973. Loi n° 73-1227 du 31 décembre 1973 autorisant la ratification de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales signée à Rome le 4 novembre 1950, et de ses protocoles additionnels. JORF du 3 janvier 1974 p. 67. http://legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19740103 &num Texte=&pageDebut=00067&pageFin= Consulté le 31 mars 2014.

[131]Article 8.1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950.

[132] La vie privée comprend *l'intégrité physique et psychologique d'une* personne (X et Y c.Pays-Bas, arrêt du 26 mars 1985, série A no. 91, p. 11, § 22), y compris *le traitement médical et les examens psychiatriques* (Glass c. Royaume-Uni, no. 61827/00, §§ 70 à 72, CEDH 9 mars 2004-II ou *les informations sur les risques pour sa santé (*McGinley et Egan c. Royaume-Uni, arrêt du 9 juin 1998, Recueil des arrêts et décisions1998-III, p. 1362, § 97 ou *la réputation* (Fayed c. Royaume-Uni, arrêt du 21 septembre 1994, Série A no. 294-B, pp. 50-51, § 67 ; CEDH 29 juin 2004; Gunnarsson c. Islande décision N°. 4591/04, 20 octobre 2005)

[133]Article 8.2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950

[134] CEDH., arrêt Z. c. La Finlande du 25 février 1997, R.D.P.C, 1998, p. 311-345.

La CEDH[135] , organe juridictionnel supranational créé le 18 septembre 1959 pour veiller au respect de cette convention traite des recours portés contre un État membre du Conseil de l'Europe pour non respect des droits civiques et politiques des personnes telles qu'énoncé par la Convention. Veillant particulièrement au respect de la vie privée et familiale la CEDH a notamment rendu le 18 avril 2013 un arrêt[136] relatif à la protection des données personnelles comme un volet fondamental du droit au respect de la vie privée. Dans cette affaire, les empreintes digitales des requérants avaient été prélevées au cours de deux enquêtes pour vol. Des années plus tard, ayant demandé sans succès l'effacement de données collectées, le requérant a saisi la CEDH au motif que ce régime de conservation des empreintes constituait une violation de l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales. Confirmant la position des juges européens, la CEDH a rappelé que « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale* ». C'est pourquoi les législations nationales doivent prendre les mesures nécessaires pour veiller à ce que seules les données pertinentes et non excessives au regard des finalités du traitement soient collectées, que la durée de conservation soit strictement nécessaires pour remplir les objectifs du traitement, et que les données soient protégées efficacement contre les usages impropres et abusifs.

b. Le droit à la vie privée dans les récentes conventions européennes

i. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981[137] dite « *convention 108* » est entrée en vigueur le 1er octobre 1985 et a été ratifiée le 24 mars 1983[138] par la France. 40 États

[135] Cour européenne des droits de l'homme.

[136] CEDH, 18 avril 2013. M.K c. France, requête n° 19522/09. http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-118597. Consulté le 3 avril 2014.

[137] Cette convention est disponible sur le site du Conseil de l'Europe. http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm. Consulté le 3 avril 2014.

[138] L'approbation de la convention par la France a été faite par la loi n° 82-890 du 19 octobre *1982 autorisant l'approbation d'une convention pour la protection des personnes à l'égard du traitement automatisé des données*

européens l'ont ratifié à ce jour. Son but est expressément énoncé en son article 1er : il s'agit de « *garantir, sur le territoire de chaque partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée à l'égard du traitement automatisé des données à caractère personnel la concernant (" protection des données ")* ». Ce texte a été adopté pour renforcer les garanties de protection de la vie privée prévue à l'article 8[139] de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. « En 1968, l'Assemblée parlementaire du Conseil de l'Europe avait adressé au Comité des ministres sa recommandation 509 dans laquelle elle lui demandait de déterminer si la convention européenne des droits de l'homme et les législations internes des États membres suffisaient à protéger le droit à la vie privée face à la science et à la technologie moderne. Pour donner suite à cette recommandation, le Comité des ministres a fait entreprendre une étude dont les résultats ont révélé que les législations nationales actuelles offraient une protection insuffisante à la vie privée ainsi qu'aux autres droits et intérêts des personnes physiques vis-à-vis des banques de données automatisées. Se fondant sur cette constatation, le Comité des ministres a adopté en 1973 et 1974, deux résolutions concernant la protection des données. La première de ces résolutions, la résolution (73) 22, énonçait les principes de la protection des données pour le secteur privé, la seconde, la résolution (74) 29, a fait de même pour le secteur public. Cette résolution énumère les règles fondamentales à observer en cas d'enregistrement d'informations à caractère personnel dans les banques de données électroniques. Bien qu'elles aient laissé aux États membres toute latitude pour déterminer comment donner effet à ces règles, on constate que la quasi-totalité desdits États ont décidé ou envisagé de le faire par la

---

à caractère personnel. JORF du 20 octobre 1982. p. 3163. La publication de la Convention a été faite par décret n° 85-1203 du 19 novembre 1985 portant publication de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, fait à Strasbourg le 28 janvier 1981. JORF du 20 novembre 1985. p. 13436.
La liste de l'état des signatures est disponible sur le lien suivant: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=FRE. Consulté le 3 avril 2014.

[139] « *Toute personne doit pouvoir :*
a. connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier ;
b. obtenir à des intervalles raisonnables et sans délai ou frais excessifs la confirmation de l'existence ou non dans les fichiers automatisés, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible ;
c. obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente convention ;
d. disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article. »

voie législative. Au cours des 5 années qui ont suivi l'adoption de la seconde résolution, des lois générales sur la protection des données étaient promulguée dans 7 États membres. L'assemblée parlementaire du Conseil de l'Europe, tenant compte de ces dernières tendances, a recommandé au Comité des ministres dans sa recommandation 890 (1980), d'étudier l'opportunité d'insérer dans la Convention des droits de l'homme une disposition sur la protection des données[140] ». La Convention 108, premier instrument international juridiquement contraignant dans le domaine de la protection des données personnelles, fixe des normes minimales destinées à protéger les personnes contre les abus susceptibles de se produire lors de la collecte et du traitement de données à caractère personnel. Dans cette optique, elle proscrit le traitement des données sensibles à l'absence de garanties offertes par le droit interne et veille au droit à l'information et à la rectification des personnes concernées par un traitement sauf si les intérêts majeurs de l'État sont en jeu.

La convention 108 vise également à réglementer les flux transfrontières de données en fixant le niveau minimum de protection que les législations des États membres doivent mettre en place pour assurer le respect des droits et libertés fondamentales et notamment le droit à la vie privée[141]. Ils sont autorisés à adopter des règles de protection de plafond plus élevé et à s'en prévaloir contre le libre flux transfrontières de données. Les États parties ne sont pas obligés de maintenir un niveau équivalent de protection mais sont tenus de respecter un standard minimum élevé et à équivalence de protection, la libre circulation des informations. En

[140] Rapport explicatif de la convention. http://conventions.coe.int/treaty/fr/Reports/Html/108.htm. Consulté le 9 avril 2014.

[141] Article 12 de la convention issue de la proposition de modernisation adoptée par la 29ème réunion plénière du 27 au 30 novembre 2012 :
« *1. Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale le transfert de données à un destinataire relevant de la juridiction d'une autre Partie à la convention, à moins que la partie visée au début du présent paragraphe ne soit régie par des règles de protection harmonisées contraignantes et communes à des États appartenant à une organisation internationale régionale et que le transfert de données ne soit encadré par des mesures visées au paragraphe3.b.*
2. Lorsque le destinataire relève de la juridiction d'un État ou d'une organisation internationale qui n'est pas partie à la Convention, le transfert de données n'est possible que si un niveau approprié de protection des données à caractère personnel basé sur le principe de la présente convention est assuré.
3. Un niveau de protection des données approprié peut être assuré par :
a) Les règles de droit de cet État ou de cette organisation internationale, y compris les traités ou accords internationaux applicables, ou
b) Des garanties ad hoc ou standardisées agréées établies par des instruments juridiquement contraignants et opposables, conclus et mis en œuvre par les personnes impliquées dans le transfert et le traitement ultérieur des données ». Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Strasbourg, le 18 décembre 2012. Http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_F_Convention%20108%20modernisée%20version%20F.pdf. Consulté le 7 avril 2014.

général, l'équivalence de protection est présumée par la ratification de la convention, mais il revient à chaque État d'en apprécier le niveau en fonction de son droit interne. Au plan européen, une évaluation a été mise en place dans le cadre de l'appréciation du niveau adéquat des pays tiers conformément à l'article 25 de la directive 95/46. Des pays comme la Hongrie, la Suisse ont déjà été reconnus comme assurant un niveau de protection adéquat par l'Union européenne.

ii. La Charte européenne des droits fondamentaux du 7 décembre 2000

La Charte européenne des droits fondamentaux du 7 décembre 2000[142] tient sa valeur contraignante[143] du Traité de Lisbonne[144]dont la loi n° 2008-125 du 13 février 2008[145] a autorisé la ratification. En 1950, la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales énonçait déjà le droit au respect de la vie privée et familiale et au respect de son domicile et de sa correspondance. Mais, ce n'est qu'avec l'entrée en vigueur, fin 2009 du traité de Lisbonne que la charte des droits fondamentaux de l'Union a consacré ce droit au respect de la vie privée en la modernisant. En plus d'être un droit fondamental, la vie privée est aussi intégrée comme un élément majeur du traité de fonctionnement[146] de l'Union européenne. « *C'est donc un deuxième enjeu tout à fait important pour l'Europe : celui de pouvoir garantir un traitement de données qui respecte la vie privée, et d'empêcher les utilisations abusives d'où qu'elles viennent, que ce soit du*

[142] Charte européenne des droits fondamentaux. 18 décembre 2000.[en ligne] JOCE C 364/1. Disponible sur: http://www.europarl. europa.eu/charter/pdf/text_fr.pdf. Consulté le 3 avril 2014.

[143] Article 6 du traité de Lisbonne : « 1. L*'Union reconnaît les droits, les libertés et les principes énoncés dans la charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, tel qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités*. »

[144] Le traité de Lisbonne est un traité signé le 13 décembre 2007 à Lisbonne entre les 27 États membres de l'Union européenne, qui tend à transformer l'architecture institutionnelle de l'Union. JOUE C 306 du 17 décembre 2007.

[145] Loi n° 2008-125 du 13 février 2008 autorisant la ratification du traité de Lisbonne modifiant le traité sur l'Union européenne, le traité instituant la communauté européenne et certains actes connexes. JORF n° 0038 du 14 février 2008. p. 2712 texte n°1. NOR : MAEX0802893L.

[146] Le TEFU ou traité de fonctionnement de l'Union européenne est, depuis l'entrée en vigueur du traité de Lisbonne, le nouveau nom du traité de Rome (ou traité instituant la communauté européenne) actualisé. La protection des données personnelles y figure à l'article 16.

pouvoir politique, des techniques commerciales abusives, des harcèlements sur la vie privée ou enfin des tentatives de fraude[147] ».

Le respect de la vie privée et la protection des données personnelles sont étroitement liées, mais sont traités comme des droits fondamentaux distincts par les articles 7 et 8 de la Charte. L'article 7 de la Charte dispose que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* ». S'agissant spécialement de la protection des données personnelles, son article 8 stipule que : « *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* ». Par ces dispositions, ce texte, quoi qu'européen, semble s'être inspiré de la loi informatique et libertés du 6 janvier 1978 en ce qui concerne les conditions de licéité du traitement automatisé des données personnelles. De manière synthétisée, cet article 8 reprendre le contenu des articles 6 et 7 de la loi informatique et libertés.

En application de ces traités internationaux[148], le Conseil Constitutionnel a rendu plusieurs décisions où il s'est attelé à veiller au mieux au respect de la vie privée.

2. Le droit à la vie privée dans la jurisprudence du Conseil Constitutionnel

La jurisprudence du Conseil Constitutionnel en matière de traitement des données à caractère personnel laisse au législateur une grande liberté d'appréciation tout en protégeant les libertés individuelles. La valeur constitutionnelle du droit à la vie privée n'a été reconnue pour la première fois qu'en 1995 par une décision[149] du Conseil Constitutionnel alors qu'il

[147] FELCOURT. *L'usurpation d'identité*. p. 180.

[148] Voir également le traité d'Amsterdam de l'Union Européenne (art. 213 B) qui édicte qu'à partir de 1999, toutes les institutions communautaires issues du Traité seront tenues d'appliquer les règles protectrices des données personnelles et de créer une autorité autonome de surveillance.

[149] Conseil constitutionnel décision n° 94-352 DC, 18 janvier 1995. JORF du 21 janvier 1995.

n'avait jusque-là qu'une valeur législative. Ensuite, dans une décision[150] de Juillet 1999, il a précisé que la vie privée découle de l'article 2 de la Déclaration des droits de l'homme et du citoyen aux termes duquel : « *le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression* ». Cette position a d'ailleurs été plusieurs fois reprise dans d'autres décisions[151] depuis lors. Le Conseil Constitutionnel a fait remarquer que l' échange et leur partage des données personnelles entre organismes publics ne pourront se faire sans le consentement des intéressés qu'à une double condition: Premièrement, il faut que ce soit fait dans un but d'intérêt général, en particulier lié à des exigences constitutionnelles (protection de la santé, lutte contre la fraude fiscale, sauvegarde de l'ordre public, équilibre financier de la sécurité sociale…). Deuxièmement, le dispositif prévu doit être assorti de limitations et précautions propres à concilier la poursuite de ce but et le droit au respect de la vie privée des personnes concernées[152].

Suivant la même logique, dans une décision n° 2004-499 DC du 29 juillet 2004 le Conseil Constitutionnel a encore censuré une disposition visant à permettre aux personnes morales victimes d'infractions ou agissant pour le compte desdites victimes de mettre en place des traitements de données à caractère personnel relatives à des infractions ou condamnations pour les besoins de la prévention et de la lutte contre la fraude. Il a notamment prononcé cette censure au motif que la loi laissait sans réponses plusieurs questions essentielles : celle de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées et celle de savoir si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles

[150]Décision n° 99-416 DC du 23 juillet 1999, (cons 45), journal officiel du 28 juillet 1999. Considérant qu'aux termes de l'article 2 de la Déclaration des droits de l'homme et du citoyen : *« Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression ; que la liberté proclamée par cet article implique le respect de la vie privée » ;*

[151] Conseil constitutionnel, décision n° 99-419 DC, 9 novembre 1999. JORF du 16 novembre 1999. Décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, JORF du 13 mars 2003, p. 4789 ; décision n° 2004-492 DC du 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, JORF du 10 mars 2004, p. 4637 ; ou encore décision n° 2005-532 du 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, JORF du 24 janvier 2006, p. 1138.

[152] Décisions n° 93-325 DC du 13 août 1993 (cons. 121), JORF du 18 août 1993, p. 11722; Décision n° 98-405 DC du 29 décembre 1998 (cons. 60), JORF du 31 décembre 1998, p. 20138; n° 99-416 DC du 23 juillet 1999 (cons. 46 et 47), JORF du 28 juillet 1999, p. 11250; Décision n°2003-484 DC du 20 novembre 2003 (cons. 20 à 23), JORF du 27 novembre 2003, p. 20154 ; n° 2004-504 DC du 12 août 2004 (cons. 5, 7 et 8), JORF du 17 août 2004, p. 14657; Décision n° 2005-532 DC du 19 janvier 2006 (cons. 10 et 18 à 21), JORF du 24 janvier 2006, p. 1138, et, dernièrement, Décision n° 2007-553 DC du 3 mars 2007, JORF du 7 mars 2007, p. 4356.

soient capables de commettre une infraction. En outre, la loi était silencieuse sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations[153]

La décision[154] du Conseil Constitutionnel relative à la loi HADOPI vient confirmer sa constance en matière de défense de la vie privée. En effet, le texte offrait à la haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) l'accès à des données sur les connexions des internautes. Elle serait donc amenée à collecter, à stocker et à utiliser des données personnelles sur pratiquement toute la population française. Son pouvoir l'autorisait même à prononcer certaines sanctions allant jusqu'à la coupure de l'accès à Internet. Le Conseil n'a donc pas manqué de préciser que ce dernier pouvoir ne peut incomber qu'au juge et non à une autorité administrative, en l'occurrence l'HADOPI. Celle-ci n'agit que « *dans l'intérêt d'une bonne administration de la justice* », afin de « *limiter le nombre d'infractions dont l'autorité judiciaire sera saisie*[155] ». Ce rôle détermine également, de façon étroite la finalité du traitement des données qu'elle collecte d'autant plus qu'*« il appartiendra à la Commission nationale de l'informatique et des libertés, saisie pour autoriser de tels traitements, de s'assurer que les modalités de leur mise en œuvre, notamment les conditions de conservation des données, seront strictement proportionnées à cette finalité*[156] ».

Finalement, il ne faut pas ignorer que même si le Conseil Constitutionnel défend régulièrement le droit à la vie privée, il reste toujours fidèle à la mission pour laquelle il a été créé par la Constitution du 4 Octobre 1958 : contrôler la conciliation faite par le législateur entre les libertés et l'ordre public. C'est pourquoi il veillera à ce que le traitement automatisé des données personnelles se fasse dans le sens de la sauvegarde de l'ordre public.

[153] Décision n° 2004-499 DC du 29 juillet 2004, *Loi 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.14087

[154] Décision n° 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur internet (*Cons 27 et 30)

[155] Considérant 28 de la décision n° 2009-580 DC du 10 juin 2009

[156] Considérant 29 de la décision n° 2009-580 DC du 10 juin 2009

B. La sauvegarde de l'ordre public

L'ordre public apparemment simple est une notion dont la définition n'est pas aisée à trouver. Philippe MALAURIE, auteur d'une vingtaine de définitions de l'ordre public écrivait, à juste titre : « *définir l'ordre public, c'est s'aventurer sur des sables mouvants*[157] » ; pour montrer la difficulté d'un tel exercice. On ne peut valablement garantir la sécurité des titulaires des données à caractère personnel que si l'ordre public est préservé.

1. La notion d'ordre public

L'ordre public n'a pas été défini par les textes de loi. Il n'est expressément cité que dans l'article 11 de la Déclaration de 1789 qui dispose que «*Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi*».

Pour avoir une approche de sa définition, il faut se référer à la jurisprudence du Conseil Constitutionnel. En effet, la lecture de ses décisions permet de déduire que l'ordre public recouvre les notions de « *bon ordre, sécurité, salubrité et tranquillité publique*[158] ». Il est proche de « l'intérêt général », présente un fort lien de parenté avec celui-ci mais en est différent. L'intérêt général est entendu comme « *la satisfaction de l'intérêt de la communauté des citoyens dans son ensemble*[159] » (définition débattue depuis deux siècles sans achèvement définitif). L'ordre public est un corollaire de l'intérêt général et constitue la garantie de la sécurité des personnes et des biens. Pour la jurisprudence du Conseil c'est le bouclier de certaines des plus fondamentales de nos libertés : « *la prévention des atteintes à l'ordre public est nécessaire à la sauvegarde de droits de valeur constitutionnelle*[160] ». Le Conseil a donc

[157] MALAURIE, Philippe. *Les contrats contraires à l'ordre public*. Paris 1953. T.1. p.69

[158] Conseil constitutionnel dans la décision n° 2003-467 DC du 13 mars 2003 (cons 2), loi pour la sécurité intérieure en rappelle cette disposition de l'article L 2212-2 du Code Général des Collectivités Territoriales (CGCT) pour l'entériner.

[159] BOUCHARD, Marie, Gilles L. Bourque, Benoît Lévesque, avec la collaboration d'Élise Desjardins *L'évaluation de l'économie sociale dans la perspective des nouvelles formes de régulation socio-économique de l'intérêt général.* p.11. https://depot.erudit.org/id/001694dd. Consulté le 20 juillet 2013.

[160] Décision n° 80-127 DC du 20 janvier 1981, cons. 58 et 62 ; n° 2008-562 DC du 21 février 2008, cons. 13.

donné un statut juridique à cette notion traditionnelle d'ordre public en faisant de sa sauvegarde un objectif de valeur constitutionnelle c'est-à-dire un impératif lié à la vie en société qui doit guider l'action normative[161].

2. La sauvegarde de l'ordre public et les données personnelles

Les données personnelles constituent un aspect de la vie privée de l'individu ; laquelle fait aussi partie des libertés énoncées par l'article 2 de la Déclaration des droits de l'homme de 1789 selon la jurisprudence de Conseil Constitutionnel. Or, le même Conseil considère l'ordre public comme le bouclier des plus fondamentales des libertés. Partant, on pourrait peut-être prétendre que de même qu'en préservant la vie privée on protège les données personnelles, en sauvegardant l'ordre public, on préserve aussi les données personnelles.

Si certaines lois établissent une conciliation *«qui n'est pas manifestement déséquilibrée entre le droit à une vie familiale normale, le respect de la vie privée de l'enfant et du père et la sauvegarde de l'ordre public*[162]*»*, paradoxalement, au nom de l'ordre public, il peut aussi arriver que les données personnelles soient exposées à de graves atteintes. Ainsi, dans la décision du Conseil Constitutionnel du 13 mars 2003, précitée le gardien de la Constitution devait se prononcer sur une requête concernant les articles 21 et 25 de la loi sur la sécurité intérieure quant aux traitements automatisés de données nominatives utilisées par les services de la police nationale et de la gendarmerie nationale dans le cadre de leurs missions. Les députés et les sénateurs requérants soutenaient que ces dispositions portaient atteinte au respect de la vie privée. En renvoyant au pouvoir réglementaire le soin de fixer certaines caractéristiques desdits traitements, en particulier la durée de conservation des données, le législateur n'avait pas épuisé sa compétence ; certaines utilisations étaient sans lien avec la finalité des traitements. En particulier, en permettant la consultation des données nominatives à des fins d'enquête administrative, le législateur permettrait qu'il en soit fait un usage préjudiciable aux intérêts légitimes des personnes concernées et contraire au droit à une vie

[161] *Libertés et ordre public* « *Les principaux critères de limitation des droits de l'homme dans la pratique de la justice constitutionnelle* » 8ème séminaire des cours constitutionnelles tenu à Erevan du 2 au 5 octobre 2003 www.Conseil-constitutionnel.fr/Conseil-constitutionnel/root/bank_mm/pdf/Conseil/libpub.pdf. 20 juillet 2013.

[162] Conseil constitutionnel n° 2007- 557 DC du 15 novembre 2007 - Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile (cons 11). JORF du 21 novembre 2007, p. 19001. Recueil, p. 360.

familiale normale. Mais le Conseil n'a pas jugé inconstitutionnelles de telles dispositions car « *la consultation est (...) permise pour l'exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public*[163] *...».* Le traitement automatisé des données personnelles dans un but d'intérêt général permet à maints égards, de renforcer l'efficacité de l'action publique au bénéfice des administrés. C'est une grande adaptabilité du service public aux attentes des citoyens qui est assuré garantissant la continuité du service, la simplification des procédures. La dématérialisation des procédures peut contribuer à réduire les facteurs de vulnérabilité à la délinquance[164]. L'anticipation permise par ce type de traitement a fait craindre à la Ligue des droits de l'homme une atteinte au droit à la vie privée et à la présomption d'innocence de certains citoyens qui seraient fichés dans le cadre de l'application du décret[165] du 4 mai 2012 relatif au traitements d'antécédents judiciaires[166]. Ce décret autorise les services de la police et de la gendarmerie nationale à collecter et conserver dans un fichier informatique dénommé « *TAJ*[167]» des données personnelles relatives aux personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer à la Commission de certains crimes, délits ou contraventions de 5ème classe ainsi qu'aux victimes de ces infractions et à certaines personnes concernées par des enquêtes ou instructions. Mais, le Conseil d'État saisi par la Ligue des droits de l'homme en recours contre ce règlement en avril 2014, a rejeté le recours en estimant que les traitements sont adéquats, pertinents et non excessifs par rapport aux finalités légitimes poursuivies. L'objectif poursuivi par ce fichier est de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs.

---

[163] Conseil constitutionnel dans la décision n° 2003-467 DC du 13 mars 2003 Cons 31.

[164] BRAIBANT, Guy. Rapport. *Données personnelles et sociétés de l'information. Rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46*. 3 mars 1998. p. 4-5. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/984000836/0000.pdf. Consulté le 25 avril 2014.

[165] Décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires. JORF n° 0107 du 6 mai 2012, p. 8047. NOR : IOCD1125123D.

[166] Ce décret est pris en application de l'article 11 de la loi n° 2011-267 du 14 mars 2011 d'orientation de programmation pour la performance de la sécurité intérieure. JORF n° 0062 du 15 mars 2011. p. 4582. NOR : IOCX0903274L.

[167] Traitement des antécédents judiciaires. Ce fichier remplace les fichiers STIC de la police nationale et le JUDEX de la gendarmerie nationale le 31 décembre 2013. Communiqué de presse du Conseil d'État du 11 avril 2014. http://www.Conseil-État.fr/fr/communiques-de-presse/fichiers-informatiques.html. Consulté le 25 avril 2014.

« *L'enregistrement de données nominatives dans le TAJ ne porte, par lui-même, aucune atteinte au principe de la présomption d'innocence garanti par ces stipulations ; qu'en outre, les données personnelles concernant les personnes mises en cause, en cas de décision de relaxe ou d'acquittement devenue définitive, sont en principe effacées et ne peuvent être maintenues dans le fichier par décision du procureur de la République que pour des raisons liées à la finalité du TAJ et pour des nécessités d'ordre public, mention de la relaxe ou de l'acquittement étant faite dans le fichier ; qu'enfin, les données personnelles concernant les personnes mises en cause, en cas de décision de non-lieu ou de classement sans suite, qui sont en principe conservées, peuvent être effacées du fichier sur décision du procureur de la République, s'il estime que les nécessités de l'ordre public n'y font pas obstacle*[168] ».

Les données personnelles et l'ordre public entretiennent un rapport bien particulier. Au-delà des données, c'est le droit à la vie privée qui est concerné. Il est mis au second plan dès qu'il faut sauvegarder l'ordre public alors même que c'est un principe de valeur Constitutionnelle confirmée. Ce qui n'empêche pas le législateur de prévoir des principes non constitutionnels à respecter pour que le traitement des données personnelles soit licite.

Paragraphe 2 : Les principes issus des règlements européens et de la loi informatique et libertés

La Convention n° 108 du 28 janvier 1981[169] du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et la 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 sont à l'origine de l'énoncé des principes fondamentaux que doit respecter la mise en œuvre

[168] Conseil d'État. 11 avril 2014. Ligue des droits de l'homme. Décision n° 360759. http://www.Conseil-État.fr/fr/selection-de-decisions-du-Conseil-d-État/ce-11-avril-2014-ligue-des-droits-de-l-homme-.html. Consulté le 30 mai 2014.

[169]Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Strasbourg, 28 janvier 1981, N° de série des traités européens : 108.

de traitements informatisés. Ceux-ci ont été repris[170] dans la loi du 6 janvier 1978[171] relative à l'informatique, aux fichiers et aux libertés – loi modifiée par la loi du 6 août 2004[172]– pour tenir compte des nouvelles dispositions de la directive de 1995[173].

La directive du 24 Octobre 1995[174] précise que les principes de protection doivent être vus sous deux angles (ce qui se retrouve aussi dans la Convention 108 mais présenté différemment) : d'une part, ceux relatifs aux obligations mises à la charge des personnes qui traitent les données et d'autre part ceux qui se réfèrent aux droits reconnus aux personnes dont les données font l'objet d'un traitement.

A. Les principes liés aux obligations du responsable du traitement

Au regard des articles 5 de la Convention 108, 6 de la directive de 1995 et l'article 6 de la loi informatique et libertés les obligations peuvent se résumer dans les principes suivants : la loyauté et la transparence, la finalité, et la confidentialité, sous l'œil bienveillant de la CNIL (Commission Nationale de l'Informatique et des Libertés), autorité administrative mise en place par la loi informatique et libertés pour veiller au respect desdits principes.

[170]En réalité, la loi du 6 janvier 1978 a plutôt inspiré la Convention et la Directive européennes car elle est plus ancienne mais elle a dû faire une certaine mise à jour en 2004 pour respecter la hiérarchie des normes.

[171]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 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 NOR: JUSX0100026L

[172] 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 NOR: JUSX0100026L

[173] 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. JOCE n° L 281 du 23/11/1995 p. 0031 – 0050

[174] Considérant 25 de la Directive: «C*onsidérant que les principes de la protection doivent trouver leur expression, d'une part, dans les obligations mises à la charge des personnes, autorités publiques, entreprises, agences ou autres organismes qui traitent des données, ces obligations concernant en particulier la qualité des données, la sécurité technique, la notification à l'autorité de contrôle, les circonstances dans lesquelles le traitement peut être effectué, et, d'autre part, dans les droits donnés aux personnes dont les données font l'objet d'un traitement d'être informées sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voire de s'opposer au traitement dans certaines circonstances;* » http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML Consulté le 30 mai 2014.

1. Le principe de loyauté et de transparence

L'article 6, 1° de la loi informatique et libertés dispose : « *Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :1° Les données sont collectées et traitées de manière loyale et licite ; ».*

La loyauté du traitement suppose que les données personnelles ne soient pas obtenues ou traitées à l'aide de moyens illicites ou déloyaux. Les données ne doivent pas être collectées et traitées à l'insu de la personne concernée et celle-ci doit avoir connaissance de l'identité et du lieu d'établissement de la personne qui traite ses données, des finalités poursuivies, du caractère obligatoire ou facultatif de l'opération, des destinataires des informations, ainsi que toute information nécessaire à l'exercice de ses droits. Les informations obtenues de manière loyale sont celles qui ont fait l'objet d'une information préalable de la personne concernée lui donnant ainsi la possibilité de s'opposer à leur utilisation conformément à l'article 38 de la loi informatique et libertés. Le manquement à ces obligations constitue un délit[175] puni par la loi. C'est aussi le cas lorsqu'on collecte des informations par un moyen frauduleux déloyal ou illicite, ou qu'on procède à un traitement automatisé d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des raisons légitimes[176]. Est considéré comme constitutif d'une collecte déloyale, par la pratique du spamming, le fait de procéder à la collecte d'adresses de courrier électronique dans les espaces publics de l'Internet - espaces de discussion, listes de diffusion, annuaires, sites Web - sans que les personnes concernées ou le responsable du site diffusant les données n'en aient eu connaissance[177]. Ainsi, dans l'affaire Fabrice H. / Ministère public[178] du 14 mars 2006 la Cour de cassation a condamné Fabrice X, au versement de 3000 euros d'amende. Ce dernier "aspirait" sur internet, sans leur consentement, des adresses

[175]Article 226-18 du code pénal : *« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.* Les articles 226-18 à 226-20 traitent tous d'infractions connexes.

[176] Cour de cassation, chambre criminelle, 28 septembre 2004 : Condamnation pour délit de traitement de données nominatives malgré opposition en vertu de l'article 226-18 du Code Pénal. Des personnes ayant fait opposition par l'intermédiaire de la CNIL, de leur droit d'opposition à être maintenues dans les fichiers de l'ASESIF (église de scientologie) ont néanmoins continué à recevoir des courriers postérieurement.

[177] ROQUES-BONNET, Marie-Charlotte. *Le droit peut-il ignorer la révolution numérique ?* p. 223.

[178] Cour de cassation, chambre criminelle, 14 mars 2006, Fabrice H. / Ministère public,

électroniques de personnes physiques en vue de la diffusion de messages publicitaires aux titulaires de ces adresses. Il commettait ainsi une collecte déloyale de données nominatives au sens de l'article 226-18 du Code Pénal.

La loyauté exige également que les informations soient exactes ou complètes car dans le cas contraire, elles peuvent nuire à la personne à laquelle elles se rapportent. Il faut donc que le responsable du traitement prenne toutes dispositions utiles pour s'assurer que les données traitées sont correctes et actuelles. Sinon, elles doivent être rectifiées ou, carrément effacées[179]. Cette version de la loi qui reprend pratiquement la directive de 1995 (article 6, d[180]) à l'exception de l'adjectif « raisonnables » a le mérite de corriger des imperfections qui avaient été reprochées à cet article de la directive. En effet, le terme « *raisonnables* » s'apprécie comme une subjectivité qui risque de permettre à beaucoup de responsables de traitement de ne pas faire d'effort pour mettre à jour leurs fichiers. Cependant, cette amélioration est affaiblie par le ton souple de l'article 6 de la loi du 6 janvier 1978 modifiée qui reprend, en substance, l'exigence de licéité de traitement qu'émettait l'article 37 de sa version initiale. L'ancien article 37[181] de la loi informatique et libertés comportait un ton plus contraignant dans ce domaine vis-à-vis des responsables de traitement. L'article 6 de la loi modifiée reprend ces conditions de licéité des traitements de données à caractère personnel en son point 4°[182] dans des termes qui paraissent généraux et impersonnels. La lettre de l'ancienne loi offrait moins d'alternative aux responsables de traitements. L'article 37 employait le verbe « devoir » (*doit être*) et les adverbes « *même d'office* » qui véhiculent une idée d'urgence alors que l'article 6 utilise l'expression « *si nécessaire* » ; ce qui a pour effet d'exercer moins de pression sur les responsables du traitement. Fort heureusement, la régulation exercée par la CNIL pallie à certaines des insuffisances de la loi. Ainsi, un contrôle

[179] Article 6, 4° de la loi informatique et libertés : « Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ».

[180] *« [les données doivent être] exactes et si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes [...] soient effacées ou corrigées ».*

[181] *« Un fichier nominatif doit être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information nominative contenue dans ce fichier. »*

[182] « *Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées* ».

du fonctionnement du STIC[183] (Système de traitement des infractions constatées), a permis à la Commission de relever que les mises à jour des fichiers n'étaient pas régulières ; ce qui pouvait « *entraîner des conséquences désastreuses en termes d'emploi pour les citoyens*[184] ». A l'issue de ses investigations, l'autorité de régulation a formulé 11 propositions visant « *à rappeler les exigences de la loi et à les faire respecter par les différents acteurs concernés*. » Les 3 dernières insistaient sur les dispositions à prendre pour assurer la mise à jour des fichiers, salutaires pour les citoyens concernés.

La transparence des traitements doit être assurée d'une part, par l'information, de manière loyale, des personnes concernées sur la finalité poursuivie par la collecte de données. Elles doivent savoir qui sont les destinataires de leurs données et le lieu où s'exerce le droit d'accès et de rectification. De même, elles doivent être informées du caractère facultatif ou obligatoire des informations demandées ainsi que des conséquences éventuelles d'un défaut de réponse. D'autre part, le responsable du traitement doit procéder à la déclaration des traitements avant leur mise en œuvre à l'autorité de contrôle (la CNIL) qui en assure la publicité. L'enregistrement des bases de données auprès de la Commission nationale contribue à la transparence. Elles constituent un registre public des traitements de données personnelles consultable sur le site Internet[185] de la CNIL. Ainsi, le 4 Avril 2006[186], le TGI de Paris avait suspendu l'application d'un dispositif d'écoute téléphonique de France Telecom mis en place pour permettre aux managers d'écouter les conversations téléphoniques des salariés avec les clients et d'établir une grille d'écoute influant sur la rémunération des

[183]Ce fichier répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées. Il facilite la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il permet également d'élaborer des statistiques.
Depuis la loi du 15 novembre 2001 pour la sécurité quotidienne, le STIC peut être consulté dans le cadre des enquêtes administratives devant précéder les décisions d'habilitation des personnes en ce qui concerne l'exercice de missions de sécurité et de défense, les autorisations d'accès à des zones protégées en raison de l'activité qui s'y exerce et les autorisations concernant les matériels ou produits présentant un caractère dangereux. www.cnil.fr. Consulté le 2 avril 2014.

[184] CNIL. *Conclusions du contrôle du système de traitement des infractions constatées (STIC)*. Rapport remis au Premier ministre le 20 janvier 2009. p. 29 . http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Controles_Sanctions/Conclusions%20des%20controles%20STIC%20CNIL%202009.pdf. Consulté le 3 avril 2014.

[185] http://www.cnpd.lu/fr/registre/index.html. Consulté le 3 avril 2014.

[186] TGI Paris, 1ère chambre 4 avril 2006 Syndicat Sud Télécom Paris c/ S.A. France Télécom, Monsieur Patrick C. et Monsieur Bertrand G. N° RG : 05/18400.

salariés. La raison en était que celui-ci n'avait pas été déclaré par France Télécom avant sa mise en œuvre.

2. Le principe de la finalité

Par finalité d'un traitement on entend le « pourquoi » dudit traitement, l'objectif poursuivi en recueillant les données, l'usage que l'on entend faire des données recueillies. Les données personnelles doivent être collectées dans un but précis. Ce principe garantit les libertés individuelles contre l'arbitraire.

La finalité des traitements que l'on compte effectuer est à préciser lors de la déclaration ou de la demande d'avis présentée à la CNIL ; c'est une condition essentielle pour la recevabilité d'une requête. Seul cet objectif détermine les données à recueillir. Ainsi, une information qui n'est pas nécessaire à l'objectif poursuivi ne doit-elle pas intervenir dans la collecte et le traitement. Le responsable du traitement est également tenu d'informer la personne concernée de la finalité et celle-ci doit être respectée tout au long du traitement.

Toute modification ultérieure à la déclaration est constitutive d'un détournement de finalité, un délit pénal passible d'une peine de cinq ans d'emprisonnement et d'une amende de 300000 euros (art. 226-21 du Code pénal[187]). Ainsi, dans l'affaire Sonacotra / Syndicat Sud Sonacotra[188] du 25 avril 2003, alors que la société Sonacotra avait établi un annuaire d'adresses électroniques de ses salariés, non diffusé à l'extérieur en déclarant à la CNIL qu'il servirait à l'utilisation par les seuls salariés entre eux ou avec des correspondants choisis par eux. Mais le syndicat Sud Sonacotra s'était servi de cet annuaire pour effectuer des envois massifs de mails. Le Tribunal de grande instance de Paris, jugeant que l'annuaire d'adresses électroniques des employés d'une entreprise, destinés à des échanges entre collaborateurs, ne

[187] *« Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. »* Depuis le 8 juillet 2004 cet article a été modifié par la loi n°2004-801 du 6 août 2004 - art. 14 du JORF du 7 août 2004

[188] TGI de Paris, 3ème chambre, 2ème section N° RG: 02/02978, 25 avril 2003, Sonacotra / Syndicat Sud Sonacotra

peut être utilisé à des fins de diffusion de tracts syndicaux, avait condamné le syndicat à 2000 euros de dommages et intérêts pour détournement de la finalité du traitement déclaré. Mais l'article 6, 2[189] de la loi informatique et libertés permet une modification ultérieure à des fins statistiques, de recherche scientifique ou historique à condition que le traitement présente des garanties particulières consistant notamment, en la notification à la personne concernée, au respect des obligations préalables à la charge du responsable, etc...

En dehors des entreprises privées et des particuliers susceptibles de porter une atteinte à ce principe de finalité, l'administration publique est potentiellement tentée de détourner la finalité du traitement des données personnelles. La raison en est que dans le cadre de l'établissement d'actes état civil, notamment les passeports biométriques, des données biométriques morphologiques de la population sont collectées et traitées. Mais, par exemple en cas d'infraction, la police pourrait recourir aux bases de données ainsi constituées dans le cadre d'enquêtes de police judiciaire. Il y aurait là un détournement de la finalité prescrite par le règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004[190] établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres. A ce sujet, la doctrine ne manque pas de tirer la sonnette d'alarme. Le Professeur GUGLIELMI, attire l'attention sur ces risques dans son article[191] : Le passeport n'est plus électronique mais biométrique.

Un autre aspect de la finalité exige que les données soient « *non excessives* » au regard du but poursuivi. On parle alors de proportionnalité. Le droit positif impose − pour que le traitement soit proportionnel − que les données soient « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements*

[189]Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées.
Les « considérant 28 et 29 » de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 laissent la charge à chaque État signataire de fixer les garanties appropriées.

[190]« *Aux fins du présent règlement, les éléments biométriques des passeports et des documents de voyage ne sont utilisés que pour vérifier : a) l'authenticité du document ; b) l'identité du titulaire grâce à des éléments comparables directement disponibles lorsque la loi exige la production du passeport ou d'autres documents de voyage »*

[191]GUGLIELMI, Gilles J: *Le passeport français n'est plus électronique mais biométrique*. [en ligne], disponible sur: http://www.guglielmi.fr/spip.php?article131. Consulté le 27 mars 2014.

ultérieurs». Pour cela, la CNIL vérifie la proportionnalité entre les moyens technologiques mis en œuvre et l'objectif poursuivi. Les moyens utilisés doivent, en effet, être indispensables, nécessaires, voire incontournables pour atteindre l'objectif poursuivi. C'est pourquoi, dans deux délibérations rendues le même jour et ayant le même enjeu, la CNIL a eu à prendre des décisions diamétralement opposées.

S'agissant de la première[192], la CNIL a été saisie par l'établissement public Aéroports de Paris d'une demande d'avis concernant la mise en œuvre de traitements automatisés d'informations nominatives permettant un contrôle des accès aux zones réservées des aéroports d'Orly et de Roissy. Elle a donné un avis favorable car, pour elle, « *le dispositif présenté par Aéroports de Paris est adapté et proportionné à la finalité qui lui est assignée.* » C'est-à-dire que ce contrôle allait au-delà des intérêts du seul établissement, c'est une question de sécurité nationale qui nécessite donc que l'on emploie les meilleurs moyens.

Quant à la seconde délibération[193], elle a rendu une décision défavorable. En l'espèce, la demande d'avis était présentée par le Centre hospitalier d'Hyères pour la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels. La décision se justifie par le fait que, pour la Commission « *l'objectif d'une meilleure gestion des temps de travail, s'il est légitime, ne paraît pas de nature à justifier l'enregistrement dans un lecteur biométrique des empreintes digitales des personnels du Centre hospitalier. Aussi le traitement pris dans son ensemble n'apparaît-il ni adapté ni proportionné à l'objectif poursuivi.* »

Finalement, pour garantir la protection de la vie privée, la pertinence d'une donnée s'apprécie en fonction du contexte. Elle n'est pas prédéfinie ou décrétée pour un type précis de traitement. Doivent entrer en ligne de compte les motifs et l'opportunité du traitement. Le professeur TRUDEL affirmait : « *il importe de revenir aux fondements véritables du principe*

---

[192] Délibération n°04-017 du 8 avril 2004 08 Avril 2004 - relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en œuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy.

[193]Délibération n°04-018 du 8 avril 2004 relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels.
Voir aussi : Tribunal de Grande Instance de Paris, 1ère chambre, section sociale, jugement du 19 avril 2005, Comité d'entreprise d'Effia Services, Syndicat Sud Rail / Effia Services. La société avait mis en place un système de contrôle des horaires de travail à l'aide d'empreintes digitales compilées dans une base de données. Le but recherché était l'amélioration de l'établissement des bulletins de paie des salariés. Mais le tribunal a interdit ce dispositif car l'utilisation des informations biométriques ne peut se justifier que par une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés. Dès lors, le traitement mis en œuvre n'était ni adapté ni proportionné au but recherché.

de la finalité » afin *« de s'assurer que les informations utilisées sont de qualité adéquate pour servir aux fins envisagées, non érigé la redondance [de la collecte] en garantie de la vie privée*[194] ». Cette garantie qui est notamment renforcée par les mesures de confidentialité et de sécurité prise par le responsable des traitements pour le traitement automatisé de données personnelles.

3. Le principe de la confidentialité et de sécurité

L'article 34 alinéa 1 de la loi informatique et libertés dispose que *« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». C'est dire que les responsables de traitements de données doivent mettre en œuvre toutes les mesures techniques et toute l'organisation appropriées pour assurer la protection des données. Ces mesures doivent viser à prévenir la destruction accidentelle ou illicite, la perte accidentelle, la mise à jour, l'altération, la diffusion ou l'accès non autorisé aux données[195]. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger[196]. C'est pourquoi, Il est nécessaire de définir précisément les personnes ou catégories de personnes autorisées à enregistrer, modifier ou traiter les données et, pour les traitements les plus sensibles, de prévoir des mesures de sécurité appropriées (habilitation individuelle, délivrance d'un mot de passe personnel, mémorisation des consultations…), voire le contrôle de l'autorité judiciaire.

L'obligation de sécurité pèse principalement sur le responsable du traitement même lorsqu'il a recours aux services d'un hébergeur. La responsabilité par rapport à la sécurité ne peut jamais être impartie entièrement à un tiers. Une impartition de services équivaut à

[194] TRUDEL, Pierre. *Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau*. CRDP. Université de Montréal. P. 29. Mars 2003. Clôture de la mise en demeure adoptée à l'encontre du centre hospitalier de Saint-Malo. 17 octobre 2013. www.cnil.fr

[195] Voir également le paragraphe 11 des Lignes directrices de l'OCDE régissant la protection de la vie privée, ainsi que le paragraphe 56 de l'Exposé des motifs : « *Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non-autorisés* ».

[196] Article 17- 1°, 2éme alinéa, de la directive du 25 Octobre 1995 consacrée à la sécurité des traitements

l'impartition de sa réputation, de la protection de ses données, des risques associés à cette activité et à sa conformité réglementaire. Le fournisseur de services a la responsabilité de rendre les services de façon sécuritaire, par contre toutes divulgation ou bris de sécurité demeurera, à l'égard des tiers, la responsabilité du client[197] (ici, le responsable de traitement).

Dans un souci de sécurité les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier (par exemple, un mois pour les enregistrements de vidéosurveillance, deux ans à compter de la dernière aide pour le fichier d'aide sociale, un an après le dernier contact avec l'intéressé pour le fichier des demandeurs d'emploi). En effet, plus on détient de données, plus le risque de détournement est grand.

Ce principe est d'importance capitale car il conditionne la fiabilité du traitement, c'est un gage de confiance à l'égard des titulaires des données à traiter. En matière de santé par exemple, le secret professionnel dont est tenu le médecin par le Code de déontologie étend le secret professionnel à tout ce que le médecin a vu, connu, appris, constaté, découvert ou surpris dans l'exercice de sa profession[198]. Cette confidentialité apparaît comme un outil qui permet la préservation de valeurs : permettre l'accès aux soins de santé sans crainte de divulgation.

Tous les principes précités trouvent aussi leur source dans les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990. Ces principes constituent des orientations que donnent les Nations Unies quant aux règlements concernant les fichiers informatisés contenant des données à caractère personnel. Les modalités d'application sont laissées à la libre initiative des États. Comme pour confirmer qu'il n'y a jamais trop de dispositions prises pour assurer la sécurité de la vie privée, le législateur français a complété les obligations des responsables du traitement par des droits reconnus aux titulaires des données à traiter.

[197] PAUL, Daniel. *Le droit des technologies de l'information au Québec*. P. 166.

[198] Article R 4127-4 du code de la santé publique.

B. Les droits des personnes dont les données font l'objet de traitement

Les textes qui régissent les principes liés aux obligations des responsables de traitements précités sont également unanimes sur le fait de respecter les droits des personnes concernées : Il s'agit du droit d'information, du droit d'accès, du droit de rectification et de radiation et du droit d'opposition de tout citoyen.

1. Le droit à l'information préalable

Les personnes fichées doivent être informées de l'enregistrement des données les concernant. L'article 32[199] de la loi informatique et libertés impose à l'auteur de la collecte d'informations une obligation de renseignement. Cela l'oblige à informer préalablement les personnes auprès desquelles sont recueillies les informations nominatives de l'identité du responsable et de la finalité du traitement. En outre, il doit leur être notifié le caractère obligatoire ou facultatif des réponses, des conséquences à leur égard d'un défaut de réponse, des personnes physiques ou morales destinataires des informations et de l'exercice d'un droit d'accès et de rectification.

S'agissant de la forme sous laquelle doit être donnée cette information, la loi informatique et libertés ne donne pas davantage de précisions sur la manière de notifié les renseignements aux citoyens. Est-ce par voie orale, par écrit, ou par tout moyen ? Le législateur se contente de dire que l'information doit se faire préalablement au traitement de données. En l'absence de toute précision, on est en droit de retenir que cela peut se faire par

[199] Article 32 de la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel modifiant la loi du 6 janvier 1978.
« *I. La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :*
1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
2° De la finalité poursuivie par le traitement auquel les données sont destinées ;
3° Du caractère obligatoire ou facultatif des réponses ;
4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;
5° Des destinataires ou catégories de destinataires des données ;
6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre (droits des personnes à l'égard des traitements de données) ;
7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne.
Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°. »

tout moyen. Dans la pratique, il est d'usage que le responsable du traitement fasse signer une décharge par la personne concernée par laquelle elle donne son autorisation pour le traitement de ses données personnelles.

Quant au fond, la stricte application de la loi entre en conflit avec d'autres textes. En matière de santé, par exemple, le respect de ce droit des patients posait un problème aux médecins, notamment ceux responsables des registres épidémiologiques, des cancers avant le 1er juillet 1994. En effet, l'article 35 du code de déontologie impose aux médecins, dans l'intérêt du malade et pour les raisons légitimes qu'il apprécie discrétionnairement, de tenir celui-ci dans l'ignorance d'un diagnostic ou d'un pronostic grave[200]. Ce qui s'opposait littéralement au principe de l'obligation d'information. En pratique, certains courraient le risque d'y déroger mais ces médecins responsables de ces registres qui ont privilégié le code de déontologie n'ont jamais fait l'objet de poursuites, sans doute, en reconnaissance du bien-fondé de la faculté de réserve énoncée par l'article 43[201] de la loi informatique et libertés.

Cette difficulté a été atténuée par la loi du 1er juillet 1994[202] en son article 40-5 qui institue, de manière explicite, sous réserve de l'approbation de la CNIL, la possibilité d'une dérogation à l'obligation de renseignement lorsqu'il y a certaines difficultés à retrouver les titulaires des données traitées. En effet, pour les besoins de la recherche dans le domaine de la santé, certaines informations médicales nominatives peuvent émaner d'autres sources que le patient lui-même. Il peut s'agir, par exemple de laboratoires de biologie ou de services de radiologie, et les informations peuvent avoir été initialement collectées plusieurs années auparavant, à d'autres fins. Il devient donc parfois, très difficile de retrouver les personnes titulaires de ces données et c'est probablement pour ne pas s'opposer à l'intérêt que présentent ces recherches que le rédacteur de la loi du 1er juillet 1994 a institué cette dérogation.

---

[200] Article 35 du code de déontologie : «*... toutefois dans l'intérêt du malade et pour des raisons légitimes que le praticien apprécie en conscience, un malade peut être tenu dans l'ignorance d'un diagnostic ou d'un pronostic grave...*»

[201]Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique.

[202] Loi 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.
Ce texte est aujourd'hui repris par l'article 57 de la loi du 6 août 2004 «*Dans le cas où les données ont été initialement recueillies pour un autre objet que le traitement, il peut être dérogé à l'obligation d'information individuelle lorsque celle-ci se heurte à la difficulté de retrouver les personnes concernées. Les dérogations à l'obligation d'informer les personnes de l'utilisation de données les concernant à des fins de recherche sont mentionnées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui statue sur ce point*».

Le droit à l'information du citoyen peut être limité, dans certains cas, à l'identité du responsable du traitement et à la finalité de données collectées « *si les données à caractère personnel recueillies sont appelées à faire l'objet, à bref délai d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la [...] loi par la Commission nationale de l'informatique et des libertés*[203]*... »*. Mais, il ne doit pas être omis par le responsable de traitement. Une sanction prononcée par la CNIL a été confirmée par le Conseil d'État dans ce sens, le 12 mars 2014. Le site d'annuaires en ligne pages jaunes avait été sanctionné d'un avertissement public en 2011 de la part de la CNIL pour avoir utilisé les informations personnelles recueillies automatiquement sur les réseaux sociaux sans en avoir, au préalable, informer les concernés. Le Conseil d'État, a confirmé la décision de la Commission en retenant que les données ont été collectées de façon déloyale et illicite en l'absence de consentement explicite et éclairé des intéressés[204].

Le droit à l'information donne un droit d'accès aux informations collectées sur une personne.

2. Le droit d'accès

Le droit d'accès est prévu par l'article 39[205] de la loi informatique et libertés. Il est défini comme le droit qu'à une personne d'interroger le responsable du fichier pour savoir s'il

[203]Article 32. IV de la loi informatique et libertés du 6 août 2004.

[204] Conseil d'État, 10ème et 9ème sous-sections réunies, 26 mars 2012. Requête n° 353193. Sociétés pages jaunes groupe c/ Commission national de l'informatique et des libertés. Publié dans les tables du recueil Lebon 2014.

[205] Article 39 de la loi informatique et libertés

I. - Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.

contient des informations nominatives la concernant et d'en connaître le contenu. Ce droit a été institué par le législateur pour permettre aux personnes de pouvoir vérifier les informations collectées sur elles et la régularité des traitements dont ces informations sont l'objet. *« Mentionné parmi les principes généraux placés en tête de la loi*[206] », le droit d'accès permet à tout individu déclinant son identité, d'obtenir la vérification des informations le concernant et même d'en demander une copie pour un prix modique n'excédant pas le coût de la reproduction. Il peut éventuellement les contester.

Si, en principe tout citoyen peut accéder à toutes les informations nominatives le concernant, la loi prévoit des dispositions contradictoires pour garantir l'intérêt du développement de l'informatique et éviter les abus de personnes désireuses de s'opposer de manière systématique et injustifiée au traitement de leurs données. Elle autorise le responsable du fichier à saisir contradictoirement la Commission pour obtenir des délais de réponse. Il peut être également autorisé à ne pas tenir compte des demandes si elles paraissent vraisemblablement abusives[207] ou si les données sont conservées sous une forme ne présentant aucun risque[208].

Le droit d'accès peut être indirect. Il est prévu pour les informations jugées particulièrement sensibles : celles concernant la sûreté de l'État, la défense et la sécurité publique[209] (fichiers de police et de gendarmerie, fichiers de renseignement, fichier Schengen,

---

[206] MORANGE, Jean. *Manuel des droits de l'homme et libertés publiques.* p. 171

[207] Article 39 de la loi informatique et libertés
II. - Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées.

[208] Article 39 de la loi informatique et libertés, II, 2ème paragraphe.
Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36 *(traitement de conservation d'archives)*, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés.

[209] Article 41 de la loi informatique et libertés
Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.
La demande est adressée à la Commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la Commission. Il est notifié au requérant qu'il a été procédé aux vérifications.

etc.) celles ayant un caractère médical[210]. C'est aussi le cas lorsqu'il s'agit de traitements effectués par des personnes publiques ou privées ayant une mission de service public relative à des infractions de tout genre dont celles touchant au paiement de l'impôt[211].

Le droit d'accès aux informations personnelles peut s'exercer par écrit mais également sur place[212]. Il permet d'user de son droit de rectification et de radiation.

3. Le droit de rectification et de radiation

Aux termes de l'article 40 alinéa 1er de la loi informatique et libertés modifiée, *« Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».*

Il énonce ainsi les droits de rectification et de radiation qui sont reconnus à tout individu dont les données personnelles font l'objet de traitement. Il est en effet, autorisé à demander la correction de ses données en cas d'erreur ou même la suppression. L'application de ce droit se fait essentiellement par lettre écrite à l'organisme détenteur desdites informations. Le responsable du traitement devra alors justifier qu'il a procédé aux rectifications demandées en faisant parvenir gratuitement, à la demande de la personne concernée, un exemplaire de l'enregistrement qui a été modifié.

Ce pouvoir de modification s'applique à la fois aux informations saisies sur la personne et sur les raisonnements utilisés dans le traitement automatisé de décisions prises à partir de leurs résultats. Il peut ne pas être exercé ou ne pas conduire forcément à la suppression

---

[210] Article 43 de la loi informatique et libertés.
Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique

[211] Article 42 de la loi informatique et libertés.
Les dispositions de l'article 41 sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions, ou de contrôler ou recouvrer des impositions, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25 *(autorisation par la CNIL)*, 26 *(autorisation par décret en Conseil d'État ou arrêté)* ou 27 *(autorisation par décret en Conseil d'État, arrêté ou décision de l'organe délibérant)*.

[212] CNIL. *Guide droit d'accès*. Les guides de la CNIL, édition 2010. p.4. www.cnil.fr. Consulté le 17 avril 2014.

d'informations. Mais, il est impératif que le responsable du traitement renonce à les conserver au delà de la durée obligatoirement indiquée dans la déclaration ordinaire ou la demande d'avis soumise à la CNIL : c'est « le droit à l'oubli[213] ».

Cette notion, couramment employée par la doctrine de la CNIL véhicule l'idée selon laquelle des informations nominatives ne peuvent être conservées plus longtemps que le nécessite la finalité des traitements. Craignant, le cas échéant, que des informations peu honorables suivent une personne durant toute sa vie, la CNIL prône l'adoption de ce droit à l'oubli numérique au rang de principe à caractère Constitutionnel. Le Président Alex TÜRK[214] en est bien conscient et déplore que si cela devient effectif en France, la solution ne soit pas totalement efficace tant que les Américains et le reste du monde n'adhèrent pas à cette politique[215]. La position de l'Union européenne, jusque-là défavorable au droit à l'oubli donne des signes de changement dans le sens inverse. Alors que la cour de justice de l'Union, par son avocat général NIILO JÄÄSKINEN[216] a refusé le bénéfice du droit à l'oubli[217] à une personne contre Google en juin 2013, la proposition de règlement européen consacre ce droit en son article 17[218]. C'est l'une des innovations majeures de ce projet. L'article 17 confère un

[213]Article 6, 5° de la loi informatique et libertés.

[214] Président de la CNIL de 2004 à 2011.

[215]JULIEN L. *la CNIL favorable à l'inscription du droit à l'oubli numérique dans la Constitution*. Numerama magazine, publié le 24 novembre 2009. http://www.Numerama.com. Consulté le 7 avril 2014.

[216] Cour de justice de l'Union européenne. Communiqué de presse de cette décision n° 77/13. Luxembourg, le 25 juin 2013. Conclusions de l'avocat général dans l'affaire C-131/12, Google Spain SL, Google Inc./Agencia espagnola de protecciòn de datos, Mario Costeja González. http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077fr.pdf. Consulté le 7 avril 2014.

[217] La requête d'un citoyen espagnol auprès de l'éditeur du journal qui avait publié une adjudication sur saisie immobilière pratiquée en recouvrement des dettes de la sécurité sociale pour lui demander d'effacer et de mettre à jour les informations la concernant avait été rejetée. L'éditeur lui a répondu qu'il n'y avait pas lieu d'effacer les données le concernant, au motif que la publication avait été effectuée sur ordre du ministre du travail et des affaires sociales. S'étant tourné sans succès vers Google pour réclamer que les résultats des recherches ne fassent plus mention d'aucun lien vers le journal, le requérant a également saisi l'agence espagnole de protection des données. Cette dernière ayant fait droit à sa requête contre Google et non contre l'éditeur, sa décision a été portée devant l'Audience nationale de l'Espagne qui l'a annulée. C'est dans ce contexte que cette juridiction a déféré une série de questions devant la Cour de justice notamment celle relative au droit à l'oubli. L'avocat général a rejeté la demande au motif que la directive européenne 95/46 n'établit pas de « droit à l'oubli » de portée générale. Un tel droit ne saurait être invoqué à l'encontre des fournisseurs de moteurs de recherche sur Internet en s'appuyant sur la directive, même si celle-ci est interprétée en conformité avec la charte des droits fondamentaux de l'Union européenne. Communiqué de presse de cette décision n° 77/13. Luxembourg, le 25 juin 2013. Conclusions de l'avocat général dans l'affaire C-131/12, Google Spain SL, Google Inc./Agencia espagnola de protecciòn de datos, Mario Costeja González. http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077fr.pdf. Consulté le 7 avril 2014.

[218] « 1. *la personne concernée a le droit d'obtenir des responsables du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données, en particulier en ce qui*

droit à l'oubli numérique et à l'effacement. Il développe et précise le droit d'effacement prévu à l'article 12, point b) de la directive 95/46/CE et fixe les conditions du droit à l'oubli numérique, notamment l'obligation qui est faite aux responsables du traitement ayant rendu public des données à caractère personnel d'informer les tiers de la demande de la personne concernée d'effacer tout lien vers ces données ou les copies ou reproductions qui en ont été faites. Il intègre aussi le droit de limiter les traitements dans certains cas, en évitant le thème équivoque de « verrouillage »[219].

Pour l'heure, ce droit ne peut s'exercer qu'en l'absence de dispositions législatives contraires. La loi sur les archives du 3 janvier 1979[220] qui n'autorise à détruire les fichiers portant sur des données nominatives que si elles sont sans intérêts scientifique, statistique ou historique en constitue un obstacle. Les généalogistes, archivistes et historiens sont opposés à la proclamation d'un droit à l'oubli par le règlement européen. Pour Michel SEMENTERY, Président de la fédération française de généalogie, un tel traitement rendrait dans le futur impossible les recherches généalogiques ou historiques, les archives n'ayant plus de données personnelles à conserver et à communiquer ; le croisement des sources serait également impossible, la mise en ligne des données anciennes interrompues[221]. La pétition lancée en mars 2013 par l'association des archivistes français a recueilli plus de 40 000 signatures et intéresse non seulement les archivistes, les historiens mais également les chercheurs et les statisticiens toutes matières confondues.

---

concerne les données à caractère personnel que la personne concernée avait rendu disponible lorsqu'elle était enfant, ou pour l'un des motifs suivants :

a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées,

b) la personne concernée retire le consentement sur lequel est fondé le traitement conformément à l'article 6, paragraphe 1, point a) ou lorsque le délai de conservation a expiré et qu'il n'existe pas de motif légal au traitement des données;

c) la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19.

d) le traitement des données n'est pas conforme au présent règlement pour d'autres motifs...».

8 autres hypothèses sont émises dans la suite du même article. Proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection de données). Article 17, 1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 9 avril 2014.

[219] Proposition de règlement du Parlement européen et du Conseil. p. 10. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 9 avril 2014.

[220]Article 4-1 de la Loi n° 79-18 du 3 janvier 1979 sur les archives publiques.

[221] DE MORANT, Guillaume. *Europe : les archivistes en alerte*. Le Mag Coulisse des archives. p. 16. rfg. n° 205 Avril- Mai 2013. Http://www.cil.cnrs.fr/CIL/IMG/pdf/coulisses_des_archives_rfg_205.pdf. Consulté le 9 avril 2014.

La CNIL est, au contraire, un fervent défenseur de ce droit. C'est ce qui l'a amené en 1981, à s'opposer à la mise en œuvre de certains fichiers comme celui dénommé GAMIN[222]. Une délibération[223] avait même été prise à cet effet, à l'époque.

Dans le domaine bancaire[224], la CNIL avait aussi obtenu des résultats en réussissant à convaincre les banques de retirer immédiatement du fichier central des retraits de cartes "CB" qui constitue un sous-ensemble du Fichier central des chèques (FCC) les noms des personnes qui y ont été inscrites suite à une décision de retrait de leur carte bancaire consécutive à un incident (manque de provision lors du retrait ou d'une transaction). En effet, les noms des personnes concernées doivent être inscrits pendant 2 ans après l'incident et jusque-là le retrait ne se faisait pas avant même si celles-ci régularisaient leur situation. Certaines s'en sont plaint à la CNIL et, débutée depuis 2004, la négociation n'a pu aboutir que 5 ans plus tard.

En 2001, une autre délibération[225]a eu pour objectif de demander l'anonymisation des décisions de justice publiées sur internet. Cette position de la CNIL peut évoluer en fonction des cas. Une récente sanction de la CNIL entérinée par le Conseil d'État[226] donne de comprendre que la violation de la loi informatique et libertés fait perdre ce droit à l'oubli au contrevenant. En effet, La CNIL a infligé à une société spécialisée dans l'administration de

[222]GAMIN avait pour objet de permettre, sur la base des informations de nature médicale et sociale recueillies à partir des certificats de santé établis dans le cadre de la protection maternelle et infantile, la sélection automatique des enfants devant faire l'objet d'une surveillance médico-sociale particulière. LDH Toulon, *Il y a 30ans, G.A.M.I.N ou l'oubli de l'humain*, article publié le 20 juin 2009, http://www.ldh-toulon.net/spip.php?article3353. Consulté le 28 avril 2014.
Pour Michel GENTOT, président de la Cnil de février 1999 à janvier 2004, cela revenait à faire du nouveau né un enfant qui fait l'objet d'un suivi et plus tard un adulte qui a été suivi. L'enfant serait « marqué », « fiché » à jamais. *La protection des données personnelles à la croisée des chemins*, chapitre 1 du tome 3 de *La protection de la vie privée dans la société d'information*, p.39
Voir également le rapport de l'Assemblée nationale, tome 2, n°3125 (première session 1977 - 78), P. 2.

[223]Délibération n°81-74 du 16 juin 1981 portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile

[224] CNIL. *Un pas vers le droit à l'oubli.* http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/un-pas-vers-le-droit-a-loubli-bancaire/. Consulté le 3 mars 2010.

[225]Délibération n° 01-057 de la CNIL du 29 novembre 2001, portant recommandation sur la diffusion des données personnelles sur internet par les banques de données de jurisprudence. www.cnil.fr

[226] Conseil d'État. 10ème et 9ème sous-sections réunies. 12 mars 2014. (Requête n° 354629) société Foncia Groupe c/ CNIL. http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CÉ TATEXT 000028717845&fastReqId=95403750&fastPos=1. Consulté le 3 avril 2014.

biens immobiliers un avertissement[227] rendu public, pour avoir exploité un traitement informatique recensant des biens immobiliers disponibles pour des opérations de vente et de location, en méconnaissance de la loi informatique et libertés. Estimant la sanction disproportionnée et sollicitant l'anonymisation de la décision lorsqu'elle va être publiée sur internet, la société a saisi le Conseil d'État. Mais la Haute autorité administrative, jugeant la sanction de la CNIL proportionnelle à la gravité des fautes commises a rejeté la demande tendant à rendre la décision anonyme.

Le droit de rectification constitue un élément essentiel du droit d'accès en ce sens qu'il permet de garantir l'exactitude des données traitées et d'en assurer ainsi la qualité[228]. Ce droit permet non seulement, de protéger les libertés individuelles et publiques mais également, de maîtriser les effets fantasmiques des traitements informatiques face à la fascination exercée sur les néophytes. En cas de demande de rectification, le responsable du traitement doit justifier sans frais pour la personne qui en fait la demande, des opérations effectuées dans ce sens. Devant les tribunaux, il pèse également sur lui la charge de la preuve qu'il a faite suite à une demande de rectification.

4. Le droit d'opposition

Selon l'article 38 de la loi informatique et libertés, toute personne a le droit de s'opposer à ce que ses données fassent l'objet de traitement à condition de justifier de « *motifs légitimes* ». Mais ce droit ne peut pas être exercé lorsque « *le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement*[229] ».

Dès lors, même si ce texte semble consacrer un droit essentiel de l'individu à refuser que ses données personnelles soient utilisées à des fins de prospection, il prévoit certaines limites à

[227] CNIL. Délibération n° 2011-205 du 6 octobre 2011. [en ligne]. Avertissement public. Disponible sur: http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2011-205_ Avertissement_FONCIA.pdf. Consulté le 28 mai 2014.

[228] La qualité de données renvoie à un traitement qui respecte l'ensemble des principes énumérés ci-dessus comme obligations incombant aux responsables du traitement selon l'article 6 de la directive européenne 95/46/CE sus-mentionné ou encore des données dont la sécurité a été préservées et, notamment, que le responsable a empêché qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès au sens de l'article 34, alinéa1 de la loi informatique et libertés. .

[229]Article 38, alinéa 3 de la loi informatique et libertés.

l'exercice de cette liberté par le citoyen notamment, l'exigence de motifs légitimes et la barrière légale prévue à l'alinéa 3.

S'agissant des raisons légitimes, l'absence de précision de la loi quant à l'étendue de la légitimité laisse toute latitude aux tribunaux pour déterminer si la requête est recevable ou non et cela peut être source de difficultés certaines. Cela sera le cas surtout dans les disciplines où l'avis d'un expert s'avère nécessaire comme en matière de santé par exemple.
Mais lorsque la légitimité est établie, passer outre l'opposition d'un individu expose à des sanctions exemplaires. Ainsi, en dehors des peines que pourraient prononcer les tribunaux sur la base de l'article 226-18.1[230] du code pénal, la CNIL a déjà requis des condamnations à l'encontre de certaines entreprises commerciales. Ce fut le cas lorsque par une délibération en date du 6 novembre 2008[231] elle a condamné Cdiscount à une amende[232] de 30 000 euros suite à plusieurs plaintes de personnes qui ne parvenaient pas à exercer leur droit d'opposition pour ne plus recevoir de mails publicitaires de la part de Cdiscount.

Concernant la limite légale de l'article 38, alinéa 3, elle ôte à la personne la possibilité de jouir d'un droit dont elle est, en principe, détentrice avant même que l'abus n'ait été commis. Cet alinéa 3 n'est pas non plus explicite en ce sens qu'il ne précise pas les cas où une disposition légale pourrait empêcher l'individu de manifester son opposition ni quel type d'acte pourrait prévoir d'évincer ce droit. Mais on pourrait se référer aux anciens articles 15 et 26 de loi informatique et libertés de 1978 pour déduire qu'il pourrait bien s'agir de fichiers créés pour le compte de l'État, d'un établissement public, de collectivité territoriale ou de

[230] « *Article 226-18-1.* - Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

[231] Délibération n° 2008-422 du 6 novembre 2008 portant décision de la formation restreinte à l'égard de la société Cdiscount. [en ligne], disponible sur: http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/147/. Consulté le 20 mai 2010.

[232] Saisie de plaintes de personnes ayant tenté sans succès de se désabonner, à plusieurs reprises, des listes de diffusion de la société Cdiscount afin de ne plus recevoir de courriers électroniques publicitaires, la Commission a alors adressé à la société Cdiscount un courrier lui demandant de procéder à la radiation de ses fichiers commerciaux des informations relatives aux personnes concernées. Les plaintes se multipliant, la Commission a mis en demeure la société Cdiscount, sous un délai d'un mois à compter de la notification, de :
- prendre toutes mesures de nature à garantir qu'il soit tenu compte, de manière efficace, systématique et immédiate, du droit d'opposition exercé par toute personne concernée à recevoir de la prospection commerciale, en application de l'article 38 de la loi du 6 janvier 1978 dite loi informatique et libertés ;
- préciser à la Commission national informatique et libertés, l'origine des adresses électroniques des personnes démarchées par courriel et les modalités du recueil de leur consentement préalable à l'envoi de ces courriels (...).
Faute de réponse et considérant que la société Cdiscount ne s'était pas exactement conformée à la mise en demeure en ce qui concerne le manquement au droit d'opposition, la CNIL prononça une sanction pécuniaire de 30.000 euros. www.journaldunet.com/. Consulté le 20 mai 2010.

personne morale de droit privé gérant un service public. Ainsi, les patients des hôpitaux publics ou les personnes participant au service public hospitalier ne peuvent pas s'opposer à l'enregistrement de leurs informations nominatives. Cela s'expliquerait par le fait que les traitements effectués dans le secteur public sont censés avoir obtenu, au préalable, l'aval de la CNIL. Ils sont obligatoirement soumis à une procédure de création par acte réglementaire pris après avis motivé de la CNIL. Il y a donc une présomption de sécurité des informations personnelles qui pèse sur ces types de traitement.

Cet alinéa 3 de l'article 38 de la loi de 2004 semble rejoindre l'interprétation que la CNIL avait faite en 1992 pour dénoncer l'alinéa 2 de l'article 26 qui, ramenant à l'article 15[233], prévoyait que le droit d'opposition *ne s'applique pas aux traitements limitativement désignés dans l'acte réglementaire prévu à l'article 15* c'est-à-dire ceux opérés par le secteur public. En reprenant de façon large, cet article en ces termes: « *le droit d'opposition s'applique dans tous les cas sauf mention contraire expressément portée dans l'acte réglementaire créant le traitement*[234] » dans son 13ème rapport annuel d'activité, la CNIL entendait dénoncer cette restriction de liberté. Dans ce cas, on est tenté de croire avec certains auteurs que la « *CNIL semblait à la fois, aller à l'encontre du texte de la loi et à l'encontre de sa propre autorité en matière d'appréciation des risques pour les libertés individuelles, puisque le traitement auquel elle reconnaît à la personne le droit de s'opposer a reçu son aval*[235] *».*

Ce consentement de la CNIL pour le traitement des données personnelles est plus difficile à obtenir lorsqu'il s'agit de données médicales en ce sens que celles-ci sont soumises à un régime particulier.

---

[233] Article 15 de la version initiale de la loi informatique et libertés du 6 janvier 1978 : « *Hormis les cas où ils doivent être autorisés par la loi, les traitements automatisés d'informations nominatives opérés pour le compte de l'État, d'un établissement public ou d'une collectivité territoriale, ou d'une personne morale de droit privé gérant un service public, sont décidés par un acte réglementaire pris après avis motivé de la Commission nationale de l'informatique et des libertés »*

[234] 13ème rapport annuel d'activités de la CNIL, 1992. Paris: La documentation française. 1993. p. 22.

[235] DUCROT, Henry. DUSSERRE, Liliane, ALLAËRT. *L'information médicale, l'ordinateur et la loi*. 2ème édition. p. 47

CHAPITRE II : LE CADRE JURIDIQUE PARTICULIER DU TRAITEMENT AUTOMATISE DES DONNEES MEDICALES

Comme pour l'ensemble des données sensibles, il est en principe, interdit de traiter les données médicales (Section 1). Mais, ce principe est assorti d'exceptions et dans les cas où ces données de santé peuvent être traitées, elles sont soumises à une procédure exorbitante du régime de droit commun des traitements de données personnelles (Section 2).

Section 1 : Le principe de l'interdiction de traitement automatisé

Il est de principe que les données médicales soient exclues des traitements automatisés (Paragraphe 1) mais la loi admet des exceptions à cette règle (Paragraphe 2).

Paragraphe 1 : L'exposé du principe

Le principe de l'interdiction de traiter les données sensibles, notamment les données médicales a des sources tant supranationales (1) que nationales (2).

A.Les sources supranationales du principe de l'interdiction

S'il est admis que la dangerosité d'un traitement de données pour les droits et libertés de la personne concernée s'apprécie en fonction de la finalité poursuivie par le responsable du traitement, s'agissant des données « sensibles » dont celles de santé, leur seul contenu expose déjà leur titulaire à des risques sans tenir compte de la finalité. Toute utilisation de celles-ci impliquant ainsi automatiquement des risques d'atteinte aux droits et libertés, les législateurs

ont décidé d'en interdire le traitement. Cette interdiction a été posée par la convention n°108 de 1981 et reprise par la directive européenne 95/46 qui a consacré le même principe.

1. La convention n° 108

La convention 108 dispose que : *« les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales*[236] *»*. Ainsi, la convention est le premier texte international à valeur contraignante à consacrer le principe de l'interdiction de traitement des données de santé en tant que *«catégories particulières de données »*. Cette disposition subordonne le traitement des données sensibles à des garanties appropriées apportées par le droit interne. Cette garantie doit avoir pour objectif de « *prévenir les risques que le traitement de données sensibles peut présenter pour les intérêts, les droits et libertés fondamentales de la personne concernée, notamment les risques de discrimination*[237]».

Antérieurement à la Convention, un ensemble de lignes directrices du Conseil de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du 23 septembre 1980 avait déjà émis des recommandations[238] allant dans ce sens pour l'ensemble des données personnelles. Mais elles fixaient un principe de limitation en matière de collecte des données à caractère personnel sans préciser celles qui sont considérées comme sensibles et ne mentionnaient pas particulièrement les données de santé. L'OCDE laissait toute latitude aux États membres de le faire « *selon les traditions et les attitudes propres à chaque pays Membre*[239] » sachant qu'aucune donnée n'est en elle-

[236] Convention 108 du 21 janvier 1981, Article 6 – Catégories particulières de données.

[237] Convention 108 du 21 janvier 1981 (version modernisée), Article 6 – Traitement de données sensibles.

[238] Recommandation du Conseil de l'OCDE concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du 23 septembre 1980, 5ème partie, paragraphe 7, Les points 50 à 52. Disponible sur: http://www.oecd.org/document/57/0,3343,fr_2649_34255_1815225_1_1_1_1,00.html. Consulté le 3 septembre 2011.

[239] Point 51, paragraphe 7 de la recommandation du 23 septembre 1980 op. cit.

même privée ou sensible mais peut le devenir en fonction du contexte et des circonstances dans lesquels elle est traitée. Certes, ce n'était qu'une recommandation, mais elle jetait les prémisses d'une harmonisation en matière de protection des données personnelles à partir des motifs[240] de l'élaboration de ses lignes directrices. Cela a probablement eu pour effet d'accélérer l'adoption de la Convention n° 108 pratiquement 4 mois plus tard. Depuis 2011, un processus de modernisation de la convention a été lancé en vue d'adapter les dispositions à l'évolution actuelle des technologies de l'information et de la communication. S'agissant des données sensibles, l'article 6 intitulé traitement « *catégories particulières de données* » a été remplacé par le « *traitement de données sensibles* ». La liste des données dites sensibles a été complétée par les données génétiques et biométriques, des données relatives à l'appartenance syndicale et celles concernant les infractions et les autres mesures de sûreté connexes. Alors que l'interdiction de traitement était exprimée par l'expression « *les données (…) ne peuvent être traitées automatiquement à moins que* » la proposition de modernisation emploie l'expression « *le traitement (…) n'est autorisé qu'à la condition que* ». Si ces différences dans la terminologie ne doivent pas être interprétées comme entraînant des divergences autres que de pure forme, cette formule laisse sous-entendre une plus grande tendance à l'autorisation de traitement ou, du moins, une plus grande tolérance, que la première. Il faut croire que l'intérêt économique de traitement accru de données personnelles, particulièrement des données médicales a influencé les rédacteurs de cette proposition de modernisation. A défaut de passer du principe de l'interdiction à celui de l'autorisation, le ton a été assoupli ; ce qui n'est pas rassurant pour l'avenir de la protection des données sensibles de plus en plus en proie à la commercialisation.

La Convention 108 a été suivie de l'adoption par plusieurs États membres de législations sur la protection des données personnelles. Mais, pour veiller à une meilleure harmonisation au sein de l'Union, des dispositions ont été prises au début des années 90 qui ont conduit à l'adoption de la directive européenne de 1995 relative à la protection des

[240] *« Compte tenu de l'essor pris par le traitement automatique de l'information, qui permet de transmettre de vastes quantités de données en quelques secondes à travers les frontières nationales et même à travers les continents, il a fallu étudier la question de la protection de la vie privée sous l'angle des données de caractère personnel. Des législations relatives à la protection de la vie privée ont été adoptées ou le seront prochainement dans près de la moitié des pays de l'OCDE (l'Allemagne, l'Autriche, le Canada, le Danemark, les États-Unis, la France, le Luxembourg, la Norvège et la Suède ont promulgué une législation. La Belgique, l'Espagne, les Pays-Bas et la Suisse ont établi des projets de loi) en vue de prévenir des actes considérés comme constituant des violations des droits fondamentaux de l'homme, tels que le stockage illicite de données de caractère personnel qui sont inexactes, l'utilisation abusive ou la divulgation non autorisée de ces données. »* 1er paragraphe de la préface de la recommandation op. cit.

personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qui renchérit le principe de l'interdiction et se montre plus explicite[241].

2. La Directive 95/46/CE

10 ans après l'entrée en vigueur de la convention 108 du Conseil de l'Europe, la Commission des communautés européennes a jugé nécessaire de relancer le débat en proposant un texte de directive relative à la protection des personnes à l'égard des traitements de données à caractère personnel[242]. « *Pour éliminer les obstacles à la circulation des données à caractère personnel, le niveau de protection des droits et libertés des personnes à l'égard des traitements de ces données doit être équivalent dans tous les États membres ;(...) cet objectif, fondamental pour le marché intérieur, ne peut être atteint par la seule action des États membres compte tenu en particulier de l'ampleur des divergences (…); une intervention de la Communauté visant un rapprochement des législations est donc nécessaire*[243] ». La Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a été adoptée le 24 octobre 1995[244]. Elle précise et amplifie les principes de la convention 108[245]. L'objet de la directive est présenté par son article premier comme visant, d'une part, la protection des libertés et des droits fondamentaux des personnes physiques, notamment de la vie privée, à l'égard du traitement des données à caractère personnel et, d'autre part, la garantie de la libre circulation des données à caractère personnel entre États membres sans limitation justifiée par l'insuffisance de protection des personnes concernées.

---

[241] HERVEG, Jean. *La gestion des risques spécifiques aux traitements de données médicales en droit européen.* p. 83.

[242] Position commune n° 1/95 du Conseil de l'Europe du 20 février 1995 en vue de l'adoption de la directive relative à la protection des personnes physiques à l'égard des données à caractère personnel à la libre circulation des données. JOCE n° C 93/1 du 13 avril 1995. Isabelle de LAMBERTERIE. *Informatique, libertés et opinions religieuses* in Archives des sciences sociales des religions 1995, n° 91 (Juillet-septembre) p.22.

[243] Considérant 8 de la position commune du Conseil de l'Europe du 20 février 1995, op cit..

[244] JOCE, n° L 281/31 du 23 novembre 1995. p. 0031-0050.

[245] Préambule de la directive.

Pour ce qui est des traitements portant sur des catégories particulières de données, l'article 8.1 de la directive prévoit que : *« les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle* ». Cette interdiction met en exergue une dérogation au principe de la libre circulation des données à caractère personnel au sein de l'Union européenne[246] qui est, pourtant, prôné par la directive. Cette opposition s'explique par le fait que même si des dispositions sont prises pour assurer la sécurité de ces informations, il est essentiel d'accorder une attention toute particulière à celles de la catégorie des données médicales du fait de leur caractère singulièrement « sensible ». Le texte est explicite en la matière en disposant : « *les données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée ne devraient pas faire l'objet d'un traitement*[247] *»*. La priorité semble alors, être ainsi accordée au respect des libertés fondamentales et de la vie privée sur les intérêts économiques de la communauté. Mais ce n'est, en réalité, qu'une apparence car face au caractère incontournable des nouvelles technologies notamment, dans le milieu médical, un compromis est vite trouvé. La gestion informatique des données personnelles étant devenue indispensable pour les opérateurs économiques, la Directive a prévu des solutions conciliant le respect de la vie privée avec la liberté de circulation des données en vue de préserver simultanément les impératifs économiques et les libertés fondamentales.

Malgré l'importance de cette directive et les injonctions de Bruxelles, sa transposition s'est avérée longue et parfois complexe. La France a, par exemple, mis 9 ans pour la transposer[248] dans son système juridique. Pendant ce temps, la rapide évolution des technologies a créé de nouveaux enjeux pour la protection des données à caractère personnel. Le partage et la collecte de données ont connu une augmentation spectaculaire entraînant un climat de méfiance des individus. Pour instaurer la confiance dans l'économie numérique, essentielle au développement économique, la Commission européenne a entrepris depuis

[246] Voir les «considérant» 3 à 9 de la directive 95/46/CE.

[247] Considérant 33 de la directive 95/46/CE.

[248] Par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF n° 182 du 7 août 2004. p. 14063. Texte n°2. NOR : JUSX0100026L.

2009[249], d'établir un nouveau cadre juridique pour la protection des données à caractère personnel dans l'Union européenne. En lieu et place de la directive, ce cadre sera constitué par un règlement européen dont l'application sera directe et immédiate dans les États sans passer par la phase de la transposition[250]. L'objectif de ce règlement est de répondre à un besoin d'une politique plus globale et plus cohérente à l'égard du droit fondamental à la protection des données à caractère personnel au sein de l'Union. Il ambitionne de constituer « *un cadre juridique plus solide et plus cohérent en matière de protection de données, assorti d'une application rigoureuse des règles afin de permettre à l'économie numérique de se développer sur tout le marché intérieur et aux personnes physiques de maîtriser l'utilisation qui est faite des données les concernant, et de renforcer la sécurité juridique et pratique pour les opérateurs économiques et les pouvoirs publics*[251]. Le règlement reconduit l'interdiction de traitement des données à caractère personnel concernant la santé. Mais, alors qu'il proscrit par lui-même[252] cette gestion, la directive[253] laissait ce pouvoir aux États membres. C'est

[249] Du 9 juillet au 31 décembre, la consultation sur le cadre juridique applicable au droit fondamental à la protection des données à caractère personnel. La Commission a reçu 168 réponses, dont 127 provenaient de particuliers, d'organisations et d'associations professionnelles, et 12 de pouvoirs publics. Les contributions non confidentielles peuvent être consultées sur le site internet de la Commission : http://ec.europa.eu/ justice/newsroom/data-protection/events/090519_en.htm (en anglais uniquement). Proposition de règlement du Parlement européen et du Conseil op. cit. p.3. Consulté le 11 avril 2014.

[250]La Commission européenne a choisi un règlement pour remplacer la directive 95/46 car elle souhaite que l'harmonisation soit plus aboutie et plus rapide. En effet, à la différence des directives qui doivent être transposées par chacun des pays, les règlements n'ont pas à l'être et sont applicables immédiatement. Ainsi, cela devrait permettre de limiter les divergences dans l'application nationale de ce texte et éviter de reproduire ce qui avait eu lieu lors de la transposition de la directive de 1995 : tous les pays n'ont pas transposé de la même manière cette directive et les autorités de contrôle n'interprètent pas toujours les textes de la même manière ; c'est donc aujourd'hui un véritable casse-tête pour les entreprises qui sont soumises en Europe à différentes législations nationales en matière de protection de données. En outre, le choix d'un règlement devrait permettre d'éviter de trop longs délais de transposition. Pour autant, cela ne veut pas dire que ce règlement va trouver application immédiate en France. Nous avons encore beaucoup de temps avant que celui-ci ne soit applicable, au moins 4 ans : il faudrait bien deux ans avant que les règlement ne soit finalisé et publié au journal officiel de l'Union européenne. Ensuite, il ne sera pas applicable avant un délai de deux ans, dans le but de permettre aux États et aux autorités de contrôle de s'adapter. CHAFIOL CHAUMONT, Florence.*3 questions. Protection des données personnelles : propositions de la Commission européenne*. Semaine juridique-entreprise et affaires p. 5. n° 10 du 8 mars 2012.

[251] Proposition de règlement du Parlement européen et du Conseil op. cit. (Contexte de la proposition)

[252] « *Les traitements des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou la croyance, l'appartenance syndicale, ainsi que les traitements des données génétiques ou des données concernant la santé ou relatives à la vie sexuelle ou à des condamnations pénales ou encore à des mesures de sûreté connexes sont interdits.* » Article 9.

[253] « *Les États membres interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.* » Article 8.

l'application de l'effet direct des règlements comparativement aux directives. Ils introduisent une règle uniforme obligatoire, applicable directement[254] dans l'ordre juridique de tous les États membres ; ce qui rend inapplicables les réglementations nationales incompatibles avec les clauses matérielles qu'ils contiennent. Dans un souci de célérité, la Directive a été substituée par le règlement européen qui prévoit des actes délégués dans certains domaines, notamment celui de la sécurisation des données personnelles de catégorie particulière[255]. L'article 290 du traité sur le fonctionnement de l'Union définit les actes délégués comme des actes non législatifs de portée générale que la Commission peut adopter pour compléter ou modifier certains éléments non essentiels de l'acte législatif. Des actes d'exécution peuvent également être pris par la Commission conformément à l'article 291 du traité sur le fonctionnement de l'Union. Ce pouvoir lui permettra d'édicter des formulaires types ou autres documents aux fins d'assurer des conditions uniformes d'exécution du règlement. «*L'article 87 du règlement contient la disposition relative à la procédure de comité nécessaire pour conférer des compétences d'exécution à la Commission, dans les cas où, des conditions uniformes d'exécution d'actes juridiquement contraignants de l'Union sont nécessaire*[256]*s*».
De ce qui précède, on constate une tentative de décentralisation, voire de concentration, du régime relatif aux données personnelles dans les mains de la Commission. Si le désir d'harmonisation est évidemment louable, il est à craindre que cette même mainmise renforce la vision d'une Europe technocrate[257].

En attendant l'entrée en vigueur de ce règlement, la directive reste la référence qui, face au retard qu'elle prenait à se faire transposer par les États membres[258], avait été précédée en 1997 par la recommandation n° R (97) 5[259] du Conseil de l'Europe.

---

[254] L'article 91 du règlement dispose: « *Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.»*

[255] *« 3. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 86, aux fins de préciser davantage les critères, les conditions et les garanties appropriées pour le traitement des catégories particulières de données à caractère personnel mentionnées au paragraphe 1, ainsi que les dérogations prévues au paragraphe 2*. » Article 9 de la proposition de règlement.

[256] Proposition de règlement européen relative aux données personnelles. p. 17.

[257] CHAFIOL CHAUMONT, Florence. *Données personnelles Bruxelles reprend la main ! Éclairage sur le projet de règlement de la Commission européenne qui intéresse au plus haut point aussi bien les entreprises que les citoyens* in Expertise des systèmes d'information. n° 367, mars 2012. P. 99.

[258] KAUDER, Serge. *Les lois "Informatique et Liberté" en France, en Europe et dans le monde in* Technologies/Sécurité & Protection*. 16 décembre 2003.* http://www.net-iris.fr/blog-juridique/44-serge-kauder/8501/les-lois-informatiques-et-libertes-en-france-en-europe-et-dans-le-monde. Consulté le 11 avril 2014.

[259] Recommandation n° R (97) 5 du Comité des ministres aux États membres sur la protection des données

3. La recommandation n° R (97) 5

Compte tenu de la délicatesse[260] du sujet relatif aux traitements de données médicales dans la société moderne dominée par l'outil informatique, le Comité des ministres du Conseil de l'Europe a adopté le 13 février 1997 la recommandation n° R (97)5 relative à la protection des données médicales. Ce texte, constitue une mise à jour de la recommandation n° R (81)[261] relative à la réglementation applicable aux banques de données médicales automatisées. La recommandation n° R (81) apparaissait comme désuète face aux « *progrès accomplis dans les sciences médicales et les développements intervenus dans la technologie de l'information depuis 1981*[262] *»*.

La convention 108 ayant une vocation générale, elle a été complétée par toute une collection de textes destinés à traduire les principes de base qu'elle contient pour des secteurs spécifiques d'activité. Dans le domaine des données de santé, en plus de la recommandation n° R (97) 5, a été adoptée, le 30 septembre 1997, la recommandation n° R (97) 18 concernant la protection des données à caractère personnel, collectées et traitées à des fins statistiques. Celle-ci remplaçait la recommandation R (83) 10[263] du 23 septembre 1983 relative à la

---

médicales.
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=637549&SecMode=1&DocId=839736&Usage=2. Consulté le 11 avril 2014.

[260] *« Conscient du fait que le traitement automatisé des données médicales par des systèmes d'information est de plus en plus répandu non seulement pour les soins médicaux, la recherche médicale, la gestion hospitalière et la santé publique, mais également en dehors du secteur des soins de santé;*

Convaincu de l'importance que la qualité, l'intégrité et la disponibilité des données médicales revêtent pour la santé de la personne concernée et de ses proches ;

Conscient du fait que les progrès des sciences médicales dépendent dans une large mesure de la disponibilité des données médicales des individus ;

Persuadé qu'il est souhaitable de réglementer la collecte et le traitement des données médicales, de garantir le caractère confidentiel et la sécurité des données à caractère personnel relatives à la santé, et de veiller à ce qu'il en soit fait un usage respectant les droits et les libertés fondamentales de l'individu, notamment le droit à la vie privée;

Conscient du fait que les progrès accomplis dans les sciences médicales et les développements intervenus dans la technologie de l'information depuis 1981 nécessitent la révision de plusieurs dispositions de la Recommandation n° R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées,»

[261] Recommandation n° R (81) du 23 janvier 1981 relative à la réglementation applicable aux banques de données médicales automatisées. https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet. CmdBlob Get&InstranetImage=599533&SecMode=1&DocId=670462&Usage=2. Consulté le 28 avril 2014.

[262] 8éme paragraphe du préambule de la recommandation N° R (97) 5 du 13 février 1997 du Conseil de l'Europe.

[263] Recommandation R (83) 10 du 23 septembre 1983 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques. https://wcd.coe.int/com.instranet.InstraServlet ?

protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques, mais de façon partielle. Ce texte, bien que reconnaissant les principes de la convention 108, notamment celui de l'interdiction de traitement des données sensibles, entre davantage dans le cadre des exceptions reconnues à ce principe[264]. Nous nous intéresserons donc, à cette étape de l'étude, uniquement à la recommandation n° R (97) 5.

Le préambule de la recommandation R (97) 5 reprend les principes fondamentaux[265] de la Convention mais elle met un accent particulier sur la gestion des données médicales par les technologies de l'information en évolution et insiste sur le renforcement de leur protection. Ainsi, cette recommandation, malgré son caractère non contraignant, s'évertue à insister sur l'interdiction du traitement[266] sous le point 3 consacré au respect de la vie privée : «*Les données médicales ne peuvent être collectées et traitées que conformément aux garanties appropriées qui doivent être prévues par le droit interne».*

Il faut rappeler que la recommandation n° R (97) 5, comme toute recommandation d'une organisation internationale, dans la hiérarchie des normes juridiques n'a pas de force contraignante[267]. Les recommandations aux gouvernements des États membres adoptées par le

---

command=com.instranet.CmdBlobGet&InstranetImage=602932&SecMode=1&DocId=680154&Usage=2. Consulté le 28 avril 2014.

[264] Considérant 4 de la recommandation n° R (97) 18: « *Constatant le développement progressif des normes juridiques nationales et supranationales tant en matière d'activités statistiques que dans le domaine de la production de données à caractère personnel ; rappelant à cet égard les principes généraux relatifs à la protection des données de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Strasbourg 1981, série des traités européens n° 108) ; rappelant également les dérogations admises à travers des activités statistiques dans la convention à l'égard de l'exercice, par les personnes concernées, certains droits énoncés dans la Convention* ; »

Point 4.8 de la recommandation n° R (97) 18 : « *Si des données sensibles sont traitées à des fins statistiques, ces données devraient être collectées sans que les personnes concernées soient identifiables. Si l'objectif légitime et spécifique d'un traitement de données sensibles à des fins statistiques rend nécessaire le fait que les personnes concernées soient identifiées, le droit interne doit prévoir des garanties appropriées, y compris des mesures spécifiques pour séparer les données d'identification, dès la collecte, sauf si cela est manifestement déraisonnable ou infaisable.* » https : //wcd.coe.int/com.instranet.InstraServlet?command=com. instranet.CmdBlobGet&InstranetImage=2001721&SecMode=1&DocId=578636&Usage=2. Consulté le 11 avril 2014.

[265]*« Rappelant les principes généraux relatifs à la protection des données de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Série des traités européens, n° 108), notamment son article 6 qui énonce que les données à caractère personnel relatives à la santé ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées »*

[266] Recommandation n° R (97) 5, 3.2 Respect de la vie privée.

[267]Voir, à ce sujet, une analyse du Professeur VIRALLY, Michel. *La valeur juridique des recommandations des organisations internationales* in annuaire français de droit international. Volume 2, 1956, pp 66 – 96. Que ce soit les recommandations d'ordre intérieur ou celles adressées à un État membre, l'opinion générale est que la recommandation se définit par son absence de force obligatoire. Mais, la constitution d'une organisation peut

Comité des ministres constituent uniquement des normes de référence. Tout comme les résolutions, déclarations, accords, délibérations, conclusions, codes de conduite, actions ou les positions communes, les recommandations ont essentiellement une valeur politique. Elles expriment la position des institutions sur un problème donné et éclairent la Cour de justice quant à l'appréciation de la portée d'un acte juridique ayant une force contraignante. La recommandation n° R (97) 5 a donc une valeur incitative pour les États membres et ses effets dépendent alors de la volonté des États signataires de coopérer avec le Conseil de l'Europe.

A travers la disposition du point 3.2 sus-cité, la recommandation vient renchérir la responsabilité des États membres quant aux mesures à prendre pour garantir la sécurité des données médicales que la Convention avait déjà prévues. Cette insistance a sans doute eu pour effet d'encourager les États membres de l'Union à transposer la directive dans leurs lois nationales respectives. Ainsi, en 2004, la loi informatique et libertés, en France va connaître d'importantes modifications dont celles relatives aux données de santé.

B. La source nationale : la loi française informatique et libertés

Le respect de la vie privée a été consacré par tous les principaux textes internationaux, mais leur proclamation de ce principe qui suppose une non-ingérence, une abstention de l'État ou de toute autre personne n'est pas suffisante pour protéger l'individu face au développement de l'informatique. C'est le sens de la loi informatique et libertés qui a institué la CNIL pour en assurer la régulation. Ce texte reste la base du système français en matière de traitement de données personnelles.

Dans sa version initiale du 6 janvier 1978, la loi informatique et libertés disposait en son article 31 alinéa 1 qu' « *il est interdit de mettre ou de conserver en mémoire informatisée, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales des personnes* ». Les données sensibles visées étaient d'essence intellectuelle (les origines raciales, les opinions politiques, philosophiques religieuses ou les appartenances syndicales). Lors de l'adoption de la loi informatique et

donner plus de force à une recommandation (exemple de l'article 19, paragraphe 6 de la constitution de l'OIT). Il faut alors retenir que dans le cas d'espèce, *« la recommandation est un instrument de collaboration entre l'organisation et ses membres en vue de la réalisation des fins sociales: collaboration qui postule l'existence d'une volonté de coopérer chez les uns comme chez les autres »*.

libertés en 1978, l'une des préoccupations majeures du législateur était la protection des libertés individuelles et collectives face aux menaces que le développement et l'interconnexion des fichiers, combinés avec l'utilisation d'un identifiant unique faisait peser sur elles. Le législateur avait privilégié la protection des libertés par rapport à celle de la vie privée qu'il estimait ne pas être suffisamment menacée par les progrès de l'informatique. En 1995, la directive européenne, bien qu'inspirée de la loi de 1978, complète la liste des données sensibles en ajoutant d'autres types de données ayant, plutôt, lien avec l'intimité morale et physique des personnes. Il s'agit notamment, de données relatives aux origines ethniques, à la vie sexuelle et celles qui concernent la santé. Et plus tard, en 2004, lors de la modification de la loi informatique et libertés, la transposition de la directive a permis l'introduction des données médicales comme données sensibles et donc entrant dans le cadre des informations dont le traitement est interdit par principe.

Avant la transposition de la directive en 2004, la CNIL avait déjà pris des décisions allant dans le sens de la sensibilisation des professionnels de santé au travers d'un type particulier de délibération[268]. La loi informatique et libertés avait également fait l'objet de deux modifications relatives à des traitements particuliers de données de santé. La première, en 1994[269], a ajouté un chapitre portant sur le traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé et la seconde en 1999[270] a complété la loi par un chapitre portant sur le traitement de données de santé à caractère personnel à des fins d'évaluation, d'analyse des pratiques ou des activités de soins et de prévention.

Désormais, l'article 8.I de la loi informatique et libertés prévoit: *« 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 »*. C'est une reprise de l'article 8 de la directive. Le fondement de cette interdiction réside dans la volonté du législateur de consacrer dorénavant plus d'attention à la

[268] Délibération 97-008 portant adoption *d'une recommandation sur le traitement de données de santé à caractère personnel*. JORF n°86 du 12 avril 1997. p. 5606. La CNIL y précisait que les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt du patient et dans des conditions déterminées par la loi pour des besoins de santé publique mais que dès lors l'exploitation à des fins commerciales est proscrite.

[269] 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 no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. JORF n°152 du 2 juillet 1994 page 9559. NOR : RESX9200045L.

[270] Loi n° 99-641 du 27 juillet 1999, portant *création d'une couverture maladie universelle*. JORF. n° 172 du 28 juillet 1999 p. 11229. NOR : MESX9900011L.

protection de la vie privée. Dans sa version de 2004, la loi étend également, l'interdiction des traitements de données médicales aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers. C'est encore une innovation[271] par rapport à la loi de 1978 qui interdisait uniquement la mise ou la conservation en mémoire informatisée des données dites « sensibles ».

La loi informatique et libertés est soutenue dans la répression du traitement illégal des données médicales par le code pénal. En effet, l'article 226 - 19 du code pénal qui dispose que : *« le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée sans le consentement exprès de l'intéressé, des données (...) qui sont relatives à la santé (...), est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».* L'article 226 - 23[272] du code pénal a également tenu compte de l'extension précitée en incluant les traitements non informatisés dans le champ d'application des dispositions de l'article 226 - 19 du code pénal.

Comme on le constate, beaucoup de dispositions ont été prises tant au plan international que par la législation française pour prohiber le traitement des données sensibles et surtout celles relatives à la santé. Mais, les législateurs restent objectifs car ils n'ignorent pas que leur traitement peut s'avérer nécessaire dans l'évolution de la société. C'est ce qui justifie que des exceptions soient admises au principe.

Paragraphe 2 : Les exceptions au principe

La directive 95/46 autorise chaque État à prévoir d'autres dérogations que celles qu'elle a émises à condition qu'il mette en place les garanties nécessaires[273]. Aussi, la France prescrit-elle le traitement des données médicales dans d'autres hypothèses que celles précédemment prescrites par la Directive.

---

[271] C'est l'application de l'article 2 de la loi informatique et libertés qui précise que le domaine d'application de ladite loi s'étend aux traitements automatisés de données à caractère personnel mais également *« aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers ».*

[272] Code pénal. Article 22 -23: *« les dispositions de l'article 226–19 sont applicables aux traitements automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles* ».

[273] Conseil d'État, 5 juin 1987, Contentieux n° 59674, http://www.legifrance.gouv.fr/ ou M. Kaberseli, Dalloz 1987-416. RDA 1987, n° 87, p. 392.

A. Les exceptions issues de la directive 95/46 du 24 Octobre 1995

La directive cite les situations dans lesquelles les États membres peuvent lever l'interdiction de traitement des données sensibles et, en l'occurrence, les données médicales. Mais elle laisse toute latitude aux États de rester plus souples ou plus rigides quant à ces exceptions. Ce sont les hypothèses suivantes :

1. Le consentement explicite de la personne concernée

Lorsqu'une personne est consentante pour le traitement de ses données de santé, la directive donne aux États membres la possibilité de renoncer à prohiber l'opération. Mais alors, doit-on se limiter à un consentement donné de n'importe quelle manière ou l'accord doit-il revêtir une forme particulière ?

A cette question, la directive répond que le consentement doit être «*explicite*[274]» pendant que la loi informatique et libertés emploie l'adjectif «*exprès*[275]». Ces deux qualificatifs traduisant l'idée d'expression claire, précise et sans équivoque de sa volonté, il faut exclure la possibilité de donner un accord implicite. L'écrit signé est, en général, la méthode utilisée par plusieurs législations pour répondre à cette exigence même si la loi n'est pas précise à ce sujet. Cela constitue juste une mesure de prudence destinée à servir d'élément de preuve au responsable du traitement en cas de litige. L'individu peut, néanmoins, exprimer son consentement par d'autres moyens qui pourront produire les mêmes effets juridiques qu'un accord exprès, en fonction du contexte. Ainsi en est-il d'une action positive comme un don fait par une personne dans le but de participer à la lutte contre une maladie dont elle-même est victime ou du fait de demander à être traité dans un lieu reconnu comme étant un centre de recherche. Son consentement est alors présumé être donné pour le traitement de ses données médicales en vue de recherches. Le consentement donné établit un lien juridique entre le titulaire des données et le responsable du traitement ; c'est ce pourquoi il est essentiel de préciser les

[274] Selon le dictionnaire Robert, l'adjectif « explicite » désigne ce qui est réellement exprimé, formulé et « exprès », ce qui exprime formellement la pensée, la volonté de quelqu'un.

[275] Article 8, II. 1° de la loi informatique et libertés : « *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 (…)* ».

conditions (forme, fond, capacité) qui entourent l'accord donné. La CNIL a opté pour un accord nécessairement écrit mais en se gardant, dans son 7ème rapport d'activité[276], de préciser que même si l'écrit comporte un certain intérêt du fait de son formalisme, il ne garantit pas irrévocablement la légitimité du consentement. Ce dernier peut avoir été « *extorqué par l'habileté du ficheur* » ou même à l'insu du titulaire des données alors que la validité du consentement est fondé sur « *la réalité de l'accord* ». C'est pourquoi, la Commission estime que l'écrit constitue une présomption simple qui devrait donc faire l'objet d'un *« réexamen en fonction de chaque cas d'espèce »* par elle et ensuite, par les tribunaux, en dernier ressort.

La directive et la loi informatique et libertés n'ont pas été explicites quant aux conditions de recueil du consentement lorsque la personne concernée est un mineur ou un incapable en général. Il faut croire que cela ne leur a pas semblé nécessaire étant donné qu'il existe d'autres textes[277] qui ont traité le problème de la capacité juridique en droit des obligations. En droit de la santé, l'article R. 4127-42 du code de la santé publique stipule : « *un médecin appelé à donner des soins à un mineur ou un majeur protégé doit s'efforcer de prévenir ses parents ou son représentant légal et d'obtenir le consentement.* » Cette solution a été conçue pour les actes médicaux et non pour la gestion des données médicales. Toutefois, l'application de la solution au traitement de données de santé peut s'expliquer par le lien étroit qui existe entre la collecte et le traitement de celles-ci et l'acte médical qui suit lorsqu'un malade est inconscient alors qu'il est vital pour lui de subir un acte médical délicat. En effet, en la matière, la jurisprudence a forgé une théorie dite *« théorie des protecteurs naturels*[278] *»* qui oblige le médecin à requérir le consentement d'une personne ayant un lien particulier avec

[276] Le contrôle de la CNIL doit donc porter également sur le fond même de l'affaire c'est-à-dire sur la réalité du consentement. Il convient d'éviter que le contrôle de l'existence d'un document écrit ne se substitue subrepticement au contrôle de la réalité de l'accord. Ce contrôle sera plus rigoureux lorsque les intéressées seront des personnes en situation d'infériorité de droit ou de fait comme un étranger non francophone auquel il est demandé de signer une autorisation écrite. 7ème rapport d'activité de la CNIL, 1er janvier 1986 – 31 décembre 1986. La documentation française 1986. p.86.

[277] En l'occurrence, les articles 1123 à 1125 concernant la capacité des parties contractantes ; article 389-3 et 450 du code civil relatifs à la représentation légale.

[278] Sur *«la théorie des protecteurs naturels »*, la jurisprudence de la Cour de cassation du 8 Novembre 1955, l'observation de SAVATIER. René. JCP 1955, II, 9014. *« avant d'entreprendre un traitement ou de procéder à une opération chirurgicale, le médecin est tenu, hors le cas de nécessité, d'obtenir le consentement libre et éclairé du malade, ou dans le cas où il serait hors d'état de le donner, celui des personnes qui sont investies, à son égard d'une autorité légale, ou que leur liens de parenté avec lui désignent comme des protecteurs naturels »*. Cette théorie a été émise pour la première fois par un arrêt de la cour d'Appel de Lyon du 17 novembre 1952, JCP 1953, II, 7541.

l'intéressé avant de procéder à une opération. Le recours à cette théorie dans le cadre de recueil des données médicales se justifie par le fait que celui-ci précède nécessairement la réalisation de l'acte médical. L'urgence et la nécessité du second impliquant celles du premier, il serait absurde de s'attarder à attendre absolument le consentement du malade avant de procéder à tout traitement de ses données ou de transmettre ses données à un autre médecin dont l'intervention est requise.

L'article R 1111-1[279] du code de la santé publique conforte l'argument de la transposition d'une règle prévue pour les actes de soins dans le domaine du traitement des données. Il confie la demande d'accès aux informations relatives à la santé d'un mineur ou d'un majeur incapable à la personne ayant l'autorité parentale ou le tuteur ou le cas échéant, au médecin qu'une de ces personnes a désigné comme intermédiaire.

Tout comme la loi française, la directive laisse à la discrétion de la personne concernée le choix de l'autorisation de traitement de ses données de santé. Cela la met donc en situation de décider, en fonction des intérêts en jeu, l'opportunité d'une telle opération. Cette position a même fait l'objet d'une proposition de définition du droit à la vie privée par le Conseil de l'Europe dans sa résolution 1165[280]. Pour le Conseil, en effet, chaque individu doit avoir *« le droit de contrôler ses propres données »* face à l'apparition des nouvelles technologies de la communication qui permettent de stocker et d'utiliser des données personnelles. Or, d'une manière générale, les données de santé se recueillent dans un domaine (la médecine) très souvent inconnu du patient ; ce qui nous amène à nous interroger sur la valeur de l'autodétermination informationnelle[281] de la personne concernée. Dispose-t-elle du recul

[279] « *L'accès aux informations relatives à la santé d'une personne, (…) détenues par un professionnel de santé, un établissement de santé ou un hébergeur agréé en application de l'article L 1111-8, est demandée par la personne concernée, son ayant droit en cas de décès de cette personne, la personne ayant l'autorité parentale, le tuteur ou, le cas échéant, par le médecin qu'une de ces personnes a désigné comme intermédiaire*.»

[280] Conseil de l'Europe. Résolution 1165 du 26 juin 1998, droit au respect de la vie privée (24e séance), Point 5.

[281] L'autodétermination informationnelle est la maîtrise qu'a un individu sur l'information qui le concerne. C'est « le pouvoir reconnu à l'individu (...) de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués. C'est un attribut du droit de la personnalité qui est appelée droit à la maîtrise des données personnelles. La cour constitutionnelle fédérale allemande a donné cette définition de l'autodétermination informationnelle en décembre 1983 à l'occasion de la décision de l'inconstitutionnalité de la loi sur le recensement ».

Voir, à ce propos, une analyse d'Yves POULLET et Antoinette ROUVROY montrant l'autodétermination informationnelle comme un concept clé intitulée *le droit à l'autodétermination informationnelle et la valeur du développement personnel une réévaluation de l'importance de la vie privée pour la démocratie*. http://www.crid.be/pdf/public/6050.pdf. Consulté le 29 mars 2014.

Voir également des éléments de réflexion du Conseil de l'Europe sur la convention n°108 portant sur l'autodétermination informationnelle à l'ère d'Internet. *Rapport sur l'application de principes de protection des*

suffisant ou a-t-elle vraiment le choix lorsque le traitement proposé vise à œuvrer à l'amélioration de son état de santé ou à faire avancer la science ?

Pour certains auteurs[282], le consentement en tant que *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*[283], s'en trouve, dans ces conditions, quelquefois vicié[284]. Tout dépend du cas d'espèce et des dispositions prises par le droit pour protéger la personne concernée. La technique du blanc-seing[285] est interdite alors que le consentement peut être donné à l'avance c'est-à-dire indépendamment du moment où les données sont recueillies. Le consentement ne rend légitime le traitement que si celui-ci reste dans le cadre de la finalité pour laquelle l'accord avait été initialement donné alors que l'accord donné ne rend pas, pour autant, règlementaire l'intérêt poursuivi par le responsable du traitement quand celui-ci était préalablement illicite. Par ailleurs, le consentement peut être retiré mais cela ne rend pas illégitimes des opérations passées si elles ont été effectuées dans des conditions légales (notamment dans le respect de la finalité et des conditions légales d'obtention du consentement).

---

données aux réseaux mondiaux de télécommunications. Strasbourg, le 18 novembre 2004. http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD(2004)04_Poullet_report.pdf . Consulté le 2 juin 2009.

[282] HERVEG, Jean. *Introduction à la protection des données médicales en droit européen : interdiction des traités et exceptions.* In Xe séminaire d'actualité de droit médical. P. 187

[283] Article 2, h). de la directive 95/46/EC.
La recommandation de l'OCDE sur les biobanques et bases de données de recherche en génétique humaine de 2009 propose des définitions à titre indicatif mais qui permettent de comprendre combien le consentement peut recouvrir un contenu différent d'un domaine à l'autre ou encore d'un individu majeur à un mineur.
Consentement éclairé : Processus qui permet de présenter à un participant ou à un décideur substitut des informations relatives à la recherche prévue, lui donne la possibilité de poser des questions, puis recueille et consigne son approbation spécifique.
Assentiment : Ce terme est utilisé dans le contexte de la participation d'un enfant à une recherche. Même si un enfant ne peut être considéré comme légalement compétent pour consentir à participer à une recherche, il peut être considéré comme compétent pour donner son assentiment, c'est-à-dire son avis sur son souhait de participer à la recherche. *Lignes directrices de l'OCDE relatives aux biobanques et bases de données de recherche en génétique humaine*. p. 53-54 www.oecd.org/dataoecd/41/1/44054924.pdf. Consulté le 22 mai 2014.

[284] La CNIL a exprimé sa réticence à l'utilisation de consentement comme seule justification du traitement des données sensibles. Elle considère d'une part que les personnes ne mesurent pas toujours les conséquences du traitement de leurs données et d'autre part que, dans certains cas, leur consentement peut risquer d'être un peu « forcé ». Le consentement peut devenir en quelque sorte une « solution de facilité » pour le responsable du traitement. Ceci peut entraîner la collecte et le traitement de données sensibles alors qu'en réalité, soit le responsable du traitement n'en a pas réellement besoin, soit l'utilisation qui pourrait être faite de ces données est trop large. JOB, Jean-Marie. *La loi informatique et libertés et des données de santé.* Revue Lamy droit de l'immatériel du 1er janvier 2008. N° 34. P.3

[285] Signature apposée à l'avance sur un document dont la rédaction sera ultérieurement complétée par la personne à laquelle le titre sera remis.

Malgré tous ces garde-fous, lorsqu'il estime que les garanties adéquates ne sont pas réunies, chaque État est autorisé par la directive à prévoir que l'interdiction de traitement des données médicales ne puisse pas être levée par le simple consentement de la personne concernée[286]. C'est une importante restriction à cette dérogation qui a été reprise par la loi française qui dispose quant à elle : *«(…) sauf dans le cas où la loi prévoit que l'interdiction visée (…) ne peut pas être levée par le consentement de la personne concernée*[287] *»*. Ainsi, les articles L 1141-1 à L1141-3 du Code de la santé publique interdisent-ils le traitement, la prise en compte des résultats des tests génétiques aux compagnies d'assurance même si ceux-ci leur ont été transmis par la personne concernée ou avec son accord.

En dehors du consentement de la personne concernée, les États membres peuvent prévoir des exceptions «*pour répondre à des besoins spécifiques*[288]*»*. Celles-ci font l'objet d'énumération sous forme d'hypothèses dans l'article 8[289] de la directive précité.

2. La nécessité de préservation d'intérêts vitaux

Le principe de l'interdiction est également écarté lorsque les traitements sont nécessaires à la sauvegarde de la vie humaine alors que la personne concernée ne peut y donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle.

Tandis que la directive légitime le traitement des données de santé lorsqu'il est nécessaire de défendre les « intérêts vitaux » de la personne concernée ou d'une autre personne[290], la loi informatique et libertés traite de « la sauvegarde de la vie humaine », puis, revient au seul individu concerné[291]. Même si les deux textes emploient des termes différents,

[286] Article 8,2. a) de la directive 95/406/EC.

[287] Article 8, 1° de la loi informatique et libertés.

[288] Considérant 33 de la directive.

[289] Article 8. 2, b) à e) et .3 de la directive.

[290] « *Le paragraphe 1 ne s'applique pas lorsque : le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement*. » Article 8, 2. c).

[291] « *Dans la mesure ou la finalité du traitement l'exige pour certaines catégories de données, ne sont pas soumis à l'interdiction prévue au I : 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.* » Article 8, II. 2°.

l'utilisation préalable de l'expression « la sauvegarde de la vie humaine » par la loi informatique et libertés rejoint l'idée de la directive du fait de son caractère général. Ces deux législations ont donc tendance à étendre la dérogation à l'interdiction de traitement des données médicales d'un individu au consentement d'un tiers pour la sauvegarde de sa vie. La notion d'intérêt vital utilisée par la directive a été remplacée dans la loi française par celle de la « sauvegarde de la vie» parce que l'«intérêt vital» a été jugé trop angliciste par le rapporteur du Sénat[292] (il résulte de la traduction littérale « *vital interest* ») et ambigu dans la mesure où il peut désigner un intérêt essentiel ne se rattachant pas à la survie et de la personne concernée. L'expression vise la situation de péril imminent à la vie d'une personne physique. Ce péril imminent autorise donc un tiers (proche mais pas nécessairement allié au sens juridique du terme) à consentir au traitement des données en lieu et place de l'intéressé. Aucun de ces textes ne précise les cas dans lesquels cela pourrait être possible. Mais le rapport du Sénat relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel de 2003 indique que ce « *cas vise les fichiers des organisations humanitaires sur les personnes arrêtées ou disparues, ainsi que les situations d'urgence notamment en matière de santé dans lesquels le consentement de la personne concernée ne peut être recueilli, alors que sa suivi ou celle d'une personne est en jeu*[293] *»*.

On peut également, entrevoir l'hypothèse où des titulaires de l'autorité parentale ou de tuteur peuvent être concernés par les traitements de données des mineurs ou des incapables majeurs. Dans d'autres cas, on peut estimer que l'accord de la personne concernée est forcé en ce sens que le droit positif ne lui donne pas d'autres alternatives. Il est difficile d'envisager que cette dernière refuse d'autoriser le traitement de ses données médicales lorsque les intérêts vitaux d'une personne sont en jeu ; ce qui pourrait sous-tendre un «vice de consentement légalisé».

Cette seconde dérogation au principe montre que le consentement de l'intéressé jusque-là reconnu comme première exception à la prohibition de traitement n'est pas

[292] TÜRK, Alex. Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Rapport n° 218 (2002-2003). 19 mars 2003. p. 57. http://www.senat.fr/rap/l02-218/l02-2181.pdf. Consulté le 14 avril 2014.

[293] TÜRK, Alex. Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Rapport n° 218 (2002-2003). 19 mars 2003. p. 63. http://www.senat.fr/rap/l02-218/l02-2181.pdf. Consulté le 14 avril 2014.

indispensable. Il peut être relégué au second plan au profit de celui d'une tierce personne[294] face à l'urgence de la préservation d'intérêts vitaux.

La loi informatique et libertés a rajouté une condition complémentaire au consentement et à la nécessité de la sauvegarde de la vie humaine : *« dans la mesure où la finalité du traitement l'exige à certaines catégories de données »*. La directive ne prévoit pas cette condition qui se trouve être une réelle restriction au « blanc-seing » que pourrait constituer un consentement facilement obtenu. Cette exigence imposée par la loi française a le mérite d'insister sur le principe de finalité qui est, d'ailleurs, l'un des principaux fondements de la directive.

3. Le cas des traitements portant sur des données déjà rendues publiques ou en cas de nécessité de constatation, d'exercice ou de défense d'un droit en justice

Selon la directive l'interdiction de traiter des données médicales est encore levée lorsque les données sur lesquels porte le traitement sont manifestement rendues publiques par la personne concernée ou que le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice[295]. Toutes ces conditions font l'objet d'un seul alinéa dans les dispositions de la directive alors que la loi française informatique et libertés les cite en deux points différents[296]. Mais, l'idée demeure la même et l'essentiel est que le responsable du traitement devra avoir à faire la preuve que les données ont bien été rendues publiques par la personne concernée. En transposant la directive, la loi informatique et libertés a remédié à une lacune de l'article 31 de la loi de 1978 auquel s'est substitué l'article 8 traitant de la gestion électronique de données sensibles. Cette disposition interdit, en théorie, de conserver des données relatives aux engagements d'hommes politiques ou de dirigeants syndicaux. L'étendue de cette dérogation doit, cependant, être appréciée à la lumière du principe de finalité : elle ne signifie nullement que toute donnée sensible rendue publique par la personne

[294] Sur le consentement donné par une tierce personne lorsque la concernée n'est pas en état de l'exprimer, voir une analyse de CROELS Jean-Michel, *Le droit des obligations à l'épreuve de la télémédecine*. Thèse, PUF 2006. p. 310 – 312.

[295] Article 8. 2, e) de la directive 95/46/EC précité

[296] Article 8. II de la loi informatique et libertés : *« 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 »*.

concernée peut faire l'objet de n'importe quel traitement[297]. En outre, même manifestement rendues publiques le traitement de ces données tombe toujours dans le champ d'application de la législation en la matière et donc toutes les normes de protection applicables à leurs traitements doivent être scrupuleusement respectées. Le procédé d'anonymisation (transformation d'une donnée personnelle en une donnée non personnelle) permet, dans ce cas, de limiter les risques d'atteinte.

Les traitements portant sur des données nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ainsi autorisés par la directive, entre le cadre de l'article 25, I. 3° de la loi informatique et libertés qui les soumet à autorisation de la CNIL. En effet, « *sont mis en œuvre, après autorisation de la CNIL (...), les traitements automatisés ou non portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées* ». Dans ce contexte, la CNIL a pris une délibération[298], le 23 janvier 2014, portant création d'une autorisation unique concernant les traitements de données à caractère personnel relatifs aux infractions, condamnations ou mesures de sûretés mis en œuvre par les organismes d'assurance, d'assistance, les intermédiaires d'assurance et par l'AGIRA[299]. Cette mesure est nécessaire pour permettre aux organismes d'assurance de pouvoir assurer, conformément à loi informatique et libertés, la constatation, l'exercice ou la défense de leurs droits en justice ou la défense des personnes concernées, dans le cadre de la gestion des contentieux.

La formalité du recours à la l'autorisation de la CNIL répond ainsi aux normes de garanties appropriées qu'exige la directive de la part des États membres pour la mise en œuvre des exceptions. La lettre de l'article 8 de la directive ne requiert pas ces garanties pour les traitements sus-mentionnés, en particulier mais, il faut croire que le législateur français préfère en prévoir plus que pas assez compte tenu de la délicatesse du sujet. L'esprit de la directive, à travers les termes du considérant 54[300], va, d'ailleurs, dans le sens de cette

[297] TÜRK, Alex. Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Rapport n° 218 (2002-2003). 19 mars 2003. p. 62. http://www.senat.fr/rap/l02-218/l02-2181.pdf. Consulté le 14 avril 2014.

[298] Délibération 2014-015 du 23 janvier 2014. JORF n° 0032 du 7 février 2014. Texte n° 75. NOR : CNIX1402984X.

[299] Association pour la gestion des informations sur les risques en assurance.

[300] « *Considérant que,, au regard de tous les traitements mis en œuvre dans la société, le nombre de ceux présentant de tels risques particuliers devait être très restreint ; que les États membres doivent prévoir pour ces*

généralisation et de la procédure adoptée.

4. Dans le cadre des activités d'un organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale

Aux termes de l'article 8.2 de la directive, sont autorisés les traitements effectués dans le cadre de leurs activités légitimes et avec des garanties appropriées par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme et aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Il s'ensuit donc que pour pouvoir se prévaloir de cette autorisation de traiter les données médicales, le responsable de traitement doit être une personne soumise à une obligation de secret professionnel. S'agissant des associations ou fondations, ces organismes doivent poursuivre un but non lucratif et avoir un objet social qui permette l'exercice de libertés fondamentales spécifiques[301]. C'est le cas des églises, partis politiques et organismes d'opinion qui peuvent avoir un registre informatisé. Le fondement de cette disposition est la liberté d'opinion, d'association et le risque que prend volontairement le membre en privilégiant d'autres intérêts. Cette dérogation peut se heurter à de plus grandes valeurs en balance, notamment l'intérêt général, la santé, l'intérêt scientifique. D'ailleurs, la directive ne manque pas d'insister sur le fait que ces traitements doivent se faire « *avec des garanties appropriées* » alors que la législation française se contente de préciser que ces traitements doivent concerner les seules données correspondant à l'objet dudit organisme. Finalement, l'article 22 de la loi informatique et libertés modifiée exonère ces traitements de toute formalité de déclaration préalable dès lors qu'ils remplissent les conditions fixées par l'article

---

traitements, un examen préalable à leur mise en œuvre, effectué par l'autorité de contrôle ou par le détaché à la protection des données en coopération avec celle-ci; que, à la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis pour autoriser le traitement des données ; qu'un tel examen peut également être effectué au cours de l'élaboration soit d'une mesure législative du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et précise les garanties appropriées ; »

[301] Considérant 33 de la directive.

8, II. 3[302]. De ce point de vue, le législateur français est plus souple que les rédacteurs de la directive. On pourrait en déduire, mais sans conviction, que le droit français fait primer la liberté d'opinion sur la protection des données sensibles.

5. Dans le cadre de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé

Les articles 8.3 de la directive et 8. II, 6° de la loi informatique et libertés lèvent l'interdiction de traiter les données médicales lorsque le traitement de données est nécessaire pour la médecine préventive, les diagnostics médicaux, l'administration de soins ou de traitements et que le traitement de ces données est effectué par un professionnel de la santé soumis au secret professionnel ou par une personne également soumise à une obligation de secret équivalente.

Suivant les termes du considérant 33 de la Directive, cette exception s'étend à une finalité thérapeutique au sens large du terme *: «des fins relatives à la santé*[303]*»*. Ce qui implique la gestion des services de santé, notamment tous les actes accessoires nécessaires pour assurer l'octroi de soins de santé telle que la réception des patients, le secrétariat médical, le service informatique, etc. Les finalités de sécurité sociale ou de santé publique ne sont, par contre, pas prises en compte dans cette hypothèse-ci. Elles font l'objet d'un autre type d'exception entrant dans le cadre des motifs d'intérêt public.

La condition pour que cette dérogation soit admise réside dans le fait que le traitement soit effectué par un praticien de la santé soumis par son droit national ou par d'autres réglementations internes édictées par les autorités nationales compétentes au secret

[302] Voir supra: *les dispenses expresses de la loi*.

[303] Le groupe de l'article 29 estime que cette dérogation couvre uniquement les traitements de données médicales dans le but spécifique de fournir des services de santé à caractère préventif, diagnostic, thérapeutique ou de postcure et de gérer ce service de soins de santé, par exemple pour la facturation, la comptabilité ou les statistiques. La dérogation ne couvre pas un traitement ultérieur non nécessaire à la fourniture directe de ces services, notamment l'utilisation des données pour la recherche médicale, le remboursement ultérieur des frais par un régime d'assurance maladie ou le recouvrement de créances. Échappent également au champ d'application de l'article 8, paragraphe 3, d'autres opérations de traitement de données dans des domaines tels que la santé publique et la protection sociale, visant notamment à assurer la qualité et la rentabilité des procédures utilisées pour régler les demandes de prestations et des services dans le régime d'assurance maladie, puisque ces opérations sont mentionnées au considérant 34 de la directive en tant qu'exemples d'invocation de l'article 8, paragraphe 4. Document de travail a adopté le 15 février 2007 par le groupe 29 sur *le traitement des données à caractère personnel relatives à la santé contenue dans les dossiers médicaux électroniques (DME)*, P. 11. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_fr.pdf. Consulté le 5 avril 2014.

professionnel, ou par une autre personne également soumise à une obligation de secret équivalente. Ainsi, le texte n'exige pas que le professionnel de santé soit le seul habilité à collecter et à traiter les données. Une autre personne soumise à une obligation de secret professionnel similaire par voie statutaire ou par stipulation contractuelle peut procéder au traitement. A ce niveau, Me HERVEG[304] se pose la question de savoir si le consentement de la personne concernée n'est pas ainsi confondu avec le consentement aux soins prodigués. Le groupe 29[305] ou (groupe de travail de l'article 29) a répondu que l'acceptation de suivre le traitement médical ne constitue pas automatiquement un consentement au traitement de ses données médicales, en particulier, en ce qui concerne la communication ou le transfert à un tiers[306]. En outre le professionnel n'est pas tenu par ses textes de collecter et de traiter que les données des personnes qu'il soigne. Il peut donc se permettre de recueillir et traiter des données appartenant à d'autres personnes si cela est nécessaire à son activité. On peut donc croire que ce dernier pourra alors recourir à des données appartenant à des ascendants, des descendants ou des conjoints si cela s'avère nécessaire pour poser un diagnostic ou pour inciter le patient à sensibiliser ses proches pour des maladies héréditaires ou liées à une caractéristique génétique.

Cette dérogation a le mérite de permettre aux professionnels de santé de pouvoir collecter et traiter les données de leurs patients en toute quiétude ; ce qui s'avère totalement indispensable pour la bonne marche de leur métier.

Il s'agit de l'exception la plus importante à l'interdiction du traitement de données

---

[304] HERVEG, Jean. *Introduction à la protection des données médicales en droit européen : Interdiction de traiter et exceptions in Dossier médical et données médicales de santé: protection de la confidentialité, conditions d'accès, échanges pour les soins et la recherche. Xème séminaire d'actualité de droit médical*. P. 193

[305] Le groupe article 29 a été institué par la 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 circulation de ces données. Ayant un caractère consultatif et agissant en toute indépendance, le groupe est composé de représentants des autorités nationales chargées de la protection des données, du CEPD (Contrôleur européen de la protection des données) et de la Commission européenne. Il constitue une plate-forme très importante pour la coopération, et ses principales missions consistent à : donner à la Commission des avis d'experts des États membres sur des questions relatives à la protection des données ; promouvoir l'application uniforme de la directive 95/46 dans tous les États membres de l'Union européenne ainsi qu'en Norvège, au Liechtenstein et en Islande ; donner à la Commission un avis sur tout acte communautaire (premier pilier) ayant une incidence sur le droit à la protection des données à caractère personnel. COMMISSION EUROPEENNE. *Groupe de travail «Article 29»*. http://ec.europa.eu/justice/data-protection/article-29/. Consulté le 3 avril 2014.

Dès l'entrée en vigueur du nouveau règlement européen, le groupe de travail de l'article 29 sera remplacé par le secrétariat du Comité européen de la protection des données.

[306] Document de travail adopté le 15 février 2007 par le groupe 29 sur les traitements de données à caractère personnel relatif à la santé contenue dans les dossiers médicaux électroniques(DME), p. 9, note infrapaginale 10.

sensibles. Elle permettra de compenser l'effet de l'ajout de données de santé à la liste des données sensibles, tout en encadrant strictement le traitement de ces données, désormais restreint à des finalités et à des destinataires étroitement définis. La limitation par la Directive de personnes autorisées à effectuer le traitement de données constitue une garantie essentielle, et intégrée au projet français de « réseau santé social » à travers la mise en place d'une « carte des professionnels de santé » permettant de différencier les niveaux d'habilitation des personnes ayant accès au réseau[307].

6. Dans le cadre de traitements justifiés par l'intérêt général

Cette disposition de la Directive tend à établir un juste équilibre entre la protection des droits de la personne concernée, d'un côté, et les intérêts légitimes des responsables du traitement des données et des tiers et l'éventuel intérêt public, de l'autre. Elle permet aux États membres de prévoir d'autres dérogations à l'interdiction du traitement de catégories de données sensibles à certaines conditions : *« Sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle.»*

C'est la mise en application du considérant 34 qui stipule: *« Considérant que les États membres doivent également être autorisés à déroger à l'interdiction de traiter des 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 - particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie - et tels que la recherche scientifique et les statistiques publiques; qu'il leur incombe, toutefois, de prévoir les garanties appropriées et spécifiques aux fins de protéger les droits fondamentaux et la vie privée des personnes;»*. Ainsi, si un État membre entend faire usage de cette possibilité, la dérogation doit être inscrite dans une disposition légale ou une décision de l'autorité de contrôle. En

[307] TÜRK, Alex. *Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.* Rapport n° 218 (2002-2003). 19 mars 2003. p. 63. http://www.senat.fr/rap/l02-218/l02-2181.pdf. Consulté le 16 avril 2014.

France, la loi informatique et libertés prévoit en son article 8, *IV. « De même, ne sont pas soumis à l'interdiction 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 »* conformément à cet article 8 paragraphe 4 de la Directive.

Ce traitement de données sensibles doit être justifié par un important motif d'intérêt public. Le considérant 34 de la directive en donne des exemples de domaines dans lesquels des cas d'*« intérêt public important »* sont particulièrement susceptibles de se manifester. Il s'agit, notamment, « *des domaines de la santé publique et de la sécurité sociale dans le but d'assurer la qualité et la rentabilité quant aux procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie* ». C'est, aussi le cas des domaines « *de la recherche scientifique et des statistiques publiques* ».

Analysant cette disposition de la directive, le groupe de travail de l'article 29 fait les précisions suivantes : *« dans chacun de ces cas, il faut que l'ensemble du traitement de données faisant l'objet de la dérogation présente un intérêt public sérieux pour l'État membre et que ce traitement soit nécessaire à la lumière de cet intérêt public important. Toute mesure de ce type doit être proportionnée, c'est-à-dire qu'aucune autre mesure moins dérogatoire ne doit être disponible. En outre, pour que toute atteinte au droit à la vie privée et à la famille soit légitime, elle doit être conforme à l'article 8 de la convention européenne de sauvegarde des droits de l'homme*[308] *et doit être interprétée à la lumière de la jurisprudence de Strasbourg: elle doit être « prévue par la loi » et être « nécessaire dans une société démocratique »* à des fins d'intérêt public. La Cour de Strasbourg a insisté, à plusieurs reprises[309] sur le fait que la loi autorisant l'ingérence doive indiquer la portée d'un tel pouvoir discrétionnaire conféré aux autorités compétentes ainsi que les modalités de son exercice de

[308] « *1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

[309] Arrêts Leander c/ Suède du 26 mars 1987, § 48 CEDH, Leander c. Suède, série A n° 116 ; CEDH, K.U. c. Finlande du 2 décembre 2008, requête no 2872/02.; CEDH Me André c/ France du 24 juillet 2008 n° 18603 /03 http://www.cercle-du-barreau.org/archive/2008/09/22/cedh-le-soucon-hors-la-loi.html , Commentaire de Jean Pannier, Gazette du palais du 13 janvier 2009 ; CEDH, S. et Marper c/ Royaume-Uni du 4 décembre 2008, requêtes N° 30562/04 et N° 30566/04. Pour plus de lecture, tous les arrêts de la Cour de Strasbourg sont disponibles sur http://www.echr.coe.int.

manière suffisamment claire, vu l'objectif légitime de la mesure en question, afin de conférer à l'individu une protection appropriée contre les ingérences arbitraires.[310]

Quant au rapport DEBET[311], il reproche le caractère parfois peu opérant des régimes dérogatoires introduits par la loi du 6 août 2004 et la nécessité de réfléchir sur une évolution possible de la loi dans ce domaine. En effet, dans un rapport relatif à la mesure de la diversité et à la protection des données personnelles[312], il a été fait remarquer que l'appréciation du caractère d'intérêt public dans un traitement de données personnelles se fait au *« cas par cas »*. Ainsi, se pose une question : peut-on « *considérer de façon générale que la lutte contre les discriminations présente un intérêt public et dès lors légitime tous les traitements de données sensibles réalisés dans ce cadre ? Autrement dit, peut-on considérer que tous les projets de recherche présentés à la Commission et qui ont pour objectif affiché de mesurer la diversité, de suivre les trajectoires, d'analyser les facteurs de discrimination revêtent a priori tous un intérêt public, et ce quelle que soit la nature publique ou privée de l'organisme responsable de ladite recherche ? »*

La réponse à cette question se révèle être délicate. En 2006, la CNIL a eu à apprécier si les projets de recherche qui lui étaient soumis relevaient ou non de l'intérêt public. Elle a fini par le leur reconnaître non sans difficulté après plusieurs discussions[313].

Dans sa délibération[314] du 7 décembre 1982, la CNIL a estimé que la direction centrale des renseignements généraux pourrait collecter des informations sur le type racial d'individus, dès lors que ces informations constituaient des éléments de signalement des personnes. De même,

---

[310] Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007. N° 00323/07/FRWP13. P. 14. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_fr.pdf. Consulté le 4 avril 2014.

[311]Mme Anne DEBET est Professeur des universités et membre de la CNIL. Elle a été désignée en 2005 par le Président de la CNIL, avec l'approbation de ses collègues pour présider un groupe de travail sur la question de la discrimination.

[312] DEBET, Anne. *Mesure de la diversité et protection des données personnelles*. Rapport présenté en séance plénière le 15 mai 2007. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/diversite/RapportdiversiteVD.pdf. Consulté le 16 avril 2014.

[313] Procès-verbal de la séance du 8 juin 2006. DEBET, Anne. CNIL. *Rapport sur la mesure de la diversité et protection des données personnelles.*15 mai 2007. P.15. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/diversite/RapportdiversiteVD.pdf. Consulté le 16 avril 2014.

[314] Délibération n° 82-205 du 7 décembre 1982 portant avis conforme sur le projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi n° 78-17 du 6 janvier 1978 aux traitements automatisés d'informations nominatives mises en œuvre par les services des renseignements généraux. www.legifrance.gouv.fr. Consulté le 16 avril 2014.

les services de renseignements généraux sont-ils autorisés à collecter, conserver et traiter des informations faisant apparaître des activités politiques, philosophiques, religieuses ou syndicales de certaines personnes si celles-ci permettent au gouvernement ou à ses représentants d'apprécier la situation politique économique ou sociale du pays ou de prévoir son évolution[315].

Il faut, cependant, que le champ des dérogations soit limité à ce qui est strictement nécessaire à la réalisation des objectifs d'intérêt public poursuivi. Ainsi, dans sa délibération[316] du 19 décembre 2000 relative aux systèmes de traitement des infractions constatées (STIC[317]), la CNIL a-t-il demandé que les données à caractère personnel sensibles ne puissent être collectées et traitées que si elles résultent de la nature ou des circonstances de l'infraction (la pédophilie pour une infraction pédophile, les opinions politiques ou religieuses pour les infractions terroristes, etc.).

7. Dans le cadre des traitements à des fins statistiques

La Directive autorise les États membres à prendre des dispositions pour permettre qu'un numéro d'identification nationale fasse l'objet de traitements[318]. Dans cette optique, la loi informatique et libertés prévoit en son article 8, 7° que sont permis *« 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 ».*

[315] Conseil d'État - Contentieux des 10ème et 7ème sous-sections réunies, 28 juillet 1995. Confédération générale du travail. Décision n° 132453. Recueil Lebon 1995.

[316] Délibération n° 00-064 du 19 décembre 2000 relative à un projet de décret en Conseil d'État portant création du « système de traitement des infractions constatées TIC » et application du troisième alinéa de l'article 31 de la loi du 6 janvier 1978. www.legifrance.gouv.fr. Consulté le 16 avril 2014.

[317] A compter du 31 décembre 2013, ce fichier est remplacé par le TAJ par décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires. JORF n° 0107 du 6 mai 2012, p. 8047. NOR : IOCD1125123D

[318] Article 8. 7 de la directive : «*Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. »*

La loi du 17 juin 1951 impose des conditions strictes quant aux traitements de données médicales par l'INSEE, notamment en son article 7 bis, des alinéas 2 à 5[319] pour préserver au mieux la confidentialité desdites données. Elle restreint, le pouvoir d'initiative à une seule autorité et n'admet les traitements qu'à une seule finalité. C'est uniquement sur réquisition du ministre chargé de l'économie après avis du Conseil national de l'information statistique et sauf disposition législative contraire que les informations relatives aux personnes physiques peuvent être cédées à l'INSEE ou aux services statistiques ministériels. Il faut, également que cela se fasse exclusivement dans un but d'établissement de statistiques.

Cette conception de la loi informatique et libertés, si elle traduit la lettre de la directive 95/46/CE, est plus restrictive que celle de la recommandation n° R (97) 18 sur la définition des activités statistiques. Le considérant 34 de la Directive qui donne compétence au législateur français de prévoir des garanties appropriées en la matière, précise « *les statistiques publiques* » et le considérant 23 fait référence « *aux instituts de statistiques* ». Ces précisions laissent peu de place à la considération des statistiques privées comme couvertes par la dérogation à l'interdiction de traitement. Or, dans le cadre de la recommandation, les rédacteurs de la recommandation ont débattu du statut des activités statistiques visées par celle-ci et plus précisément sur la question de savoir s'il fallait faire une distinction entre les statistiques officielles ou publiques et les statistiques privées. Certains experts ont estimé que la recommandation devait faire cette distinction, car, contrairement aux statistiques privées, la statistique officielle est autorisée par la loi, organisée et contrôlée dans un cadre institutionnel, et elle est régie par des normes de droit public garantissant une large protection des données.

[319]« *Les données à caractère personnel relatives à la santé recueillies dans les conditions prévues à l'alinéa précédent ne peuvent être communiquées, sur demande du ministre chargé de la santé, à l'Institut national de la statistique et des études économiques ou aux services statistiques des ministères participant à la définition, à la conduite et à l'évaluation de la politique de santé publique que dans le cadre d'établissement de statistiques sur l'état de santé de la population, les politiques de santé publique ou les dispositifs de prise en charge par les systèmes de santé et de protection sociale en lien avec la morbidité des populations. Des enquêtes complémentaires, revêtues du visa préalable mentionné à l'article 2, peuvent être réalisées auprès d'échantillons de ces populations.*

Les modalités de communication des données à caractère personnel relatives à la santé recueillies dans les conditions prévues à l'alinéa précédent ne doivent pas permettre l'identification des personnes.

Il ne peut être dérogé à cette dernière obligation que lorsque les conditions d'élaboration des statistiques prévues au deuxième alinéa nécessitent de disposer d'éléments d'identification directe ou indirecte des personnes, notamment aux fins d'établissement d'échantillons de personnes et d'appariement de données provenant de diverses sources, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Seules les personnes responsables de l'opération, désignées à cet effet par la personne morale autorisée à mettre en œuvre le traitement, peuvent recevoir les données à caractère personnel relatives à la santé transmises à l'Institut national de la statistique et des études économiques ou aux services statistiques des ministères participant à la définition, à la conduite et à l'évaluation de la politique de santé publique. Après utilisation de ces données, les éléments d'identification des personnes doivent être détruits. »

D'autres experts ont, cependant, observé que les frontières entre statistiques privées et publiques ne sont pas toujours claires : des travaux statistiques sont parfois commandés à des sociétés d'études par l'administration et des statistiques à finalité publique sont parfois produites par des organismes privés. La distinction entre les deux types peut également varier d'un pays à l'autre en fonction des législations nationales et elle entraînerait donc une inégalité dans l'application des principes de la recommandation dans les différents États membres. Finalement, les rédacteurs ont convenu que la recommandation doit s'appliquer à toute activité statistique, qu'elle soit développée par des instances officielles ou par des entreprises, des personnes ou des institutions publiques ou privées[320].

L'article 25 de la loi informatique et libertés oblige à requérir l'autorisation de la CNIL avant de procéder à ces traitements statistiques[321]. La Commission recommande[322] que l'usage du NIR[323] comme identifiant des personnes dans les fichiers soit justifié et non systématique, ni généralisé. En effet, les responsables de la conception d'applications informatiques doivent se doter d'identifiants diversifiés et adaptés à leurs besoins propres. La consultation du répertoire doit être subordonnée à la conclusion de conventions spécifiques avec l'INSEE et les organismes habilités, qu'elle donne lieu ou non à utilisation du numéro d'inscription audit répertoire.

Finalement, il convient de remarquer que si l'autorisation de la CNIL est requise pour permettre à l'INSEE et les services statistiques ministériels de réaliser des traitements comportant des données sensibles, ils ne sont pas tenus de recueillir le consentement des personnes concernées. Cela est à mettre au compte des prérogatives de puissance publique dont jouissent les administrations publiques dans leurs rapports avec les particuliers.

---

[320] Point 60 de l'exposé des motifs de la recommandation n° R (97) 18.

[321] Article 25 de la loi informatique et libertés : « I. - *Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :*
1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ; »

[322] Délibération n° 83-058 du 29 novembre 1983 portant adoption d'une recommandation concernant la consultation du RNIP et l'utilisation du NIR. http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/35/. Consulté le 5 avril 2014.

[323] Le NIR est un identifiant personnel unique composé de 13 chiffres créés à partir de l'état civil et constitué d'une structure signifiante, permettant d'identifier sans ambiguïté toute personne inscrite au répertoire national d'identification des personnes physiques (RNIPP). Il est plus connu sous le nom de numéro de sécurité sociale. Ce numéro est signifiant, car composé d'une chaîne de caractères permettant de déterminer le sexe, la date (sauf le jour) et le lieu de naissance ; unique et pérenne, puisqu'un seul numéro est attribué à chaque individu dès sa naissance ; Il est fiable, car il est certifié par l'INSEE à partir des données d'état civil transmises par les mairies.
Quel identifiant pour le secteur de la santé ? La CNIL propose la création d'un numéro spécifique généré à partir du NIR mais anonymisé. 20 février 2007. www.cnil.fr

8. En cas de nécessité de respect des obligations et des droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates.

Dans ce cas de figure, le traitement des données médicales doit seulement être justifié par la finalité, la simple utilité ne suffit pas. Ainsi, le responsable du traitement devra-t-il prouver qu'il est essentiel pour les droits et obligations à respecter en matière de législation du travail de procéder à ces traitements. La question se pose alors de savoir comment déterminer le niveau de pertinence de la finalité du traitement pour entrer dans le cadre de cette dérogation. La Directive laisse la latitude à chaque État membre en précisant : « *dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates* ». La loi interne doit donc s'assurer de garantir la protection des données des travailleurs avant d'autoriser une telle opération. Cette dérogation n'étant pas transposée par la loi française, doit-on croire que le législateur français estime qu'il n'y a pas aujourd'hui, assez de garanties, dans le domaine, pour autoriser de tels traitements ?

La première condition que pose la loi informatique et libertés avant d'accepter les hypothèses qui dérogent au principe de l'interdiction est que " *la finalité du traitement l'exige pour certaines catégories de données"*. En réalité, il faut chercher la réponse ailleurs. Cette dérogation vise les cas dans lesquels la législation nationale prévoit le prélèvement à la source par l'employeur de cotisations syndicales ou de contributions fiscales aux églises. Or cela n'est pas le cas en France ; ce qui rend la transposition inopportune. Par contre, conformément à la possibilité à lui offerte par la Directive d'autoriser d'autres exceptions[324] la loi française a prévu des dérogations propres à elle.

B. Les exceptions spécifiques à la législation française

Le législateur français a usé de la faculté que lui donne la Directive pour ajouter deux exceptions qui lui sont particulières. Ce sont celles qui sont de nature à favoriser la recherche et celles relatives à l'anonymisation.

[324] Article 8. 4 de la Directive : *« Sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle ».*

1. Dans l'intérêt de la recherche dans le domaine de la santé

La législation française a autorisé *« les traitements nécessaires à la recherche dans le domaine de la santé*[325] *»* dans la mesure où cela se fait dans le respect des modalités prévues au chapitre IX[326] de la loi informatique et libertés. Ce chapitre, consacré aux traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, en délimite le cadre légal en disposant que « *les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients ne sont pas soumis aux dispositions du présent chapitre. Il en va de même des traitements permettant d'effectuer des études à partir des données ainsi recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif*[327] *».*

Cette dérogation est née du déplacement du contenu du chapitre V bis de l'ancienne loi informatique et libertés vers le chapitre IX actuel pour permettre le traitement des données sensibles dans le secteur de la recherche dans le domaine de la santé selon les modalités du chapitre IX. C'est la suite d'un amendement[328] adopté par l'Assemblée nationale avec l'avis favorable du gouvernement présenté par le député Gérard GOUZES. Elle trouve son intérêt dans le fait que la recherche médicale est l'un des motifs d'intérêt public important prévu par l'article 8, paragraphe 4 de la directive, qui permet à l'autorité de contrôle de prévoir d'autres dérogations sous réserve de garanties appropriées. La recherche médicale a besoin de collecter de nombreuses informations concernant les patients qui participent à une étude pour pouvoir en exploiter les résultats. Or, cela s'avère plus difficile avec les seules capacités humaines ; c'est pourquoi, pour gérer l'accumulation des données nominatives de santé, les progrès

[325] Article 8, II, 8° de la loi informatique et libertés.

[326] Le contenu de ce chapitre IX est né d'une loi qui a été votée le 1er juillet 1994 (Loi n°94-548 du 1er juillet 1994 relative au traitement des 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. 9559-9560. NOR : RESX9200045L) pour modifier, en complétant, la loi informatique et libertés face à l'accumulation des informations personnelles et la multiplication des traitements possibles en matière de recherche médicale. Vivement attendue par les milieux scientifiques et la CNIL, elle visait à résoudre les problèmes juridiques et pratiques de secret médical, de protection de données et de respect de la vie privée qui se posaient encore 15 ans après la loi du 6 janvier 1978.

[327] Article 53 de la loi informatique et libertés.

[328] GOUZES, Gérard. 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. Amendement n° 15. 19 janvier 2002. N° 3526. http://www.assemblee-nationale.fr/11/rapports/r3526.asp. Consulté le 28 avril 2014.

informatiques se révèlent être indispensables. En plus, les traitements d'anonymisation en matière de recherche dans le domaine de la santé permettent de protéger la vie privée des personnes concernées.

Les chercheurs apprécient, pour leur part, que la CNIL leur permette désormais[329] d'utiliser (même à certaines conditions) le NIR dans le cadre de leurs travaux alors que cela leur était jusque-là interdit. En effet, à moins d'utiliser le NIR, ils n'arrivent pas toujours à fournir aux autorités des résultats statistiques fiables pour l'élaboration et l'évaluation des politiques de santé publique et la surveillance sanitaire de la population.

2. Dans le cadre d'un procédé d'anonymisation

L'interdiction de traiter les données sensibles est levée si celles-ci font *« l'objet à bref délai d'un procédé d'anonymisation préalablement reconnu conforme (*aux dispositions de la loi informatique et libertés*) par la Commission nationale de l'informatique et des libertés (…)*[330] *»*.

L'anonymisation n'a pas été définie par la loi mais les correspondants informatique et libertés, dans un souci d'aide à la compréhension des termes informatiques aux non informaticiens, proposent la définition suivante : c'est le processus par lequel des données sont rendues anonymes et à l'issue duquel elles ne peuvent plus être affectées ou rattachées à une personne en particulier, à un individu[331]. Lorsqu'elles sont anonymisées, les données ne

[329] CNIL. *La CNIL demande une utilisation encadrée du NIR pour faciliter la recherche médicale*. 11 janvier 2011. *« Compte tenu des enjeux que soulève cette question et de la nécessité de maintenir le niveau de la recherche française sur le plan international, la CNIL a décidé d'œuvrer activement pour l'élaboration de solutions juridiques et techniques pour remédier à cette situation. Elle a donc engagé une réflexion de fond sur le sujet, conduit plusieurs réunions de travail et auditionné divers acteurs concernés, parmi lesquels l'Institut de Veille Sanitaire et le Haut Conseil de la Santé Publique. A l'issue de ces travaux, la CNIL a demandé aux pouvoirs publics de prendre les mesures réglementaires nécessaires pour définir une politique d'accès au NIR à des fins de recherche et d'études de santé publique. En conséquence, elle a saisi le Premier ministre et les ministres de la santé et de la recherche de cette demande. En effet, un "décret cadre", pris après avis de la CNIL, pourrait autoriser les chercheurs et les autorités sanitaires à utiliser le NIR. Cette utilisation pourrait se faire dans des conditions définies dans le cadre d'une concertation entre la CNIL et l'ensemble des acteurs concernés. La Commission est déterminée à faciliter le travail de la recherche médicale et les évaluations de santé publique, dans le respect des droits des citoyens et de la confidentialité des données de santé.* » http://www.cnil.fr/la-cnil/actu-cnil/article/article/lutilisation-encadree-du-nir-par-les-chercheurs-et-les-autorites-sanitaires-un-veritable-enje/. Consulté le 12 février 2011.

[330] Article 8, III de la loi informatique et libertés

[331]Glossaire de l'anonymisation de données du groupe Référentiels et Labels de l'AFCDP (Association française des correspondants à la protection des données à caractère personnel) http://www.afcdp.net

permettent plus de ré-identifier les personnes concernées. Les données pseudonymisées ne sont pas des données anonymes selon le groupe de l'article 29. Ce regroupement d'autorités de protection des données a publié en avril 2014, un avis[332] sur les principales techniques d'anonymisation, afin d'expliquer comment les mettre en œuvre. Ces techniques se regroupent autour de deux grands principes : transformer les données pour qu'elles ne se réfèrent plus à une personne réelle et généraliser les données de façon à ce qu'elles ne soient plus spécifiques à une personne mais communes à un ensemble de personnes. Pour chaque technique, une analyse de ses forces et faiblesses au regard des trois critères d'évaluation est fournie ainsi que des recommandations pratiques pour son utilisation. L'anonymisation et la ré-identification des données sont des thématiques des recherches particulièrement actives et par conséquent, il est indispensable, pour tout responsable de traitement mettant en œuvre des solutions d'anonymisation, d'effectuer une veille régulière pour préserver, dans le temps, le caractère anonyme des données produites[333].

Le processus d'anonymisation est irréversible et se fait sous le contrôle de la CNIL.

La législation française n'a pas, non plus, explicité l'expression *« à bref délai »*. Cette expression proche de «*meilleurs délais*», plus fréquemment utilisée dans le code de procédure pénale à titre d'illustration est inhabituelle en droit français. En plus, le temps correspondant à ce délai et accordé aux responsables de traitement n'est pas spécifié. Il faut juste retenir que le responsable doit s'assurer de l'efficacité et de la rapidité du procédé tendant à transformer les données à caractère personnel en données anonymes. En outre, l'on pourrait supposer que le délai est fixé de façon discrétionnaire par la CNIL dans le cadre de l'autorisation qu'elle doit donner.

La CNIL « *peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables*». Il apparaît donc que l'appréciation de la pertinence de la finalité soit

---

Pour plus d'informations sur le procédé d'anonymisation, voir un article de la CNIL : *L'état des lieux en matière de procédés d'anonymisation.* http://www.cnil.fr/la-cnil/actu-cnil/article/article//lÉtat-des-lieux-en-matiere-de-procedes-danonymisation/. Consulté le 17 Août 2010.

[332] GROUPE DE l'ARTICLE 29. Communiqué de presse de l'avis sur les techniques d'anonymisation. 10 avril 2014. Disponible sur : http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140410_pr_9_10_april.pdf. Consulté le 19 avril 2014.

[333] CNIL. Le G 29 publie un avis sur les techniques d'anonymisation. 16 avril 2014. Disponible sur: http://www.cnil.fr/nc/linstitution/actualite/article/article/le-g-29-publie-un-avis-sur-les-techniques-danonymisation/?utm_source=rss&utm_medium=rss&utm_campaign=le-g-29-publie-un-avis-sur-les-techniques-danonymisation-cnil-Commission-nationale-de-linformatique-et-des-liberts. Consulté le 19 avril 2014.

également laissée à la discrétion de la CNIL et celle-ci l'assume en veillant à ce que des garanties soient prises pour préserver la sécurité des données nominatives[334] avant d'autoriser les traitements (le procédé d'anonymisation doit avoir été « *préalablement reconnu conforme aux dispositions* » de la loi informatique et libertés par la CNIL[335]). Des lors, cette dérogation ne sera applicable qu'aux traitements d'anonymisation dont les procédés auront été préalablement homologués par la Commission. En effet, une des missions de la CNIL prescrites par l'article 11 de la loi informatique et libertés consiste à donner un avis sur la conformité aux dispositions de la loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel ou à l'anonymisation de ces données, qui lui sont soumis. Elle porte alors une appréciation sur les garanties offertes par des règles professionnelles qu'elle a précédemment reconnues conformes aux dispositions de la loi, au regard du respect des droits fondamentaux des personnes[336].

Les données appartenant au domaine des chapitres IX et X sont exclues du champ des procédés d'anonymisation tels que perçus par l'article 8, III. Les informations concernées sont les données sensibles du paragraphe I dudit article. Il s'agit également de toutes les données médicales expressément exclues du champ desdits chapitres[337].

Les données qui font l'objet des chapitres IX et X de la loi informatique et libertés ont été exclues de cette exception afin d'éviter une confusion sur le régime applicable. La dérogation porte sur l'anonymisation alors que le chapitre IX prévoit, sauf exception, que les

[334] Ainsi, concernant sa décision du 10 décembre 2009, les expérimentations ont toutes pour objet de permettre la transmission aux organismes d'assurance maladie complémentaire (AMC) des codes des médicaments et en matière d'optique des codes produits et prestations délivrées à l'assuré. L'accès à ces données qui figurent sur les feuilles de soins électroniques permet aux complémentaires de mieux identifier les soins remboursés et ainsi de simuler ou de proposer à leurs assurés des garanties contractuelles modulées, d'affiner leur tarification sur la prise en charge de spécialités non remboursées par le régime obligatoire et d'inciter les assurés à adhérer à des actions de prévention. Alors que la politique du gouvernement vise à diminuer ou à rembourser certains produits ou prestations à service médical rendu estimé insuffisant, l'accès apparaît pour les AMC d'autant plus nécessaire qu'elles souhaitent jouer un rôle accru en matière de maîtrise des dépenses de santé. Afin de s'assurer que les données qui pourraient conduire à identifier les assurés ne viennent à la connaissance des AMC tout en permettant à ceux-ci d'affiner les garanties qu'ils proposent, la Commission a demandé que l'anonymisation repose sur l'utilisation d'une boîte noire, c'est-à-dire un dispositif matériel inviolable même par les complémentaires santés auditées par un organisme extérieur à l'AMC. CNIL. 30ème rapport annuel d'activités de la CNIL p. 71. www.cnil.fr.

[335] Article 8, III de la loi informatique et libertés

[336] Article 11, 3° a) et b), loi informatique et libertés.

[337] Voir les articles 53, alinéa 2 et 62, alinéa 2 de la loi informatique et libertés.

données soient codées et le chapitre X exige également que les données soient traitées sous forme de statistiques anonymisées ou agrégées. L'objet est donc le même mais l'objectif du législateur est, au contraire, d'appliquer le mécanisme d'autorisation de l'article 25, qui constitue le droit commun en la matière dans certains cas, et de réserver le processus d'autorisation des chapitres IX et X aux seuls traitements répondant aux finalités spécifiques, objet de chacun de ces chapitres[338]. Le rapport DELATTRE dénonce cette multiplication des régimes d'autorisation. « *Elle n'est pas pleinement satisfaisante et pourrait conduire, dans le silence du texte adopté par le Sénat, à faire relever les traitements d'anonymisation d'au moins trois procédures concurrentes. Dans ces conditions, et par souci de simplification, il serait préférable d'unifier les régimes d'autorisation au profit de la procédure de droit commun prévue par l'article 25* »[339]. Malgré les amendements adoptés par la Commission des lois de l'Assemblée nationale en ce sens, l'article 8, III a conservé, en l'état actuel, le même contenu.

Cette catégorie d'exception a été ajoutée par le Sénat pour faciliter le développement des traitements d'anonymisation des données. Cette volonté « *s'explique par l'intérêt qu'il y a, tant pour les pouvoirs publics que pour les personnes privées, de disposer d'études qualitatives en matière médicale, sanitaire ou sociologique pour ne citer que ces quelques exemples.*[340] » tout en préservant la vie privée.

Les données médicales sont particulièrement encadrées par un régime juridique exorbitant du droit commun des traitements automatisés de données personnelles.

---

[338] Chapitre IX : Traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé.
Chapitre X : Traitements de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention. Loi informatique et libertés http://www.legifrance.gouv.fr

[339] DELATTRE, Francis, *Rapport n° 1537 de l'Assemblée nationale sur le projet de loi, modifié par le sénat (n° 762), 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. 13 Avril 2004 publié le 14 Avril 2004. p. 16.* http://www.assemblee-nationale.fr/12/rapports/r1537.asp. Consulté le 27 mai 2014

[340] DELATTRE, Francis, *Rapport n° 1537 de l'Assemblée nationale sur le projet de loi, modifié par le sénat (n° 762), 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. 13 Avril 2004 publié le 14 Avril 2004. p. 8.* http://www.assemblee-nationale.fr/12/rapports/r1537.asp. Consulté le 27 mai 2014.

Section 2 : Le traitement automatisé des données médicales : un régime exorbitant

La version initiale de la loi informatique et libertés n'avait prévu qu'une seule disposition relative à l'exercice du droit d'accès à l'égard *« des informations à caractère médical »*. Les formalités préalables aux traitements des données de santé étaient différentes selon que le responsable du traitement était une personne publique ou privée. Mais le secteur de la santé a connu d'importantes modifications technologiques dues à la généralisation et à l'automatisation du traitement des informations aussi bien en matière de soins que de politique de santé publique. Les professionnels du secteur, à l'instar des médecins, des hôpitaux, mais également des laboratoires d'analyses ou des caisses de sécurité sociale ont été de plus en plus amenées à échanger, à partager et à transférer dans le cadre de leurs activités les informations médicales susceptibles de concerner directement les patients. C'est dans ce cadre que des modifications ont été apportées à la loi du 6 janvier 1978 en 1994, puis en 1999. La procédure est devenue identique, que le traitement envisagé profite à une personne publique ou à une personne privée. Des dispositions spécifiques relatives aux traitements de données nominatives à des fins de recherche dans le domaine de la santé et à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention ont été insérées. Cela a eu des incidences sur les droits reconnus aux titulaires des données et les obligations à la charge des responsables des traitements (Paragraphe 1). Des formalités très particulières aux traitements des données dans certains secteurs de la santé ont vu le jour (Paragraphe 2).

Paragraphe 1 : Les droits des personnes concernées et les obligations des responsables de traitement

De prime abord, il faut rappeler que les dispositions générales de la loi informatique et libertés relatives aux droits des personnes et aux obligations de responsable du traitement sont celles applicables aux données médicales. Mais, certains droits et obligations comportent des aspects spécifiques au secteur de la santé.

A. Les droits des personnes concernées

Les personnes concernées sont celles dont les données sont collectées, mais aussi les destinataires des données médicales. Toutefois, l'article 58 de la loi informatique et libertés dispose que « *sont destinataires de l'information et exercent les droits prévus aux articles 56 et 57 les titulaires de l'autorité parentale, pour les mineurs, ou le représentant légal pour les personnes faisant l'objet d'une mesure de tutelle* ». Cette disposition ne mentionnant pas les majeurs placés sous sauvegarde de justice et ceux ayant fait l'objet d'une mesure de mise sous curatelle, les reconnaît comme personnellement destinataire de l'information en matière de santé.

Les droits reconnus aux destinataires des données de santé qui connaissent des modifications sont essentiellement, le droit à l'information, le droit d'accès et le droit à l'opposition.

1. Le droit à l'information

Pour les traitements relatifs aux données de santé, le contenu du droit à l'information est différent de celui de droit commun édicté par l'article 32 de la loi informatique et libertés. L'article 57[341] prévoit, comme l'article 32, que la personne doit être informée de la finalité du

[341] *« 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 ;

traitement, des destinataires des données, de ses droits d'accès et de rectification. Par contre, l'identité du responsable de traitement ne lui est pas obligatoirement due. Dans la pratique, la personne concernée est, tout de même, informée de l'identité du promoteur lorsqu'il s'agit de recherche biomédicale conformément aux dispositions du code de la santé publique. La déclaration d'Helsinki[342] rappelle que les sujets se prêtant à des recherches médicales doivent être volontaires et informés des modalités de leur participation au projet de recherche.

Les termes de l'article 57 n'obligent pas, non plus, à informer l'individu concerné du transfert de ses données en dehors de l'Union européenne car, les données sont censées être protégées[343] lorsque l'on les transfère sauf exception autorisée par la CNIL. La nature des données transmises doit, par contre, lui être précisée. Cette disposition constitue une différence avec l'article 32 qui ne prévoit pas ce droit.

Le droit à l'information a un contenu bien plus important lorsqu'il s'agit de recueil de *« prélèvements biologiques identifiants[344] »*. En effet, l'article 56 alinéa 2 de la loi informatique et libertés exige le consentement «*éclairé et exprès*» des personnes avant toute collecte de données les concernant. La délicatesse de cette situation est due au fait que tout prélèvement biologique est potentiellement identifiant compte tenu des techniques d'identification génétique qui peuvent être mises en œuvre (à partir d'un simple cheveu par exemple). Il s'ensuit donc que la personne doive recevoir l'information générale mais elle doit également obtenir une information plus appropriée et plus approfondie sur la recherche envisagée. Les prélèvements biologiques identifiants sont considérés par la CNIL comme des prélèvements

---

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. (…) »
Les modalités d'information des personnes concernées sont fixées par les articles 36 et 37 du décret n°2005-1309 du 20 Octobre 2005 modifié par le décret n°2007-451 du 25 mars 2007. JORF n°74 du 28 mars 2007. P. 5782. Texte n° 30.

[342] Déclaration d'Helsinki. Juin 1964. The journal of the American Medical Association. 27 novembre 2013. Volume 310. n° 20. http://www.wma.net/fr/30publications/10 policies/b3/index.html. Consulté le 5 avril 2014.

La déclaration d'Helsinki a été élaborée par l'association médicale mondiale. Déclaration de principes éthiques dont l'objectif est de fournir des recommandations aux investigateurs participant à la recherche médicale sur des êtres humains. Elle a été adoptée pour la première fois en 1964 et a été amendé 6 fois depuis. Le dernier amendement date de l'Assemblée générale d'octobre 2013. Cette dernière version est la seule officielle. Les principes éthiques consacrés par ce texte constituent la base des textes applicables aux recherches médicales sur des sujets humains. http://www.wma.net/fr/20activities/10ethics/10helsinki/index.html. Consulté le 5 avril 2014.

[343] Article 68 à 70 du chapitre XII de la loi informatique et libertés

[344] «*Dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données*». Article 56, alinéa 2, loi informatique et libertés..

de données d'ordre génétique. Or, depuis la transposition de la directive de 1995 et la modification de la loi informatique et libertés de 2004, le traitement des données génétiques ne peut se faire que dans le cas d'un traitement autorisé par la CNIL. Le code de la santé publique[345] et les bonnes pratiques cliniques[346] exigent également un accord exprès et éclairé de l'individu pour la participation d'une personne à une recherche. Le consentement doit donc être explicite et précédé d'une information suffisante. Certes, il n'y a pas d'exigence légale de l'écrit mais il est de l'intérêt des responsables du traitement de requérir le consentement écrit de la personne préalablement informée par un moyen lui permettant de comprendre la situation.

Le droit à l'information préalable et individuelle connaît deux limites importantes (prévue par l'article 57) dues à la spécificité des données traitées (médicales). La première dérogation consiste dans le fait que les « *informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave* ». Le médecin traitant peut se soustraire à l'obligation d'information en décidant de ne pas aviser son patient d'un diagnostic ou d'un pronostic grave. La personne se contentera, alors, de déduire sa situation de la finalité du traitement qui lui sera obligatoirement indiquée.

Quant à la seconde, elle réside dans le fait que *« dans le cas où les données ont été initialement recueillies pour un autre objet que le traitement, il peut être dérogé à l'obligation d'information individuelle lorsque celle-ci se heurte à la difficulté de retrouver les personnes concernées »*. C'est le cas lorsque des données sont recueillies chez des patients pour d'autres fins que la recherche et qui ont quitté le centre de soins ou de recherche.

Retenons que ces dérogations ne peuvent être mises en œuvre que si elles ont été signifiées et approuvées par la CNIL à travers la demande d'autorisation.

L'article 59 prévoit un droit à l'information collective *« dans tout établissement ou centre où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement visé à l'article 53 »* c'est-à-dire, un traitement entrant dans le domaine de la recherche dans le secteur de la santé. Dans ce cas, l'information se fait par la remise d'un document ou tout autre moyen approprié (article 37 du décret n° 2007-451 précité).

[345] Articles L. 1111-1, L. 1111-2 et L. 1111-4 du Code de la santé publique.

[346] Articles 35 et 36 du Code de déontologie médicale.

Les informations concernant une personne décédée y compris celles qui figurent sur les certificats de décès, peuvent être traitées sans recourir à l'information de sa famille sauf si l'intéressé a manifesté, de son vivant, son refus, par écrit[347]. La recherche peut, en effet, être effectuée longtemps après le décès de l'individu et il pourrait s'avérer difficile de retrouver un membre de sa famille. Cette dérogation se justifie également par l'intérêt scientifique évident face au très faible risque d'atteinte à la mémoire du défunt et à la vie privée de ses proches compte tenu de ce que les données sont codées. D'ailleurs, l'article 55 de la loi informatique et libertés exige que la présentation des résultats du traitement de données ne puisse, en aucun cas, permettre l'identification directe ou indirecte des personnes concernées.

Le droit à l'information ouvre sur un droit d'accès direct aux informations de santé.

2. Le droit d'accès aux données médicales

Aux termes de l'article L 1111-7 du code de la santé publique, « *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, (…) 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. Elle peut accéder à ces informations directement ou par l'intermédiaire d'un médecin qu'elle désigne et en obtenir communication…*». Cette disposition a été intégrée au code de la santé publique par la loi Kouchner de 2002[348]. Le patient peut directement accéder à ses données de santé et le recours à la médiation médicale ne constitue qu'une faculté.

Le respect du droit d'accès direct aux patients posait un problème aux médecins, notamment ceux responsables des registres épidémiologiques des cancers, avant le 1er juillet 1994[349]. Antérieurement, le devoir d'information du patient qui pesait sur le médecin, même

[347] Article 56, loi informatique et libertés.

[348] Loi 2002-303 du 4 mars 2002, op cit

[349] Date d'adoption de 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. JORF n° 152 du 2 juillet 1994. p. 9559. NOR : RESX9200045L.

non codifié, mais entretenu par la jurisprudence[350] de la Cour de Cassation, l'obligeait à donner au patient une information « *simple, approximative, intelligible et loyale* » sur son état et sur les soins envisagés. L'article 40.5 de la loi du 1er juillet 1994 qui reprend l'obligation d'information qui pèse sur les responsables des traitements de données médicales autorise, toutefois, le médecin traitant à ne pas délivrer des informations au malade, si pour des raisons légitimes qu'il apprécie en conscience, il doit le laisser dans l'ignorance d'un diagnostic ou d'un pronostic graves. Cette disposition va être renchérie en 1995 par l'article 35[351] du code de déontologie médicale, aujourd'hui abrogé puis remplacé par l'article R 4127-35 du code de la santé publique. Ce dernier donne cette possibilité au praticien, sous réserve des dispositions de l'article L 1111-7. Or, cela apparaît littéralement comme une dérogation au principe de l'obligation d'information. Mais l'article 43[352] de la loi informatique et libertés en légiférant sur un droit d'accès indirect aux personnes concernées par les informations médicales atténue les effets d'un tel contournement. Il donne, ainsi, la possibilité aux médecins de prendre les dispositions utiles pour ménager les patients atteints d'affections graves qu'ils ne soupçonnaient pas ou dont la confirmation brutale risque d'occasionner de plus graves conséquences avant qu'ils ne prennent connaissance de l'information par leur droit d'accès.

La disposition sur le droit d'accès indirect aux informations médicales (par l'intermédiaire d'un médecin désigné par l'intéressé) est reprise par l'article 6 bis de la loi du 17 juin 1978[353], le décret du 30 mars 1992[354] et la loi du 10 janvier 1994[355]. L'insistance du législateur sur cette disposition dans plusieurs textes législatifs et réglementaires et le fait de consacrer particulièrement l'article 43 de la loi informatique et libertés aux données de santé traduisent la volonté de celui-ci de rester en accord avec l'ancien article 35 du code de

---

[350] Cour de Cassation 1ère chambre civile, 21 février 1961. Bulletin 1961, I, n° 112. P. 90.

[351] « *Toutefois, dans l'intérêt du malade et pour des raisons légitimes que le praticien apprécie en conscience, un malade peut être tenu dans l'ignorance d'un diagnostic ou d'un pronostic graves, sauf dans les cas où l'affection dont il est atteint expose les tiers à un risque de contamination* ». Article 35, al 2.

[352]Lorsque l'exercice du droit d'accès s'applique à des données de santé à caractère personnel, celles-ci peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet, dans le respect des dispositions de l'article L. 1111-7 du code de la santé publique

[353] 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.

[354] Décret n° 92 - 329 du 30 mars 1992 relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santé publics et privés et modifiant le code de la santé publique (deuxième partie : décret en Conseil d'État). JORF n° 78 du 1er avril 1992. P.4607. NOR : SANH9200522D.

[355] Loi n° 94-43 du 18 janvier 1994 relative à la santé publique et à la protection sociale (annexes 5). JORF n° 15 du 19 janvier 1994 P. 960. NOR : SPSX9300136L.

déontologie médicale précité. Faut-il le rappeler, l'article 35, en limitant l'information du patient, veille à le protéger contre des nouvelles sur son état de santé qui risquent de lui porter préjudice.

Même si le caractère indirect de ce droit apparaît comme une limitation des libertés individuelles elle est légitimée par la directive européenne du 24 octobre 1995. Celle-ci prévoit, dans son considérant 42, que « *les États membres peuvent, dans l'intérêt de la personne concernée ou en vue de protéger les droits et les libertés d'autrui limiter le droit d'accès et d'information ; qu'ils peuvent par exemple préciser que l'accès aux données à caractère médical ne peut être obtenu que par l'intermédiaire d'un professionnel de la santé* ». De plus, l'accès indirect aux données médicales ne constitue qu'une faculté pour le patient car le texte de l'article 43 dispose bien que «*celles-ci peuvent être communiquées à la personne concernée selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet ».* La question peut, par contre se poser de savoir dans quelles hypothèses la personne concernée peut accéder directement et dans quels autres cas, elle peut accéder indirectement à ses données médicales personnelles.

On pourrait croire que tout dépend de la volonté du patient, mais comment celui-ci saura s'il peut consulter directement ses données ou s'il doit le faire par l'intermédiaire d'un médecin ? La loi ne donne pas de précisions à ce sujet. L'exemple qu'offre la loi belge du 22 août 2002 relative aux droits du patient est édifiant en ce qu'elle précise les hypothèses[356] dans lesquelles le patient à un droit d'accès indirect aux annotations personnelles du médecin. Ce texte pourrait servir à inspirer des pistes de réflexion sur les situations où un individu peut recourir à un intermédiaire pour accéder à ses propres informations médicales.

Le droit d'accès conduit logiquement à un droit à rectification car toute personne peut demander la rectification des erreurs commises lors de la collecte de ses données. Pour Claire MARIAC-NEGRIER, « *ce droit est largement théorique en matière médicale dans la mesure où, pour les données de santé, le patient n'a pas toujours la compétence requise pour déceler l'erreur. Certes, les médecins requis consultant un dossier comportant des fausses informations ou des informations suspectes pourraient le souligner au patient, mais ces cas sont une hypothèse d'école dans la mesure où le dossier se forme avec le concours des*

[356]BRILLON, Stéphanie. *Le droit d'accès aux annotations personnelles de praticien professionnel*, in http://www.hospitals.be n°1 Mai - juin - juillet 2003. Voir également les articles 9, §2, alinéa 4 ; article 7, §4, alinéa 2 et article 9, §2, alinéa 5, article 9, §4 de la loi du 22 août 2002 relative aux droits du patient.

praticiens au service du patient[357] ». Pour cet auteur, également, parmi les droits qu'elle estime uniquement théoriques, figure le droit d'opposition.

3. Le droit d'opposition

L'article 38 de la loi informatique et libertés reconnaît à toute personne physique le droit de s'opposer, pour des motifs légitimes à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. Ainsi, les destinataires de données peuvent-ils refuser de figurer dans certains fichiers ou de laisser communiquer leurs informations personnelles médicales à des tiers[358]. On aurait pu craindre que l'intérêt général de la recherche médicale fasse écarter ce droit d'opposition au traitement automatisé de données à l'individu concerné. Mais, il n'en est rien et ce dernier peut y parvenir rien qu'en exprimant son refus par tout moyen[359] auprès, soit des responsables de la recherche, soit de l'établissement ou du professionnel de santé détenteur de ses données. Le droit d'opposition apparaît donc ainsi comme une faculté offerte à la personne concernée. En matière de recherche médicale, cette faculté a été jugée peu protectrice par des députés qui, dans un rapport en date du 7 avril 2010[360], rappellent leur volonté d'accorder plus d'importance à ce droit en fonction du niveau d'implication de la personne humaine dans la recherche clinique.

Si l'article 38 de la loi informatique et libertés reconnaît le droit d'opposition à la personne concernée par rapport au traitement de ses données médicales, l'article 56 de la même loi accorde ce droit lorsque les données sont menacées de faire l'objet d'une levée du secret professionnel rendue nécessaire par la nature du traitement. Dans ce second cas, le législateur n'impose pas de motifs légitimes au demandeur pour exercer ce droit d'opposition.

---

[357] MARLIAC-NEGRIER, Claire. *La protection des données nominatives informatiques en matière de recherche médicale.* Tome 1, p.317.

[358] Les modalités d'exercice de leur opposition sont fixées par les dispositions des articles 28 et 29 du décret n° 2005 - 1309 du 20 octobre 2005 tel que modifié par celui du 25 mars 2007 (décret n° 2007 - 451, 25 mars 2007).

[359] Mais il est préférable de le faire par écrit.

[360] Rapport de l'Assemblée Nationale n° 2444 concernant la proposition de loi modifiée par le Sénat relative aux recherches cliniques ou non interventionnelles impliquant la personne humaine. M. Olivier JARDE, rapporteur exprimait par exemple la proposition suivante : *« une gradation des procédures de protection des personnes, en les proportionnant au degré de risques et de contraintes que comportent ces trois catégories de recherche : consentement écrit pour les recherches interventionnelles, consentement libre et éclairé pour les recherches à risques et contraintes minimes, simple information et droit d'opposition pour les recherches observationnelles* ». http://www.assemblee-nationale.fr/13/rapports/r2444.asp.

Le retrait de ses justifications laisse présager de la volonté de faire prévaloir les droits de la personne concernée sur les exigences des chercheurs à l'encontre desquelles il paraissait délicat de fournir une raison légitime et valable d'opposition au traitement envisagé. « *Le droit d'opposition doit être purement discrétionnaire pour laisser aux personnes leur pleine et entière liberté*[361] ».

La loi impose, cependant, le refus par écrit préventif de l'utilisation post-mortem des données concernant la personne décédée si celle-ci ne souhaite pas voir ses données médicales traitées après sa mort. Cette disposition a le mérite de légaliser, de manière subtile, les traitements de données appartenant à des défunts effectués par les épidémiologistes et les services de l'État par l'INSERM[362]. Il est rare de voir des personnes user de ce droit d'opposition avant leur décès.

Dans le domaine de la télémédecine, la question se pose de savoir s'il est possible de s'opposer à une transmission de données. Le droit existe et il n'y a pas de raison que l'on refuse à un individu de s'en prévaloir. Mais, son opportunité est moins certaine en ce sens que les professionnels intervenants sont tenus au secret médical et que cela réduit considérablement le risque d'intrusion dans la vie privée du concerné. De plus, le transfert se fait pour une raison qui apparaît en elle-même comme légitime : soigner efficacement le patient. N'y aurait-il pas une contradiction entre le fait d'accepter de recourir à un procédé de télémédecine et le fait de refuser la transmission des informations nécessaires à son bon déroulement ? Ce droit n'a donc pas véritablement d'importance en matière de télémédecine et il ne s'applique pas non plus aux traitements de données médicales ayant pour fin le suivi thérapeutique et médical.

C'est, forte de ces constats que Mme MARLIAC a déduit que ce droit d'opposition est purement théorique[363]. Cela n'empêche que l'information obligatoire et individuelle doive toujours mentionner la faculté d'opposition ainsi que le régime particulier auquel sont soumis les prélèvements biologiques identifiants lorsque ceux-ci sont opérés.

---

[361] MALLET-POUJOL, Nathalie. *La loi du 1er juillet 1994 : contraindre ou convaincre ?*, DIT 1995/1, p. 20.

[362] Article 25, alinéa 3 et 4 de la loi 93-23 du 8 janvier 1993 modifiant le titre VI du livre III du code des communes et relative à la législation dans le domaine funéraire : « *Ce certificat, rédigé sur un modèle établi par le ministère chargé de la santé, précise, de manière confidentielle, la ou les causes du décès à l'autorité sanitaire de la santé dans le département. Ces informations ne peuvent être utilisées que par l'État, pour la prise de mesures de santé publique ou pour l'établissement de la statistique nationale des causes de décès par l'Institut national de la santé et de la recherche médicale. »* JORF n°7 du 9 janvier 1993 p.499. NOR : INTX9200170C.

[363] MARLIAC-NEGRIER, Claire. La protection des données nominatives informatiques en matière de recherche médicale. Tome 1, p. 318.

B. Les obligations des responsables de traitement

Comme pour tous les traitements relatifs aux données personnelles, les responsables du traitement de données médicales doivent, prioritairement, veiller à la sécurité et à la confidentialité des informations conformément à l'article 34 de la loi informatique et libertés. Mais, compte tenue de la sensibilité de ces informations, le droit positif se montre plus rigoureux à leur égard. Le non respect de cette obligation les expose à des sanctions pénales.

1. Des obligations plus strictes pour les responsables de traitements des données médicales

L'alinéa 2 de cet article prévoit la possibilité, pour le gouvernement, de fixer, par décret, *« des prescriptions techniques auxquelles doivent se conformer les traitements »*. Ce texte vise les traitements nécessaires à la sauvegarde de la vie humaine mais auxquels la personne n'a pas pu donner son consentement et les traitements nécessaires aux fins de la médecine et à l'administration de soins. L'article 55 précise certaines de ces dispositions pour garantir la sécurité des informations recueillies. En dehors des cas particuliers comme l'étude de pharmacovigilance ou en cas de recherche particulière, ou encore en cas de protocoles de recherches réalisées dans le cadre d'études coopératives nationales ou internationales, les responsables sont tenus de coder les données avant leur transmission. Les personnes concernées ne doivent pas pouvoir être identifiées directement ou indirectement par la présentation des résultats du traitement de données.

L'ancienne rédaction de la loi du 6 janvier 1978 imposait à l'État destinataire une protection équivalente à celle de la loi française avant de permettre la transmission de données nominatives codées en matière de recherches de santé. Le transfert devait, en outre, faire l'objet d'une autorisation de la CNIL. Il n'y avait pas de distinctions entre les États membres de l'Union européenne et les autres. Mais la nouvelle loi soumet, à l'exception de données codées, le transfert de données personnelles dans le cadre de recherches médicales aux dispositions du droit commun prévu aux articles 68 à 70. La mise en œuvre est interdite en principe sauf si l'État (hors Union européenne) dans lequel se situe le destinataire des données assure un niveau de protection suffisant de *« la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent*

faire l'objet[364] ».

Ils doivent limiter la durée de conservation des données collectées à la durée nécessaire à la finalité du traitement. Les données traitées ne peuvent, en principe, pas être conservées sauf pour des faits historiques, statistiques ou scientifiques. Dans ce dernier cas, le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212 - 4[365] du code du patrimoine.

Les responsables de traitement des données médicales en cours de sanctions pénales en cas d'infraction.

2. Des sanctions pénales pour le non-respect des obligations

Des sanctions pénales sont prévues par la loi en cas de non-respect par le responsable du traitement de ses obligations vis-à-vis des personnes concernées. D'une part, l'article 226-19-1 du code pénal punit de 5 ans d'emprisonnement et 300 000 € d'amende (cette dernière pouvant aller jusqu'à 1 500 000 € lorsque le responsable du traitement est une personne morale) le fait de procéder à un traitement en matière de données personnelles collectées dans le cadre des recherches médicales :

- sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données personnelles sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des informations transmises et des destinataires des données ;
- malgré l'opposition de la personne concernée ou lorsqu'il est prévu par la loi, en l'absence de consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimée par celle-ci de son vivant.

D'autre part, la présentation des résultats du traitement de données ne doit, en aucun cas, permettre l'identification directe ou indirecte des personnes concernées. Les responsables de traitement ainsi que ceux qui y ont accès sont astreints au secret professionnel sous peine de

[364] Article 68 alinéa 1 de la loi informatique et libertés.

[365] *« Les archives publiques qui, à l'issue de la sélection prévue aux articles L. 212-2 et L. 212-3, sont destinées à être conservées sont versées dans un service public d'archives dans des conditions fixées par décret en Conseil d'État… »*

sanctions prévues par l'article 226 - 13 du code pénal[366] (un an d'emprisonnement et 1500 € d'amende).

Certaines catégories de traitements de données médicales font l'objet de procédures particulièrement réglementées par la loi informatique et libertés.

Paragraphe 2 : Les procédures spécifiques à certains traitements des données de santé

Tous les traitements de données personnelles de santé répondent à des formalités différentes selon leur finalité. Certaines sont soumises au régime de droit commun des articles 25 et 26 de la loi informatique et libertés. Ainsi, le responsable de traitement doit-il procéder à une déclaration préalable dans les cas suivants :

- lorsque la dérogation est fondée sur le consentement exprès de la personne ;
- pour les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par la suite d'une incapacité juridique ou d'une impossibilité matérielle ;
- pour les traitements portant sur des données à caractère personnel rendues publique par la personne concernée ;
- pour les traitements nécessaires aux fins de la médecine et mises en œuvre par un membre d'une profession de santé.

L'autorisation préalable de la CNIL ou l'adoption d'un arrêté ou d'un décret est requise dans les deux cas suivants :

- les traitements, automatisés ou non, justifiés par l'intérêt public ;
- les traitements avec processus d'anonymisation.

Tout comme tous les traitements de données soumis au régime de droit commun, les traitements sus-cités peuvent également bénéficier de dérogations comme les allégements prévus par les articles 23 et 24 de la loi informatique et libertés permettant de faire l'objet de

[366] « *La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende*. »

normes simplifiées[367] ou de recourir à une déclaration unique. Pour profiter d'une déclaration ou d'une autorisation unique[368], les responsables du traitement n'adressent qu'un simple engagement de conformité à la CNIL par Internet. La CNIL est particulièrement attentive au respect des conditions générales de licéité des traitements objet des articles 6 et 7 de la loi informatique et libertés, tant pour les déclarations que pour les demandes d'autorisation portant sur des données de santé.

La loi informatique et libertés a instauré des régimes d'autorisation distincts du régime prévu à l'article 25. C'est le cas des traitements ayant pour objet des recherches médicales d'une part (A) et ceux relatifs à l'évaluation des pratiques de soins, d'autre part (B).

A. La procédure spécifique aux traitements à des fins de recherches médicales

Cette procédure est régie par le chapitre IX de la loi informatique et libertés intitulé : *« traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé »*. Les dispositions de la loi s'appliquent, dans leur généralité, à ce type de traitement à l'exclusion des articles 23 à 26 (déclaration ou autorisation), 32 (information préalable) et 38 (droit d'opposition). Le champ d'application du chapitre IX[369] exclut les traitements de données pour le suivi individuel des patients (c'est-à-dire les traitements de

[367] La CNIL a adopté 4 normes simplifiées concernant les traitements mis en œuvre par les professionnels de santé : normes simplifiées n° 50 - délibération n° 2005-296 du 22 novembre 2005 portant adoption de normes simplifiées relatives au traitement automatisé 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; - normes simplifiées n° 52 - délibération n° 2006 - 161 du 8 juin 2006 portant adoption d'une norme simplifiée relative au traitement automatisé de données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de la pharmacie ; - normes simplifiées n° 53 - délibération n° 2006-162 du 8 juin 2006 portant adoption d'une norme simplifiée relative au traitement automatisé de données à caractère personnel mis en œuvre par les biologistes à des fins de gestion du laboratoire d'analyses de biologie médicale ; - normes simplifiées n°54 du 21 décembre 2006 relative au traitement automatisé de données à caractère personnel mis en œuvre par les opticiens lunetiers pour la gestion d'une activité professionnelle, JORF n° 45 du 22 février 2007. www.cnil.fr.

[368] Les autorisations uniques constituent pour les autorisations ordinaires, en quelque sorte, ce que sont les normes simplifiées pour les déclarations. Ce dispositif a été utilisé pour le traitement de données en matière de pharmacovigilance : Autorisation unique n°AU-013 - Délibération n° 2008-005 du 10 janvier 2008 portant autorisation unique de mise en œuvre par les entreprises ou organismes exploitants de médicaments de traitements automatisés de données à caractère personnel relatifs à la gestion des données de santé recueillies dans le cadre de la pharmacovigilance des médicaments postérieurement à leur mise sur le marché. 10 Janvier 2008. JORF n°0039 du 15 février 2008 p. texte n° 84 - NOR : CNIA0800002X.

[369] Les articles 53 à 61 de la loi du 6 janvier 1978 telle que modifiée par celle du 6 Août 2004.

données mises en œuvre par les professionnels de santé relatifs à leurs patients et qui relèvent du régime des exceptions de l'article 8) ainsi que les traitements liés à des études menées par les soignants sur les données de leurs patients (de travaux de recherche menés au sein des services hospitaliers est destiné à leur usage exclusif notamment pour une thèse de médecine).

En raison de la nature particulièrement intime des traitements de données médicales ayant pour finalité la recherche dans le domaine de la santé, ils sont soumis à des règles exorbitantes quant à la procédure d'autorisation et à la gestion du secret médical.

1. La procédure d'autorisation

Cette procédure se compose de deux phases successives : la sollicitation de l'avis du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé (CCTIRS) suivi de l'autorisation de la CNIL.

a. L'avis du CCTIRS

Le CCTIRS est un Comité consultatif institué auprès du ministre chargé de la Recherche. Il est composé de 15 personnes compétentes en matière de santé, d'épidémiologie, de génétique et de biostatistique[370]. Le CCTIRS est né de la modification par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 Août 2004. Il a été institué pour l'application des dispositions relatives aux traitements des données à des fins de recherche dans le domaine de la santé (nouveau chapitre IX de la loi informatique et libertés). Son rôle[371] est d'éclairer la CNIL sur la justification du traitement de données à caractère personnel dans un but de recherche.

A l'exclusion des recherches biomédicales, tout projet nécessitant le traitement de données à caractère personnel à des fins de recherche dans le domaine de la santé doit être

[370] Article 20 du décret 2005 - 1309 du 20 octobre 2005 pris pour l'application de la loi informatique et libertés. Également l'article 54, alinéa 1 de la loi informatique et libertés.

[371] Pour plus de détail sur le fonctionnement du CCTIRS, voir : BONAÏTI-PELLIE, Catherine, ARVEUX, Patrick. *Traitement de l'information en matière de recherche dans le domaine de la santé, nul n'est censé ignoré la loi*. In médecine/sciences 2009 n°1, volume 25, Janvier 2009. pp 93-97. Ou, voir en ligne http://www.edk.fr/reserve/print/e-docs/00/00/0D/54/document_article.md. Consulté le 18 septembre 2010.

soumis pour avis aux CCTIRS avant d'être examiné par la CNIL qui, seule peut délivrer l'autorisation. Par exemple, lorsqu'un médecin et une équipe de recherches souhaitent collaborer pour effectuer un projet de recherche à partir des données recueillies dans le cadre de la prise en charge d'un patient, le responsable du projet (en général, en passant par l'organisme dont il dépend) doit soumettre un dossier au CCTIRS avant de demander l'autorisation à la CNIL. Pour remplir sa mission, le Comité consultatif émet un avis *« sur la méthodologie de la recherche au regard des dispositions de la loi, la nécessité du recours à des données à caractère personnel et la pertinence de celles-ci par rapport à l'objectif de la recherche*[372] *»*. Le Président du Comité consultatif peut mettre en œuvre une procédure simplifiée[373].

En fonction de l'avis du CCTIRS, la CNIL pourra se prononcer ou non sur la nécessité de déroger au secret professionnel qui protège les données de santé et autoriser ou non le traitement envisagé. La plupart du temps les avis du CCTIRS sont favorables et assortis de recommandations. Mais, il peut arriver que plusieurs critiques soient faites à une demande. Dans ces cas, le Comité réserve son avis et met le dossier en attente. Seuls les dossiers ne satisfaisant pas aux normes minimales d'une recherche dans le domaine de la santé reçoivent une réponse défavorable. D'autres dossiers peuvent ne pas recevoir d'avis formel de la part du CCTIRS car il considère que ceux-ci ne relèvent pas de sa compétence. C'est le cas d'études complètement anonymes, de base de données sans projet de recherche, de dossier ne comportant pas de projet de recherche dans le domaine de la santé, etc…

La mission du Comité n'est pas toujours simple car il est parfois confronté à un

[372] Article 54 de la loi informatique et libertés.

[373] Cette procédure homologuée par la CNIL a été mise en place en février 2006, pour simplifier le travail des porteurs de projets en leur évitant une soumission à de multiples Comités. Il s'agissait d'une demande forte du CCTIRS qui avait noté que ces soumissions multiples d'un même projet étaient problématiques, les Comités concernés pouvant avoir éventuellement des avis divergents, et qui souhaitait que la procédure simplifiée, qui ne concernait jusqu'ici que certains essais cliniques, soit élargie à la majorité des recherches biomédicales, à condition que les CPP (Comités de protection des personnes) soient renforcés par des méthodologistes. La procédure simplifiée concerne les recherches biomédicales relevant des dispositions des articles L.1121-1 et suivants du code de la santé publique et qui doivent être obligatoirement soumises à un CPP. Dans ce cas, les organismes adressent directement à la CNIL un engagement de conformité à la méthodologie de référence MR-001 pour les traitements de données personnelles opérés dans le cadre de recherches biomédicales (www.cnil.fr/index.php ?id=2365). Un certain nombre de traitements en sont exclus, en particulier ceux qui font apparaître l'identité complète de la personne, les recherches en génétique ayant pour objectif l'identification des personnes, et les recherches dont l'objectif principal est l'étude des comportements. BONAÏTI-PELLIE, Catherine, ARVEUX, Patrick. *Traitement de l'information en matière de recherche dans le domaine de la santé : nul n'est censé ignoré la loi. Op cit p. 95.*

souci de limite de ses compétences[374]. Dans une communication de madame BONAÏTI-PELLIE, Présidente du CCTIRS, sans méconnaître cette difficulté, elle fait remarquer qu'*«au fil du temps et des lois, les missions du CCTIRS ont été modifiées, sa manière de fonctionner a évolué, mais le principe est toujours celui de protéger l'individu, non dans son intégrité physique, ce dont sont chargés les Comités de protection des personnes (CPP[375]), mais de la divulgation des données concernant sa santé[376]* ».

Le dossier de demande de l'avis, signé par la personne ayant qualité pour représenter l'organisme de recherche, doit comprendre[377] :

- l'indication du nom de l'organisme public ou privé qui met en œuvre le traitement et, s'il est établi à l'étranger, le nom de son représentant en France ; l'identité de la personne responsable de la mise en œuvre du traitement, ses titre, expérience et fonction ; les catégories de personnes qui seront appelées à mettre en œuvre le traitement ainsi que celles qui auront accès

---

[374] Pour M. JOB, Jean-Marie, que le Comité n'a pas de difficulté, face à un protocole de recherche, à se prononcer sur la nécessité de recourir à des données personnelles et non à des données anonymes (du fait de la nécessité de pouvoir remonter à la donnée « source » pour un contrôle de qualité par exemple) ou sur la pertinence de telle ou telle donnée. Cela est dû à la compétence des personnes qui le composent. Pourtant, le Comité a tendance à se prononcer sur l'intérêt scientifique ou sur la méthodologie d'une recherche, voire sur son opportunité même, alors que sa première mission est de donner uniquement son avis « sur *la méthodologie de la recherche* » au regard de la loi informatique et libertés. JOB, Jean-Marie. *La loi « informatique et libertés » et les données de santé*. Revue Lamy droit de l'immatériel du 1er janvier 2008, n°34 p.86.

[375] Les Comités de protection des personnes (CPP) – qui remplacent désormais les Comités consultatifs de protection des personnes dans la recherche biomédicale (CCPPRB) – sont des acteurs essentiels du nouveau dispositif d'encadrement de la recherche biomédicale. La loi du 9 août 2004 leur confie, en effet, de facto, un rôle de co-décideur dans l'autorisation des recherches biomédicales. http://www.recherche-biomedicale.sante.gouv.fr/pro/comites/accueil.htm. Consulté le 5 avril 2014.

[376] BONAÏTI-PELLIE, Catherine, ARVEUX, Patrick. *Traitement de l'information en matière de recherche dans le domaine de la santé : nul n'est censé ignoré la loi*. *Op cit. p.93.* Et, la Présidente d'expliquer plus loin que « *Le Comité était initialement envisagé comme un Haut Comité sur l'Information en Santé, capable de rendre des décisions au nom de l'intérêt public. Au fur et à mesure de l'élaboration du projet de loi, nombre d'objections ont été apportées à ces propositions. En effet, celui-ci ne devait déborder ni sur la CNIL qui conservait l'autorité, ni sur les Comités qui jugeaient de la protection des personnes, ni sur les Comités scientifiques des promoteurs qui se portent garants de la valeur scientifique. Au final, il a été décidé que le Comité serait une structure légère et réactive visant à enrichir la réflexion de la CNIL, et à l'aider dans sa décision d'autoriser ou non le traitement, en proposant un avis d'experts qui porte à la fois sur la nature des informations médicales utilisées et sur leur intérêt pour la recherche envisagée. C'est ainsi qu'en définitive la mission du CCTIRS n'inclut pas un avis sur la pertinence de la recherche, comme cela avait été initialement prévu Il est à noter que le Comité est malgré tout régulièrement confronté à cette problématique et ce n'est qu'à regret que les scientifiques qui le composent s'interdisent de se prononcer sur l'intérêt d'une recherche. Étant donné la composition du Comité et le nombre très restreint de ses membres, qui ne peuvent évidemment pas couvrir l'ensemble des domaines de recherche en santé, les membres sont conscients qu'il ne serait ni possible ni légitime de juger de la pertinence de tous les projets de recherches qui lui sont soumis. » p. 94. http://www.edk.fr/reserve/print/e-docs/00/00/0D/54/document_article.md*

[377] CNIL. *Renseignements pratiques sur les formalités préalables à la création d'un fichier de recherche médicale.* p.5. http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/sante/chapIX.pdf Consulté le 5 avril 2014.

aux données ;

- le protocole de recherche ou ses éléments utiles, indiquant notamment l'objectif de la recherche, la population concernée, la méthode d'observation retenue, l'origine et la nature des données à caractère personnel recueillies et la justification de recours à celles-ci, la durée et les modalités d'organisation de la recherche, la méthode d'analyse des données ;
- les avis rendus antérieurement par des instances scientifiques ou éthiques, et notamment, le cas échéant, par le Comité national des registres.

Ce dossier doit être envoyé en recommandé avec accusé de réception, ou dépôt au secrétariat du Comité, à l'adresse du Comité consultatif sur le traitement de l'information en matière de recherche dans le domaine de la santé.

Le Comité dispose d'un délai de deux mois pour notifier son avis. Passé ce délai, l'avis est réputé favorable. En cas d'urgence, ce délai peut être ramené à 15 jours. Si le dossier déposé n'est pas complet, le Comité adresse à l'organisme concerné une demande motivée d'informations complémentaires : dans ce cas, le point de départ du délai est reporté à la date de réception des informations complémentaires.

Le CCTIRS a rédigé en avril 2007 un mode d'emploi détaillant l'ensemble des étapes de la procédure d'expertise. L'objectif de ce document est de faciliter la tâche des responsables de projets et de faire gagner du temps tant aux demandeurs qu'aux évaluateurs. Il est régulièrement mis à jour et est accessible sur le site[378] du ministère de l'enseignement supérieur et de la recherche.

Une fois l'avis du Comité obtenu, le responsable du traitement doit obtenir l'autorisation de la CNIL. Cette dernière n'est pas liée par l'avis du Comité. Il est donc possible de saisir la CNIL en présence d'un avis défavorable du Comité[379].

b. L'autorisation de la CNIL

L'autorisation de la CNIL est l'étape la plus importante de cette procédure car sans elle, le traitement serait illégal. Les projets de recherche sont soumis à une autorisation non pas tacite mais expresse de la CNIL. Les modalités de cette procédure sont fixées aux articles

[378] www.enseignementsup-recherche.gouv.fr/cid20537/cctirs.html. Consulté le 5 avril 2014.

[379] JOB, Jean-Marie. *La loi « informatique et libertés » et les données de santé*. Revue Lamy droit de l'immatériel du 1er janvier 2008, n°34 p.87.

34 à 35 du décret n° 2005 - 1309 du 20 octobre 2005[380] tel que modifié par celui du 25 mars 2007[381] en dehors des dispositions de la loi informatique et libertés.

L'article 54 de la loi informatique et libertés dispose que *« la mise en œuvre du traitement de données est ensuite soumise à l'autorisation de la Commission nationale de l'informatique et des libertés qui se prononcent dans les conditions prévues à l'article 25 »*. L'article 53 écarte l'application de l'article 25 quant à la demande d'autorisation en matière de recherche dans le domaine de la santé. Mais, les dispositions de l'article 54 indiquent que la CNIL statue selon la procédure de l'article 25 juste pour en garder le principe de l'autorisation, le délai, et notamment que le silence gardé par la CNIL pendant deux mois vaut un rejet. La stricte application de l'article 25 n'aurait pas permis l'intervention du Comité consultatif et le mécanisme des autorisations uniques aurait été appliqué en la matière alors que le dispositif utilisé est celui *«des méthodologies de référence* ». C'est un mécanisme similaire à celui des autorisations uniques mais qui n'existait pas dans la loi informatique et libertés avant les modifications de 2004. « *Ces méthodologies précisent, l'écart eu égard aux caractéristiques mentionnées à l'article 30, les normes auxquelles doivent correspondre des traitements pouvant faire l'objet d'une demande d'avis et d'une demande d'autorisation simplifiées*[382] ». Le mécanisme permet ainsi, d'alléger et de simplifier la procédure pour les recherches les plus courantes mais à condition de ne pas permettre l'identification directe des personnes concernées par le traitement. Ces personnes ne doivent être désignées que par un numéro de référence ou des initiales, par exemple.

Les méthodologies de référence sont homologuées et publiées par la CNIL pour préciser les caractéristiques des traitements pouvant faire l'objet d'une demande d'avis ou d'une demande d'autorisation simplifiée. Elles sont établies en concertation avec le Comité consultatif et des organismes publics et privés représentatifs tels que l'INSERM.

Tout comme les normes simplifiées ou les autorisations uniques, les méthodologies de références fixent la ou les finalités du traitement, le cas échéant les interconnexions, les rapprochements ou la mise en relation, les données pouvant être

[380] 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 204. JORF n° 247 du 22 octobre 2005. p. 16769. NOR : JUSC0520586D.

[381] Décret n° 2007 - 451 du 25 mars 2007 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, modifiée par la loi n° 2004-801 du 6 août 2004. NOR : JUSC0720211D. JORF n°74 du 28 mars 2007 p. 5782 texte n° 30.

[382] Article 54 alinéa 5.

collectées et traitées, l'origine des données, leurs destinataires, les modalités d'information des personnes, les conditions d'exercice de leur droit d'accès et de rectification, les services mettant en œuvre le traitement, les mesures de sécurité et les éventuels transferts hors Union européenne. Après la publication de la méthodologie, le responsable de traitement intéressé n'adresse (y compris par voie électronique) à la CNIL qu'un engagement de conformité à l'ensemble des obligations fixées par la méthodologie de référence.

Ce dispositif a le mérite de simplifier également l'activité de la CNIL, notamment dans le domaine des essais cliniques de nouveaux médicaments. La méthodologie référencée MR-001[383] de janvier 2006 est la seule, à ce jour, à avoir été publiée. Elle couvre les *« traitements de données personnelles opérées dans le cadre des recherches biomédicales*[384] *».* Les données concernées sont, non seulement, celles des personnes qui participent à la recherche mais aussi celles des investigateurs (médecins mettant en œuvre la recherche) et les données des professionnels intervenant pour le déroulement de la recherche. Cette procédure simplifiée s'applique à toutes les recherches biomédicales - y compris les essais de pharmacogénétiques - relevant des dispositions des articles L. 1121 -1 et suivants du code de la santé publique et qui doivent être obligatoirement soumis à un comité de protection des personnes. Par contre, les traitements qui font apparaître l'identité complète de la personne, les recherches en génétique ayant pour objectif l'identification des personnes, et les recherches dont l'objectif principal est l'étude des comportements en sont exclues.

L'article 54 a prévu une possibilité de simplifier les formalités pour les catégories de traitement n'entrant pas dans le champ d'application des méthodologies de référence. Le Comité consultatif fixe, dans ce cas, en concertation avec la CNIL, les conditions dans lesquelles son avis n'est pas requis. Cette distinction n'est pas toujours aussi simple pour les

---

[383]CNIL. *Méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales*. Octobre 2010. p. 4. http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/sante/MR-001.pdf. Consulté le 18 avril 2014.
Voir également, FAURAN, B. *Loi informatique et libertés et données de recherche dans le domaine de la santé* : Gazette du palais 2006,1, doctrine, p.1698. – PERRAY, R. *Traitement de données personnelles dans le cas des recherches médicales : vers un allégement des formalités* : revue Lamy droit de l'immatériel février 2007. P. 64

[384] La loi « Huriet-Sérusclat » du 20 décembre 1988 (JORF du 22 décembre 1988, p. 16032) modifiée par la loi n° 2004 - 806 du 9 août 2004 (JORF du 11 Août 2004 et rectificatif JORF 12 août 2004) relative à la politique de santé publique et son décret d'application n° 2006 - 477 du 26 avril 2006 ainsi que les arrêtés et décisions s'y rapportant constituent le dispositif légal qui régit la mise en œuvre des recherches biomédicales en France. La loi du 9 Août 2004 et son décret d'application sont entrés en vigueur le 27 août 2006. Les dispositions concernant la recherche biomédicale sont incluses dans la loi du 9 août 2004 relative à la politique de santé publique (article L. 1121-1 à L. 1126-11). http://www.recherche-biomedicale.sante.gouv.fr/pro/guide/guide-1.htm. Consulté le 18 avril 2014

responsables de projet qui se retrouvent, soit à solliciter le Comité pour des recherches entrant dans le cadre des méthodologies de référence, soit à demander à bénéficier de la procédure simplifiée alors qu'elles relèvent du champ d'application des méthodologies de référence[385].

Le dossier de demande d'autorisation, signé par la personne ayant qualité pour représenter l'organisme de recherche, doit comprendre[386] :

- le protocole de recherche ou ses éléments utiles, indiquant notamment l'objectif de la recherche, la population concernée, la méthode d'observation ou d'investigation retenue, l'origine et la nature des données à caractère personnel recueillies et la justification du recours à celles-ci, la durée et les modalités d'organisation de la recherche, la méthode d'analyse des données (il s'agit, en partie, du double du dossier transmis au Comité, complété des éléments décrits ci-après) ;
- l'avis rendu par le Comité consultatif où l'accusé de réception de la demande d'avis lorsque le Comité consultatif a rendu un avis tacitement favorable ;
- les mesures envisagées pour informer individuellement les personnes concernées par le traitement, avant le début de celui-ci : de la nature des informations transmises, de la finalité du traitement, des personnes physiques ou morales destinataires des données, du droit d'accès et de rectification, du droit d'opposition ou, dans les cas de recherches faisant appel à des prélèvements biologiques identifiants, de l'obligation de recueillir le consentement éclairé et exprès. Toute demande de dérogation à cette obligation d'information doit être justifiée auprès de la Commission ;
- les caractéristiques du traitement et en particulier, le descriptif des moyens informatiques

[385] Mme BONAÏTI a déploré le fait que depuis la mise en place de la procédure simplifiée plusieurs études pouvant en bénéficier aient été adressées au Comité, la plupart du temps en raison d'une mauvaise connaissance de la procédure. Le problème est particulier en matière de projets de recherche s'accompagnant de la constitution d'une banque d'ADN. Il ressort d'une discussion avec la CNIL que la constitution de cette banque est directement justifiée par la recherche biomédicale envisagée, celle-ci bénéficiant alors bien de la procédure simplifiée. À l'inverse, les exclusions la méthodologie de référence ne sont pas toujours bien perçues des chercheurs ni même des organismes. Certains membres du Comité découvrent fortuitement lors des propositions de collaboration, des recherches biomédicales qui auraient dû être soumises au Comité. En effet, des recherches entrant dans l'un des motifs d'exclusion (étude des maladies psychiatriques, étude dans laquelle le nom complet de la personne apparaissait dans un fichier de recherche etc.) ne l'ont pas été. Les responsables du traitement ont-ils considéré, à tort que les recherches étaient couvertes par l'engagement de conformité à la méthodologie de référence ou les responsables de la recherche ont-ils omis d'avertir leur organisme de leur recherche ? C'est une question à laquelle le Comité ne peut répondre pour l'instant avec les moyens dont il dispose. BONAÏTI-PELLIE, Catherine, ARVEUX, Patrick. *Traitement de l'information en matière de recherche dans le domaine de la santé : nul n'est censé ignoré la loi*. p. 95. http://www.scribd.com/doc/31033917/CCTIRS-MS-2009 . Consulté le 5 avril 2014.

[386] CNIL. *Renseignements pratiques sur les formalités préalables à la création d'un fichier de recherche médicale.* p.6. http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/sante/chapIX.pdf. Consulté le 5 avril 2014.

utilisés (micro-ordinateurs, recours à des réseaux...) ;
- les rapprochements, interconnexions ou toute autre forme de mise en relation des informations ;
- la disposition prise pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi ainsi que la justification scientifique et technique de toute demande de dérogation à l'obligation de codage des données et la justification de toute demande de dérogation à l'interdiction de conservation des données sous une forme nominative au-delà de la durée nécessaire à la recherche ;
- la mention de toute expédition de données à caractère personnel, non codées vers un État appartenant à la Communauté européenne.

Il convient de constituer le dossier de demande d'autorisation selon les indications précitées et en utilisant le formulaire de demande d'autorisation qui est également disponible auprès de la CNIL. Ce dossier doit être envoyé en un exemplaire en recommandé avec accusé de réception ou déposé à l'accueil de la CNIL.
La Commission dispose d'un délai de deux mois éventuellement renouvelables une fois, pour notifier son autorisation. A défaut de décision dans ce délai, son silence vaut décision de rejet. L'autorisation doit mentionner notamment les dérogations accordées en matière de codage des données, de conservation de données sous forme nominative et d'information des personnes concernées.
Si le dossier déposé n'est pas complet, la CNIL adresse à l'organisme concerné une demande motivée d'informations complémentaires : dans ce cas, le point de départ du délai est reporté à la date de réception des informations complémentaires.

A l'issue de cette analyse, il nous a paru important de reprendre quelques phrases de la communication de la présidente BONAÏTI pour rappeler l'importance de cette procédure quant à la sécurité des données de santé : *« nous voudrions souligner qu'il serait judicieux d'utiliser le passage successif des études devant ces deux instances, le CCTIRS et la CNIL, comme une garantie de la qualité méthodologique d'une part, et de la protection des personnes contre la divulgation abusive de leurs données de santé d'autre part. Cette particularité de la loi française s'accorde parfaitement avec la déclaration d'Helsinki*[387]*, et la*

[387] Déclaration d'Helsinki adoptée par la 18e Assemblée générale de l'AMM, Helsinki, Finlande, Juin 1964. C'est le document politique le plus connu de l'AMM (Association médicale mondiale). La Déclaration a été amendée à six reprises depuis, le dernier amendement datant de l'Assemblée Générale de Séoul, en Corée, d'octobre 2008. C'est la seule version officielle à ce jour et toutes celles qui sont antérieures sont caduques et ne

combinaison CCTIRS - CNIL assure un niveau de protection scientifique et éthique largement équivalent au modèle « Institutional review board/Independant ethics committee » en vigueur aux États-Unis. A ce sujet, le CCTIRS est conscient de sa responsabilité pour éviter à des personnes de participer à des recherches qui n'auraient aucune chance d'aboutir et qui risqueraient de porter atteinte inutilement à leur vie privée. Ce point éthique est le moteur principal des avis défavorables qui sont prononcés. »[388]

La procédure de demande d'autorisation à la CNIL n'est pas une étape banale en ce sens que le non-respect des règles applicables en la matière conduit à des sanctions administratives. La mise en œuvre d'un traitement de données en violation des conditions prévues aux articles 53 et suivants de la loi informatique et libertés est susceptible d'entraîner le retrait temporaire ou définitif par la CNIL de l'autorisation qu'elle a délivrée. Il en est de même en cas de refus du responsable de traitement de se soumettre au contrôle sur place que la Commission envisage d'effectuer[389].

Lorsque le responsable du traitement obtient l'autorisation requise, la mise en œuvre est marquée par la possibilité d'une dérogation au secret médical.

2. La dérogation au secret médical

Le secret médical reste l'une des meilleures garanties pour la préservation de la vie privée des personnes dont les données de santé sont prélevées. C'est une obligation d'ordre public qui s'impose aux médecins, qui est sanctionnée pénalement et que la personne concernée ne peut valablement lever par son seul consentement. Pourtant, dans le cadre d'une recherche dans le domaine médical, le législateur a permis aux professionnels de santé de déroger à ce principe. En effet, l'article 55 de la loi informatique et libertés dispose 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*

---

doivent être utilisées qu'à des fins historiques. C'est « *un énoncé de principes éthiques applicables à la recherche médicale impliquant des êtres humains, y compris la recherche sur du matériel biologique humain et sur des données identifiables* ». http://www.wma.net/fr/30publications/10policies/b3/index.html. Consulté le 05 octobre 2010.

[388] BONAÏTI-PELLIE, Catherine, ARVEUX, Patrick. *Traitement de l'information en matière de recherche dans le domaine de la santé : nul n'est censé ignoré la loi.* p. 96 http://www.scribd.com/doc/31033917/CCTIRS-MS-2009 . Consulté le 05 octobre 2010.

[389] Article 60 de la loi informatique et libertés.

traitement de données autorisé en application de l'article 53» ; cet article portant sur le traitement des données ayant pour fin la recherche dans le domaine de la santé.

Pour autoriser cette dérogation le législateur a dû se rendre à l'évidence que dans le cadre d'une recherche, les professionnels de santé sont nécessairement amenés à échanger des résultats ou à les transmettre au responsable. Or, ces résultats sont, pour l'essentiel, des données personnelles qui sont protégées par le secret professionnel. Cette contradiction constituait alors un frein à la bonne marche de la recherche. C'est d'ailleurs, la raison pour laquelle la législation en vigueur est le résultat d'une évolution due à plusieurs plaintes déposées auprès de la CNIL par des patients qui craignaient un risque d'atteinte au secret médical[390] d'un côté et d'un autre, des chercheurs qui déploraient la gêne occasionnée par l'obstacle d'ordre juridique qui leur interdisait de se transmettre les données.

Tandis que le Comité national d'éthique et le Conseil national de l'ordre des médecins espéraient élargir à nouveau, le concept de secret partagé[391], le législateur avait préféré s'orienter vers une nouvelle dérogation au secret médical en veillant à ce que toute restriction soit exclusivement définie et cantonnée à une application particulière. *« Le dispositif proposé commence par préciser que le secret professionnel ne fait pas obstacle à la transmission de données de santé nominatives. Il propose donc une exception au secret professionnel qui concerne non seulement les médecins, mais également toutes les professions de santé qui sont, elles aussi, astreintes au secret professionnel. Ce faisant, il autorise par exemple, les biologistes des laboratoires d'analyses médicales à transmettre des données de santé et permet donc d'élargir le plus possible le champ de données accessibles à la recherche. »*[392]

---

[390] Cnil, 13éme rapport annuel d'activités. p. 251 ; 14éme rapport annuel d'activités. p. 244.

[391] Le concept de secret partagé n'a pas une origine légale mais il a été voulu par les praticiens de santé. *«Le principe de l'inviolabilité du secret médical reconnaît un droit fondamental du patient : le respect de sa vie privée. Le « secret partagé » n'a aucune base légale ou réglementaire et s'oppose au caractère général et absolu du secret médical. Mais le partage de l'information entre professionnels de santé s'est imposé, au cours des siècles, dans la pratique quotidienne, afin d'assurer la continuité des soins et d'améliorer leur qualité dans l'intérêt des patients. L'exercice pluridisciplinaire a accentué cette tendance. »* Docteur Aline MARCELLI. *Rapport adopté lors de la session du Conseil national de l'Ordre des médecins de mai 1998* http://www.web.ordre.medecin.fr/rapport/secretpart.pdf. Consulté le 28 mai 2014.

[392] TÜRK, Alex. Rapport n° 209. (1993 - 1994) ou rapport n° 397. p.15. Projet de loi relatif au traitement de données nominatives ayant pour fin la recherche en vue de la protection ou l'amélioration de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. 21 décembre 1993. p.8. Sommaire du rapport en ligne sur www.senat.fr. Consulté le 26 mai 2014

Le partage du secret est ouvert à l'INSEE et les services statistiques ministériels par la lettre de l'article 7 bis de la loi[393] du 7 juin 1951 modifiée par ordonnance n°2004-280 du 25 mars 2004 relative aux simplifications en matière d'enquêtes statistiques. Pourtant, cela avait été dénoncé par la Commission des lois du Sénat et la CNIL quand elle était admise sous la version initiale de la loi du 7 juin 1951. Cette extension n'avait, alors, pas été reprise par la modification du 23 décembre 1986[394] ni par la loi du 1er juillet 1994[395]. Pour les deux institutions, ni l'INSEE, ni l'ensemble des services statistiques ministériels n'avaient vocation à traiter les données de santé. Il était contestable de classer les traitements réalisés par ceux-ci en vue de la réalisation d'études statistiques dans la catégorie des traitements ayant pour fin la recherche dans le domaine de la santé. Les services déjà concernés par la recherche médicale leur semblaient suffisamment habilités à mettre en œuvre les traitements en question.

Si le législateur se soucie de faciliter la tâche aux professionnels de santé, il n'a pas, pour autant, négligé les droits et libertés des personnes titulaires des données à traiter. Ainsi, l'article 56 de la même loi dispose : *« toute personne a le droit de s'opposer à ce que les données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel rendue nécessaire par un traitement de la nature de ceux qui sont visés à l'article 53 »*. Il revient donc, finalement, à la personne concernée de décider de la levée ou non du secret médical quant au traitement de ses données personnelles.

Le même souci de garantir la sécurité de l'individu accompagne la procédure relative aux traitements à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention.

---

[393] Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. JORF du 8 juin 1951. p. 6013.

[394] La loi n° 86-1305 du 23 décembre 1986, JORF du 26 décembre 1986 page 15596 modifiant celle du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques l'avait interdit en son article 7bis *: « Les informations relatives aux personnes physiques, à l'exclusion des données relatives à la santé ou à la vie sexuelle, et celles des personnes morales, recueillies dans le cadre de sa mission, par une administration, un établissement public, une collectivité territoriale ou une personne morale de droit privé gérant un service public peuvent être cédées, à des fins exclusives d'établissement de statistiques, à l'Institut national de la statistique et des études économiques ou aux services statistiques ministériels (..) »*

[395] 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 no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF n° 152 du 2 juillet 1994. p. 9559. NOR : RESX9200045L.

B. La procédure spécifique aux traitements à des fins d'évaluation ou d'analyse des pratiques ou activités de soin et de prévention

Issues de la loi du 27 juillet 1999[396], les règles relatives aux traitements des données de santé à caractère personnel effectués à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention font l'objet du chapitre X de la loi informatique et libertés. Il s'agit des articles 62 à 66. Ces dispositions ont pour objectif d'encadrer le développement des programmes informatisés de médicalisation dans les établissements de soins. Elles veillent à préciser les conditions dans lesquelles les données de santé, qu'elles soient issues des fichiers des professionnels de santé, des systèmes d'information hospitaliers, ou des fichiers des caisses de sécurité sociale, peuvent être diffusées et exploitées à des fins d'évaluation des pratiques de soins et de prévention. Ainsi, ces règles s'appliquent-elles à tous les traitements publics ou privés de données de santé ayant pour fin l'évaluation des pratiques de soins et de prévention à l'exclusion des *« traitements de données à caractère personnel effectués à des fins de remboursement ou de contrôle par les organismes chargés de la gestion du régime de base d'assurance maladie et des traitements effectués au sein des établissements de santé par le médecin responsable de l'information médicale dans les conditions prévues au deuxième alinéa de l'article L. 6113 - 7 du code de la santé publique*[397]» (en pratique, ce sont les informations issues des RUM[398] et des RSS[399]).
Dans un document[400] élaboré par la CNIL en vue de renseigner en la matière, elle donne des exemples entrant dans le champ d'application du chapitre X. « *Ces traitements peuvent être constitués à partir :*
- des données issues des systèmes d'information visées à l'article L. 6113 - 7 du code de la

[396] Loi n° 99 - 641 portant création d'une couverture maladie universelle. JORF n° 172 du 28 juillet 1999. p. 11229. NOR: MESX9900011L.

[397] Article 62 alinéa 2 de la loi informatique et libertés.

[398]Résumé d'unité médicale.

[399] Résumé de sortie standardisée.

[400] CNIL. Renseignements pratiques sur la procédure de déclaration de traitements de données à caractère personnel de santé à des fins d'évaluation ou d'analyse des pratiques de soins et de prévention, chapitre X, édition de juillet 2006. p.3. https://www.formulaires.modernisation.gouv.fr/gf/getNotice.do?cerfaFormulaire=13890&cerfaNotice=51353. Consulté le 19 avril 2014.

santé publique (c'est-à-dire des résumés de sortie anonyme (RSA) du PMSI[401]) diffusée par l'ATIH[402] qui ne communique les données du PMSI que si le demandeur a préalablement obtenu l'accord de la CNIL conformément aux dispositions du chapitre X.

- des données issues des dossiers médicaux détenus dans le cadre de l'exercice libéral de professions de santé et,

- des données issues des systèmes d'information des caisses d'assurance maladie.

La communication des nom, prénom et NIR des personnes reste exclue : les traitements concernés ne peuvent servir à des fins de recherche ou d'identification des personnes.»

S'agissant des exclusions, le document cite à titre d'exemple :

- les traitements ayant pour finalité la recherche dans le domaine de la santé (chapitre IX),

- les applications qui nécessitent un contact avec le patient et qui permettraient de l'identifier directement dans la mesure où le fichier n'est plus constitué alors à partir de données issues des bases de données déjà existantes et énumérées par la loi.»

Le champ d'application ainsi établi est strictement limité à la finalité du traitement : *« l'évaluation des pratiques de soins et de prévention »*. L'objectif des traitements doit être de mesurer ce qui a déjà été fait en matière de soins et ce qui va être fait et non de chercher à trouver une réponse à certaines interrogations ; ce qui constituerait une recherche et relèverait donc des dispositions du chapitre IX. La limite entre ces deux types de traitement étant très restreinte, la solution qui s'offre au responsable des traitements est de solliciter la CNIL pour une analyse au cas par cas ; cela à partir de la procédure de demande d'autorisation.

1. L'autorisation de la CNIL

Préalablement à tout traitement, le responsable doit requérir une autorisation de la CNIL. Celle-ci s'obtient à la suite d'un contrôle effectué par la Commission. En effet, l'article 64 lui confère un pouvoir de décision plus important que celui de l'article 25 car elle exerce

[401] Programme de médicalisation des systèmes d'information hospitaliers.

[402] Agence technique de l'information sur l'hospitalisation. C'est un établissement public créé par le décret n° 2000 - 1282 du 6 décembre 2000, placé sous la tutelle des ministres chargés de la santé et de la sécurité sociale. Deux missions lui sont assignées : la prise en charge des travaux concourant à la mise en œuvre et à l'accessibilité aux tiers du système d'information commun État - Assurance maladie, et la participation aux travaux relatifs aux nomenclatures de santé. Décret n° 2000 - 1282 du 6 décembre 2000 *portant création de l'agence technique pour l'information sur l'hospitalisation et modifiant le code de la santé publique (deuxième partie: Décret en Conseil d'État).* JORF n° 301 du 29 décembre 2000. p. 20814. Texte n° 15. NOR: MESH0023447D.

un contrôle d'opportunité extrêmement rigoureux. La Commission « *vérifie les garanties présentées par le demandeur et, le cas échéant, la conformité de sa demande à ses missions ou à son objectif social.* » Si le demandeur sollicite une dérogation au principe de transmission de données agréées ou anonymes, *«la CNIL s'assure de la nécessité de recourir à des données à caractère personnel et de la pertinence du traitement au regard de la finalité déclarée d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention. Elle vérifie que les données à caractère personnel dont le traitement est envisagé ne comportent ni le nom, ni le prénom de personnes concernées, ni le numéro d'inscription au répertoire nationale d'identification des personnes physiques. En outre, si le demandeur n'apporte pas d'éléments suffisants pour attester la nécessité de disposer de certaines informations parmi l'ensemble des données à caractère personnel dont le traitement est envisagé, la Commission peut interdire la communication de ces informations par l'organisme qui les détient et n'autoriser que le traitement des données ainsi réduites».*

La CNIL fixe la durée de conservation des données et apprécie les précautions prises par le demandeur en vue d'assurer la sécurité des données, leur confidentialité et le secret professionnel[403].

L'article 65, alinéa 2 autorise la CNIL à adopter des décisions uniques pour *« des traitements répondant à une même finalité portant sur des catégories de données identiques et ayant des destinataires ou des catégories de destinataires identiques ».* Cette disposition emporte facilement l'approbation de la CNIL qui est très souvent favorable lorsque les responsables des traitements sollicitent une décision unique compte tenu du caractère répétitif de certaines études qui lui sont soumises.

Le document «*Renseignements pratiques sur la procédure de déclaration de traitements de données à caractère personnel de santé à des fins d'évaluation ou d'analyse des pratiques de soins et de prévention*[404]» indique la composition du dossier de demande d'autorisation. Celui-ci doit être signé par la personne ayant qualité pour représenter l'organisme public ou privé sollicitant la communication de données précitées. Il doit comprendre :

- le formulaire sur lequel sera cochée la case « demande d'autorisation »

[403] Article 64 in fine de la loi informatique et libertés

[404] Renseignements pratiques sur la procédure de déclaration de traitements de données à caractère personnel de santé à des fins d'évaluation ou d'analyse des pratiques de soins et de prévention, chapitre X, édition de juillet 2006. www.cnil.fr. Op cit p. 4

- les annexes rédigées sur papier libre et apportant toute précision sur :

- le nom de l'organisme public ou privé qui demande la communication de données et qui met en œuvre le traitement. S'il est établi à l'étranger, le nom du représentant en France devrait être indiqué,
- les missions ou l'objet social de l'organisme, identité et les fonctions de la personne responsable de la mise en œuvre du traitement et les catégories des personnes qui auront accès aux données,
- un descriptif de la finalité du traitement et la population qu'il concerne : la nature des données de santé à caractère personnel dont le traitement est envisagé et la justification du recours à celles-ci,
- la durée souhaitée de la conservation et leurs méthodes d'analyse ; l'identification des personnes, services ou organismes qui en sont détenteurs et qui sont susceptibles de les communiquer au demandeur si celui-ci est autorisé à mettre en œuvre le traitement ; la description du type de diffusion ou de publication des résultats du traitement envisagé le cas échéant par le demandeur est nécessaire,
- les caractéristiques techniques du traitement,
- les rapprochements ou interconnexions envisagés ou toute autre forme de mise en relation des informations,
- les dispositions prises pour assurer la sécurité des traitements et des informations et la garantie des secrets protégés par la loi. La CNIL met à la disposition du demandeur un modèle d'engagement de confidentialité qui permet de répondre aux exigences de la loi (joint en annexe).
- la mention de toute expédition d'information indirectement nominative entre la France et l'étranger, sous quelque forme que ce soit, y compris lorsque le traitement est l'objet d'opérations partiellement effectuées sur le territoire français à partir d'opérations antérieurement réalisées hors de France.

Toute modification doit être portée à la connaissance de la Commission.

«*La CNIL dispose d'un délai de deux mois, éventuellement renouvelable une fois, pour notifier son autorisation. A défaut de décision dans ce délai, son silence vaut décision de rejet. Si les dossiers déposés ne sont pas complets et/ou nécessitent des précisions, la Commission adresse à l'organisme concerné une demande motivée d'informations complémentaires : dans ce cas, le point de départ du délai correspond à la date de réception*

des informations complémentaires[405] ».

L'article 65, alinéa 1 précisant le délai d'attente d'une notification d'autorisation implique, comme pour l'autorisation requise dans le cadre de la recherche dans le domaine de la santé, que l'autorisation de la CNIL soit expresse et non tacite. Ces dispositions ont été inspirées par la décision du Conseil Constitutionnel du 18 juin 1995[406] qui est elle-même fondée sur un principe de base en droit administratif : « le silence de l'administration vaut rejet de la demande et non son acceptation ». En effet, saisi de l'examen de la loi du 21 janvier 1995[407] sur la sécurité, le Conseil Constitutionnel avait considéré, à propos de la demande d'autorisation prévue auprès du préfet pour la mise en place des systèmes de vidéosurveillance, qu'une telle autorisation devrait être expresse s'agissant d'un domaine touchant aux libertés individuelles et publiques.

Finalement, force est de constater qu'en l'état actuel de la législation en matière d'autorisation de la CNIL, des efforts ont été faits pour alléger les procédures. Ce qui amène à dire que le législateur a tenu compte des observations qui avaient été faites par la doctrine quant à l'alourdissement des procédures en matière de demande d'autorisation. Par exemple, les Maîtres MOLE et BENSOUSSAN avaient jugé les formalités trop lourdes face à la multitude de procédures à suivre pour la mise en œuvre de traitements automatisés de données nominatives avant la transposition de la directive européenne de 1995[408]. Notamment, la loi française imposait une obligation déclarative pour le secteur privé, une obligation de demande d'avis pour le secteur public, un régime d'autorisation tacite pour la recherche en matière de santé, et un régime d'autorisation expresse pour l'évaluation des pratiques de santé. La CNIL elle-même, avait émis quelques craintes quant à la complexité des formalités à l'occasion de l'examen du projet de loi relative à la couverture maladie universelle, par la délibération du 18 février 1999[409]. Pour la Commission, dans certains cas, un cumul de formalités pourrait être redouté car il est possible, par exemple, que des projets de recherches en matière de santé

[405] CNIL. Renseignements pratiques sur la procédure de déclaration de traitements de données à caractère personnel de santé à des fins d'évaluation ou d'analyse des pratiques de soins et de prévention, chapitre X, édition de juillet 2006. p. 6. www.cnil.fr. Op cit p. 6

[406] Décision n° 94 - 352 DC du 18 janvier 1995, JORF du 21 janvier 1995. p.1154.

[407] Loi 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. JORF n° 0020 du 24 janvier 1995. p. 1249. NOR: INTX9400063L.

[408] MOLE, Ariane, BENSOUSSAN, Alain. *La loi informatique et liberté modifiée : les nouveaux pouvoirs de la CNIL sur l'évaluation des pratiques de santé.* Gazette du palais du 19 octobre 1999, II, Doctrine p 1463.

[409] Délibération n° 99-005 du 18 février 1999, *20ème rapport d'activités de la cnil*, p. 241.

incluent une évaluation des pratiques de santé. Dans de telles situations l'on serait amené à s'interroger sur la procédure applicable : celle de la recherche en matière de santé ou celle de l'évaluation des pratiques de santé ?

Ce souci est donc désormais écarté mais la procédure relative à l'évaluation ou d'analyse des pratiques ou activités de soins et de prévention reste profondément marquée par l'importance accordée à l'anonymisation des données nominatives.

2. L'anonymisation des données

L'anonymisation est le procédé par lequel l'on supprime tout lien qui permettrait l'identification d'une personne dans un ensemble de données recueillies auprès d'un individu ou d'un groupe d'individus. Quoi que le nom serve de racine au mot, ce radical n'est pas le seul élément susceptible de permettre l'identification. La problématique de l'anonymat concerne aussi bien les données directement nominatives (nom, prénom, date de naissance, etc.) que celles qui le sont indirectement comme un matricule, une adresse, un numéro de téléphone, un élément biométrique, une adresse IP internet, les traces des données de connexion, etc. L'identification dépend non seulement de la donnée, mais également de son contexte d'utilisation et des destinataires. Par recoupement, plusieurs informations peuvent donc permettre l'identification des personnes. Ainsi, le croisement de la commune du lieu d'habitation avec une date de consultation ou d'hospitalisation et éventuellement, un troisième critère peuvent, dans certains contextes, désigner pratiquement, nommément un individu. C'est ce qu'un processus d'anonymisation efficace permet d'éviter.

En matière de traitement de données médicales, d'une part, selon l'article 63 de la loi informatique et libertés, les données de santé transmises par les professionnels de santé, les caisses de sécurité sociale ou les hôpitaux ne doivent être exploités à des fins d'évaluation des activités ou des pratiques de soins et de prévention que si elles le sont sous la forme de statistiques agrégées ou de données par patient constituées de manière à rendre l'identification des personnes concernées impossible. D'autre part, conformément à l'article 66, alinéa 2 de la loi informatique et libertés, les résultats des traitements ne peuvent pas faire l'objet d'une communication, d'une publication ou d'une diffusion si l'identification des personnes sur l'état desquels ces données ont été recueillies est possible.

Ces mesures ont été prises pour limiter les risques d'atteintes portées au nombre

important de personnes concernées par ces traitements qui peuvent également durer dans le temps. Néanmoins, tout en respectant les conditions fixées par les articles 64 à 66[410], la CNIL peut autoriser d'autres communications à condition que les données ne soient qu'indirectement à caractère personnel[411] c'est-à-dire qu'elles ne comportent ni le nom, ni le prénom d'une personne, ni le numéro d'inscription au répertoire national d'identification des personnes physiques.

Pour rappel, la demande d'autorisation d'anonymisation des données à des fins d'évaluation des pratiques de santé et de prévention est une procédure exorbitante de celle de droit commun prescrite par l'article 25 de la loi informatique et libertés. Mais peu importe le domaine de la santé concernée, la CNIL estime que ce procédé reste l'une des meilleures garanties de confidentialité et veille particulièrement à ce qu'il soit effectué dans les règles quand cela s'impose. Ainsi, le 26 octobre 2006, le Président de la CNIL, M. Alex TÜRK a chargé un groupe de travail de la mission d'évaluer la possibilité d'utiliser le NIR[412] et plus généralement de nouveaux identifiants nationaux dans le domaine de la santé publique. A la suite de cette réflexion, la CNIL a décidé que *« la méthode la plus à même d'apporter les garanties souhaitables est la création d'un identifiant de santé spécifique, généré à partir du NIR certifié selon les procédures déjà éprouvées, actuellement utilisée pour les bénéficiaires de l'assurance maladie, mais transcodé selon des techniques reconnues d'anonymisation. Ce numéro, non signifiant, constituerait un identifiant de santé utilisable dans l'ensemble du système de soins[413]* ».

La CNIL a pris une délibération[414] en date du 1er Octobre 2009 pour donner un avis sur le projet de décret portant sur la création d'un traitement de données relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1). Dans cet avis la CNIL a clairement exigé de

[410] La mise en œuvre du pouvoir de contrôle de la CNIL.

[411] Rappelons qu'au sens de l'article 2, alinéa 2 de la loi informatique et libertés, une donnée à caractère personnel correspond à 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.

[412] Numéro d'inscription au répertoire national d'identification des personnes physiques, communément appelé numéro de sécurité sociale.

[413] CNIL. *Conclusions de la Commission nationale informatique et liberté sur l'utilisation du NIR comme identifiant de santé.* 20 février 2007 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/ NIR/Rapport% 20NIR.pdf. Consulté le 28 mai 2014

[414] Délibération n° 2009-569 du 1er octobre 2009 portant avis sur un projet de décret en Conseil d'État relatif à la création d'un traitement de données relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1) JORF n°0246 du 23 octobre 2009. Texte n° 72 NOR: CNIX0924897X.

voir les mesures adéquates[415] prises pour l'anonymisation des données avant de rendre un avis complètement favorable à la prise du décret[416] dont la finalité lui semblait déjà légitime.

Jusqu'en 2009, la Commission avait été amenée à examiner des procédés qui visent à rendre anonymes de données personnelles uniquement dans le domaine de la santé publique. La première décision de la CNIL a été d'autoriser une fédération des mutuelles à accéder, pour le compte de ses mutuelles adhérentes qui le demandent, aux données de santé figurant sur les feuilles de soins électroniques[417]. Le 10 décembre 2009, elle a permis à la Mutualité française, les sociétés Axa-France et Groupama de prolonger les expérimentations ayant pour finalité de recourir et d'exploiter, sous forme anonymisée, les données de santé figurant sur les feuilles de soins électroniques[418]. Mais, une délibération[419] du 9 décembre 2010 a également prise dans un cadre différent pour émettre des recommandations en matière de réutilisation des archives publiques contenant des données personnelles. La Commission fait les précisions quant au cas dans lesquels la réutilisation à des fins commerciales de données personnelles contenues dans des documents d'archives est à exclure. Elle insiste particulièrement sur l'anonymisation préalable[420] des données publiques comportant des données sensibles telles

---

[415] *« La Commission estime que la mise à disposition de ces données à des fins d'études statistiques et épidémiologiques est parfaitement légitime. Elle demande toutefois à avoir connaissance des modalités de cette mise à disposition et en particulier des procédures mises en œuvre pour assurer l'anonymisation des données d'identification. En conséquence la Commission demande à être rendue destinataire d'un document technique complémentaire apportant des précisions sur (...) les techniques d'anonymisation…*[415]*. »* http://www.legifrance.gouv.fr/

[416] Il s'agira du décret n° 2009-1273 du 22 octobre 2009, *autorisant la création d'un traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1)*. JORF du 23 octobre 2009. p. 17726 texte n° 19. NOR: SASS0922224D.

[417] Voir NERBONNE S. La loi du 6 Août 2004. *Les régimes d'autorisation pour le secteur privé,* Communication commerce électronique, février 2005 paragraphe II. A. 4.
Voir également, une délibération n° 2004 - 081 du 9 novembre 2004 autorisant une expérimentation présentée par la fédération nationale de la mutualité française ayant pour finalité d'accéder sous forme anonymisée aux données de santé, sur les feuilles de soins électroniques. http://www.legifrance.gouv.fr/affichCnil.do ?oldAction=rechExpCnil&id=CNILTEXT000017653182&fastReqId=973778017&fastPos=1

[418] 30ème rapport annuel d'activités de la CNIL p. 71. http://www.cnil.fr. Consulté le 16 Août 2010.

[419] CNIL. Délibération n° 2010 460 du 9 décembre 2010 portant recommandation relative aux conditions de réutilisation des données à caractère personnel contenues dans des documents d'archives publiques. JORF n° 026 du 1er février 2011. Texte n° 72. NOR: CNIA1000016X.

[420] Le séminaire organisé par la CNIL en juillet 2013 sur la problématique de l'open data a été l'occasion pour les intervenants de relever, à nouveau leurs craintes quant à aux incertitudes qui entourent l'anonymisation des données personnelles contenues dans les données publiques communicables conformément à la loi CADA. Plusieurs questions ont notamment été soulevées dont celles de M. Serge DAËL, Président de la CADA: «*Aux termes de l'article 13 de la loi CADA, les informations publiques comportant des données personnelles peuvent être réutilisées, soit si la personne concernée y a consenti, soit si elles ont été rendues anonymes ou, à défaut, si une disposition législative ou réglementaire le permet. La question de l'anonymisation des données mêle des enjeux économiques et de libertés publiques. Plusieurs questions se posent :*

que citées par l'article 8 de la loi informatique et libertés avant toute communication permise par la loi CADA[421].

Ces traitements doivent s'effectuer dans le strict respect de la loi sous peine de sanctions pénales. L'article 66, alinéa 1 de la loi informatique et libertés dispose : *« les personnes chargées de la mise en œuvre d'un traitement ainsi que celles qui ont accès aux données faisant l'objet de ces traitements ou aux résultats de ceux-ci lorsqu'ils permettent indirectement d'identifier les personnes concernées, sont astreintes au secret professionnel sous les peines prévues à l'article 226-13 du code pénal. »*

Même si certains travaux[422] montraient déjà en 2000 que le procédé d'anonymisation n'est pas suffisamment fiable pour servir de garantie légale de confidentialité des données médicales, le principe reste louable car il dénote de la volonté[423] du législateur de veiller à

- *Jusqu'à quand faut-il parler d'identification indirecte ?*

- *Qui doit anonymiser les données ? A la lecture des dispositions de la loi « Cada », l'opération ne devrait pas être assurée par le réutilisateur, mais par l'administration détentrice des données ou ses sous-traitants.*

- *Qui doit assumer la charge financière des opérations d'anonymisation ?*

- *Comment procéder à l'anonymisation ? Cette question est délicate car il ne s'agit pas seulement de rayer les nom et prénom.*

- *Quelle est l'efficacité réelle des mesures d'anonymisation adoptées ? À cet égard, seule l'anonymisation manuelle, « artisanale », au cas par cas, semble aujourd'hui opérationnelle, faute d'outils techniques performants.*

- *Qui est habilité à procéder au recueil préalable du consentement de la personne concernée en cas de réutilisation de données non anonymisées ?*

Il ne faut pas se faire d'illusion : l'anonymisation des données ne résoudra pas la totalité des problèmes d'identification : les données ainsi expurgées peuvent souvent redevenir indirectement identifiantes, pour peu qu'on les rapproche d'autres sources d'informations. CNIL. *Séminaire « open data, quels enjeux pour la protection des données personnelles ? »* [en ligne], Compte rendu, 9 juillet 2013. p. 4 Disponible sur: http://www.cnil.fr/fileadmin/documents/approfondir/dossier/OpenData/CR_Workshop_Open_Data_9_juillet_2013.pdf. Consulté le 13 juin 2014.

[421] 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.

[422] DELIS. *Selon quelles modalités peut-on assurer la confidentialité du nouveau dossier médical informatisé ? Garantissez la confidentialité de vos données médicales informatisées.* Development Institut International Paris, les 20-21janvier 2000. http://www.delis.sgdg.org/menu/sante/diidospat.htm. Consulté le 5 avril 2014.

[423] L'article 5 de l'arrêté du 19 juillet 2013 précise les mesures d'anonymisation à prendre pour les traitements de données de santé dans le cadre du SNIIRAM. «*Afin de garantir l'anonymat des personnes ayant bénéficié des prestations de soins, les données transmises ne comportent pas l'identité de ces personnes. Un numéro d'anonymat est établi par codage informatique irréversible à partir du numéro d'inscription au répertoire national d'identification des personnes physiques. Ce procédé d'anonymisation s'opère à un double niveau, une première fois avant transmission des informations par les régimes à la base nationale et, une deuxième fois, préalablement à leur enregistrement dans la base de données nationale. Ce même procédé est appliqué aux numéros d'identification des titulaires de pensions d'invalidité et de rentes d'accidents du travail ou de maladies professionnelles ainsi qu'aux numéros d'entrée des patients. Toutes les données sensibles sont chiffrées lors de leur sauvegarde*». Arrêté du 19 juillet 2013 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie. JORF n° 0187 du 13 août 2013. p. 13791, texte n° 3. Disponible sur: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027830713. Consulter le 13 juin 2014.

leur protection. Beaucoup de raisons permettent de croire que l'effort technologique suivra par la suite car plusieurs procédés[424] existent de nos jours et connaissent une évolution constante encourageant le partage des données médicales.

[424] Pour plus de détail sur les procédés d'anonymisation, lire EL KALAM, Anas Abou, DESWARTE, Y, TROUESSIN, G CORDONNIER, E. *Gestion des données médicales anonymisées : problèmes et solutions in 2ème Conférence Francophone en Gestion et Ingénierie des Systèmes Hospitaliers (GISEH'04), Mons, 9-11 septembre 2004.* http://irt.enseeiht.fr/anas/recherche.htm. Voir également CNIL, *l'état des lieux en matière de procédés d'anonymisation*, 3 mai 2010. http://www.cnil.fr/en-savoir-plus/fiches-pratiques/fiche/article/lÉtat-des-lieux-en-matiere-de-procedes-danonymisation/?tx_ttnews%5BbackPid%5D=91&cHash=0713d5cbdd. Consulté le 5 avril 2014

Deuxième partie : LE CADRE JURIDIQUE DU PARTAGE DES DONNEES MEDICALES

La gestion électronique des données de santé induit inéluctablement leur partage car plusieurs professionnels peuvent intervenir dans le processus de traitement. Ce partage s'est accru ces dernières années en France du fait de l'équipement massif[425] des professionnels en systèmes informatiques. Les professionnels font également, de plus en plus, appel à d'autres avis de confrères ou se prononcent plus souvent, seulement après des examens complémentaires. Or, toutes ces démarches impliquent plus de besoins de partage et plus de mesures de sécurité. Il est indispensable de renforcer davantage la protection des données à travers des dispositions tant techniques que juridiques.

La mise en œuvre de ce partage électronique des données de santé (chapitre 1) peut se faire de différentes manières mais celle qui, en France a le plus marqué les esprits, depuis près d'une décennie, du fait de son rôle d'outil capital dans la coordination des soins est le dossier médical personnel (Chapitre 2).

[425] Selon une étude de la CNAMTS de février 2006, en 2006, 66% des médecins généralistes utilisaient un logiciel de gestion des dossiers médicaux tandis qu'ils n'étaient que 25% à le faire en 2003 selon un rapport remis au ministre de la santé en janvier 2003 : Cour des comptes. *Le partage des données entre les systèmes d'information de santé.* p. 309. http://www.ccomptes.fr/. Consulté le 5 avril 2014.

CHAPITRE I : LA MISE EN ŒUVRE DU PARTAGE DES DONNEES MEDICALES

Il existe différentes formes de partage mais leur mise en œuvre n'est possible qu'à la condition que les systèmes d'information soient interopérables. Les données médicales peuvent principalement se partager de deux manières : en interne, entre les systèmes d'information du même établissement de santé ou avec l'extérieur, entre les systèmes d'information de plusieurs établissements du même État ou avec ceux d'un État tiers. Cette dynamique d'échange s'opère à travers des activités de télésanté.

Nous étudierons dans un premier temps, l'interopérabilité des systèmes d'information de santé (Section 1) avant d'analyser le cadre juridique de la télésanté (Section 2).

Section 1 : L'interopérabilité des systèmes d'information de santé

Quelle que soit la forme de partage utilisée, il importe de mettre en place les dispositions nécessaires à la facilitation des échanges. Le transfert doit, notamment, se faire sans interruption, entre tous les systèmes. Cette fluidité, d'ordre technique, de la communication entre les différents systèmes d'information est « l'interopérabilité ». C'est la première condition (paragraphe 1) et la plus importante à remplir, en dehors de la sécurité, pour permettre un quelconque échange. En l'état actuel de la technologie et de la législation, elle connaît des limites (paragraphe 2) que les autorités compétentes s'attèlent à corriger.

Paragraphe 1 : L'interopérabilité des systèmes d'information : une condition sine qua non

L'interopérabilité, est une notion informatique difficile à traduire dans le langage courant. En quoi consiste-telle ? Quelles sont les conditions requises pour la rendre effective ?

A. Définition de l'interopérabilité

La directive européenne 91/250/CEE[426] a utilisé une définition de l'interopérabilité dans ses « considérant » qui insiste sur le cadre technique et le l'importance de cette capacité dans le fonctionnement du système informatique: *« considérant qu'un programme d'ordinateur est appelé à communiquer et à opérer avec d'autres éléments d'un système informatique et avec des utilisateurs; que, à cet effet, un lien logique et, le cas échéant, physique d'interconnexion et d'interaction est nécessaire dans le but de permettre le plein fonctionnement de tous les éléments du logiciel et du matériel avec d'autres logiciels et matériels ainsi qu'avec les utilisateurs; considérant que les parties du programme qui assurent cette interconnexion et cette interaction entre les éléments des logiciels et des matériels sont communément appelées « interfaces »; considérant que cette interconnexion et interaction fonctionnelle sont communément appelées « interopérabilité »; que cette interopérabilité peut être définie comme étant la capacité d'échanger des informations et d'utiliser mutuellement les informations échangées*[427]*; »*

En France, l'interopérabilité n'a pas de définition légale connue à ce jour. La loi portant création d'une couverture maladie universelle de 1999[428] y fait référence sans, toutefois, la définir. Ce texte présente le groupement pour la modernisation du système d'information hospitalier et, notamment, sa mission qui consiste à *« 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*[429]*. »*

---

[426]Directive 91/250/CEE du Conseil des communautés européennes, du 14 mai 1991, concernant la protection juridique des programmes d'ordinateur**.** JOCE n° L 122 du 17/05/1991 p. 0042 – 0046. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:FR:HTML Consulté le 7 février 2011

[427]Du 10éme au 12éme considérant de la directive européenne 91/250/CEE du 14 mai 1991. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:FR:HTML Consulté le 7 février 2011

[428] Article 43 de la loi insérant l'article L. 710-8 du code de la santé publique. Loi n° 99 - 641 du 27 juillet 1999 portant création d'une couverture maladie universelle (1). JORF n° 172 du 28 juillet 1999. p. 11 229. NOR : MESX9900011L. Consulté le 7 février 2011

[429] Article L. 710 - 8, alinéa 2 du code de la santé publique, insérée par la loi portant création d'une couverture maladie universelle. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000198392. Consulté le 7 février 2011

En mars 2006, une définition a été donnée par des députés (Le DEAUT, BLOCHE, LAMBERT) dans un amendement[430] à l'occasion des débats sur la loi DADVSI (Droits d'auteurs et droits voisins dans la société de l'information). Mais l'amendement ayant été rejeté par l'Assemblée nationale, cette définition n'a pas pu avoir d'existence légale. L'amendement suggérait : « *On entend par interopérabilité la capacité à rendre compatibles deux systèmes quelconques.*»

L'association francophone pour l'utilisation des logiciels libres (AFUL[431]), après plusieurs discussions, a finalement retenu, en 2009 la définition suivante : « *l'interopérabilité est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre*[432] *». L'AFUL, tout en faisant remarquer que l'absence de définition stricte a des répercussions négatives sur l'ensemble du système informatique*, milite en faveur de l'adoption d'une définition légale de la notion d' « interopérabilité » et de la reconnaissance d'un droit à l'interopérabilité par le droit européen[433].

Face à cette multitude de définitions, la question peut se poser de savoir laquelle retenir ?

Il faut constater que malgré les différences de sources, toutes se rejoignent à des détails près et en fonction des contextes et mettent simplement en avant la possibilité d'interaction entre différents éléments. Nous retiendrons arbitrairement celle donnée par le

[430]Assemblée nationale, Article 13 visant à modifier l'article 4 de la loi du 2004-575 pour la confiance dans l'économie numérique en y insérant les définitions de « compatibilité et interopérabilité ». *Amendement n° 341*. 7 mars 2006. n° 1206. http : //www.assemblee-nationale.fr/12/amendements/1206/120600341.asp. Consulté le 7 février 2011

[431] Depuis 1998, l'AFUL a pour but de promouvoir le logiciel libre, en particulier les systèmes d'exploitation (comme GNU-Linux ou les systèmes BSD libres), et aide à la diffusion de standards ouverts. L'AFUL est une organisation à but non lucratif (association loi 1901) qui réunit des utilisateurs, des professionnels, des entreprises et d'autres associations situées dans plus de dix pays et régions francophones (France, Belgique, Suisse, Luxembourg, Québec, pays d'Afrique francophone, etc.). http://aful.org/association/. Consulté le 7 février 2011

[432] Groupe de travail sur l'interopérabilité. http://aful.org/gdt/interop. Dernière modification le 5 juin 2009.

[433]Groupe de travail interop. *Interopérabilité*. Bordeaux 13 février 2010 http://aful.org/ressources/presentation/perspectives-interoperabilite/preview_html?file=file&file_html=file_html&file_html_subfiles=file_html_subfiles. Consulté le 07 février 2011.

rapport de la Cour des Comptes[434] relatif à la sécurité sociale déposée le 29 janvier 2008 du fait de sa simplicité et de sa proximité avec celle donnée l'ASIP santé, qui est en charge de cette interopérabilité dans le domaine de la santé. En effet, selon ce rapport, « *l'interopérabilité est la capacité, pour un système informatique, d'utiliser les informations produites par un autre système informatique comme celles produites par lui-même et de mettre à disposition des autres systèmes les informations qu'il a produites* ». Et, concernant le domaine de la santé, la définition donnée par l'ASIP santé est : « *l'interopérabilité entre systèmes d'information dans les domaines santé et médico-social peut se définir comme : la capacité qu'ont plusieurs systèmes d'échanger de l'information entre eux et d'utiliser l'information qui a été échangée, pour que les utilisateurs de ces systèmes puissent en tirer parti dans leurs actes et leurs décisions, pour le mieux-être de leurs patients.*[435]»

L'interopérabilité est une question d'ordre technique dont les contours juridiques ne sont pas négligeables ; c'est pourquoi le gouvernement français a mis en place un mécanisme spécial coordonné par l'ASIP[436] santé. L'une des missions[437] les plus importantes de l'ASIP santé est de favoriser le développement de l'interopérabilité entre les systèmes d'information de santé. Le « *Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS) est le référentiel central qui sous-tend cette mission en créant 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. Ce référentiel spécifie les standards (le plus souvent internationaux) à utiliser dans les échanges et lors du partage de données de*

[434] Rapport d'information enregistré à la présidence de l'Assemblée nationale le 29 janvier 2008, déposé en application de l'article 145 du règlement par la Commission des affaires culturelles, familiales et sociales sur le dossier médical personnel et présenté par M. Jean-Pierre DOOR, député. http://www.assemblee-nationale.fr/13/rap-info/i0659.asp#p34_266743 Consulté le 27 juin 2010.

[435]Asip santé. *Cadre d'interopérabilité des systèmes d'information de santé (CI-SIS)*. http://esante.gouv.fr/ contenu/cadre-d-interoperabilite-des-systemes-d-information-de-sante-ci-sis publié le 6 décembre 2010.

[436] Agence des systèmes d'information partagés de santé, groupement d'intérêt public (GIP) constitué le 8 septembre 2009 pour prendre fin au 16 juillet 2024. Sa convention constitutive a été approuvée par arrêté le 28 novembre 2009. JORF n° 0277 du 29 novembre 2009. p. 20626, texte n° 16. NOR : SASG0925044A.

[437] Pour remplir sa mission de développement des systèmes d'information partagés dans le domaine de la santé et du secteur médico-social, l'agence s'est vue attribuer par l'arrêté du 18 septembre 2013 l'ensemble des missions auparavant dévolues aux groupements d'intérêt public « dossier médical personnel » et au groupement d'intérêt public « carte de professionnel de santé ». Arrêté du 18 septembre 2013 *portant approbation de la convention constitutive du groupement d'intérêt public « agence nationale des systèmes d'information partagée de santé* ». JORF n° 0243 du 18 octobre 2013 p.17153 texte n°20.

santé entre SIS[438]*, et contraint la mise en œuvre de ces standards par des spécifications d'implémentation destinées à faciliter le déploiement de l'interopérabilité entre SIS dans les conditions de sécurité requises* [439]*».*

L'Asip santé définit, assure la maintenance et publie les référentiels nationaux sur lesquels s'appuient les systèmes d'information de santé (SIS). Ce référentiel recouvre les domaines de l'identification, de l'interopérabilité et de la sécurité. Le répertoire national des référentiels (RNR) l'espace de publication des référentiels de nomenclatures[440] et des spécifications de référence telles que le cadre de l'interopérabilité des systèmes d'information de santé (CI-SIS), l'identifiant national de santé (INS), la politique générale de sécurité des systèmes d'information de santé (PGSSI-S). Outre les nomenclatures et les spécifications de référence, le terme "référentiel" est utilisé également pour nommer les infrastructures informatiques hébergeant des données de référence. Le RPPS[441] en est un exemple. Ces infrastructures ne font pas partie du périmètre du RNR[442].

La version majeure actuelle du référentiel CI-SIS est la version 1.3 publiée le 18 octobre 2012, après approbation le 9 octobre par les organisations représentatives des industriels de l'informatique de santé. Au sein de cette version majeure la version mineure courante et la version 1.3.1 qui concerne un nombre réduit de composants prix publiés le 14

[438] Système d'information de santé.

[439] ASIP SANTE. Cadre d'interopérabilité des systèmes d'information de santé. 8 décembre 2013. http://esante.gouv.fr/contenu/cadre-d-interoperabilite-des-systemes-d-information-de-sante-ci-sis. Consulté le 21 avril 2014.

[440] Il s'agit de la nomenclature des acteurs de santé (NAS) comprenant les nomenclatures du référentiel des acteurs santé sociaux (RASS) incluant le répertoire partagé des professionnels de santé (RPPS), celle du SI-CPS et à l'avenir celles du répertoire opérationnel des ressources (ROR) ; les nomenclatures métier du cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) qui comprennent : les nomenclatures créées par l'Asip santé pour les besoins des volets de contenus et des jeux de valeurs correspondants ; et les nomenclatures gérées par l'Asip santé incluant la SNOMED 3.5, le code identifiant des spécialité (CIS) et le code identifiant de présentation (CIP). ASIP SANTE. *Présentation du répertoire national des référentiels (RNR).* 10 décembre 2013. http://esante.gouv.fr/services/referentiels/presentation-du-repertoire-national-des-referentiels-rnr/presenta tion-du-reper. Consulté le 21 avril 2014

[441] Répertoire partagé des professionnels de santé.

[442] ASIP SANTE. *Présentation du répertoire national des référentiels (RNR).* 10 décembre 2013. http://esante.gouv.fr/services/referentiels/presentation-du-repertoire-national-des-referentiels-rnr/presentation-du-reper. Consulté le 21 avril 2014.

novembre 2012. Le détail de cette version mineure 1.3.1 est précisé dans la note de version du référentiel[443].

B. Les conditions de l'interopérabilité

« L'interopérabilité revêt différentes dimensions :

- une interopérabilité de contenu qui définit le contenu échangé, en termes syntaxiques (structure et format de fichier, encodage) et sémantiques (vocabulaire utilisé, nomenclatures, terminologies) de manière à permettre la compréhension et l'utilisation des informations par le système destinataire ;

- une interopérabilité des services qui établit le contexte et les règles de l'échange ;

- une interopérabilité des transports et communication qui permet l'interconnexion technique des systèmes et l'acheminement de l'information de l'un à l'autre »[444].

Pour atteindre ces trois dimensions dans le cas des données de santé, il faut remplir plusieurs conditions. Il s'agit, notamment, de l'identification des patients et des professionnels de santé, d'une part, et de la normalisation et la sécurisation des échanges, d'autre part.

1. L'identification des patients et des professionnels de santé

Pour assurer la fiabilité de l'échange, il importe d'identifier d'une part, le patient et d'autre part, le professionnel intervenant.

---

[443] ASIP SANTE. *Cadre d'interopérabilité des SIS. Evolutions du CI-SIS depuis la version 1.0.1. Note de version.* 14 novembre 2012. http://esante.gouv.fr/sites/default/files/CI-SIS_NOTE-DE-VERSION_V1.3.1.pdf. Consulté le 21 avril 2014.

[444] *ASIP santé.* Cadre d'Interopérabilité des SIS – Document Chapeau. 16 Novembre 2010. P.5/16. http://esante.gouv.fr/sites/default/files/CI-SIS_Document_Chapeau_v1.0.1.pdf ou GIP DMP: Cadre d'interopérabilité des systèmes d'information de santé. Publié le 29 juin 2009. http://www.i-med.fr/spip.php?article347. Consulté le 2 novembre 2011

a. L'identification des patients

Il faut que le patient soit identifié sans ambiguïté lorsque des professionnels de santé se partagent ou s'échangent des informations le concernant. Le nom, le prénom, la date et le lieu de naissance du patient ne sont pas suffisants car une erreur sur une de ces données d'identification peut donner lieu à la création de deux dossiers différents pour un même patient et, en cas d'homonymie, on peut courir le risque de confondre les dossiers de différents patients. C'est pourquoi une identification avec un niveau de fiabilité satisfaisant répond à trois solutions possibles selon un rapport[445] de la Cour des Comptes :

« - soit l'on crée, au niveau national, un système d'identification ex nihilo en attribuant, après avoir vérifié son identité, un identifiant à chaque patient, c'est-à-dire à chaque personne prise en charge par le système de soins en France et donc potentiellement à tous les résidents. La constitution d'un tel système d'identification à un coût, estimé par le ministère de la santé à 500 000 €, sans compter le coût annuel pour sa mise à jour ; »

« - soit on utilise le répertoire national identification des personnes physiques (RNIPP), géré par l'INSEE et, pour les personnes nées à l'étranger, à Mayotte, en Polynésie française, en Nouvelle-Calédonie et dans les îles Wallis et Futuna par la CNAVTS[446]. L'utilisation de l'identifiant du RNIPP, appelé NIR (numéro d'inscription au répertoire) et la communication de données issues du RNIPP, notamment pour vérifier l'exactitude des NIR, requiert soit une autorisation de la CNIL, soit des dispositions législatives ou réglementaires prises après avis de la CNIL ; »

« - soit l'on fabrique, à partir du NIR, un identifiant spécifique au domaine de la santé qui ne serait pas signifiant[447]. Cette façon de procéder dispense de créer un organisme chargé de l'identification des patients, requis pour la mise en œuvre de la première solution. Il nécessite cependant de gérer, de façon sécurisée, si possible en un lieu unique, une table permettant, à partir du NIR, d'obtenir l'identifiant santé des patients. »

[445] Cour des Comptes. *Le partage des données entre les systèmes d'information de santé in La sécurité sociale*. Septembre 2007. Chapitre X. p.310 et 311. http://www.ccomptes.fr/fr/CC/documents/RELFSS/07-securite-sociale.pdf. Consulté le 17 janvier 2011.

[446] Caisse nationale d'assurance vieillesse pour les travailleurs salariés.

[447] Le NIR est signifiant quand il permet de connaître le sexe de la personne, sa date de naissances au mois près, sa commune de naissance. Il ne protège donc pas l'anonymat.

Le 30 janvier 2007, une loi[448] prescrit qu' *« un identifiant de santé des personnes prises 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 (...)».* Mais ce texte laisse les modalités de son exécution à la charge d'un décret pris après avis de la CNIL.

La mise en application s'est heurtée alors, à des investigations tendant à la recherche du meilleur système d'identification. Pendant que le ministère de la santé optait pour l'utilisation du NIR, la CNIL préconisait la création d'un identifiant spécial (différent du NIR) pour la santé[449]. Ce n'est qu'en 2010[450] qu'un identifiant national de santé (INS[451]) a été concrètement mis sur pied par l'ASIP. En tant que maître d'ouvrage du programme d'élaboration de l'identifiant national de santé qui conduira au partage de données dont elle a la charge depuis janvier 2009, l'ASIP se doit de veiller à la mise en place d'un système d'information pérenne et sécurisée pour tous les systèmes de santé. Dans ce cadre, l'agence a signé une convention de service avec le Centre national de dépôt et d'agrément (CNDA) de la CNAM-TS chargé d'assurer l'accompagnement des éditeurs en vue de l'intégration de l'algorithme de génération des INS-C[452] dans le logiciel. L'ASIP a permis aux éditeurs de logiciels intégrant le calcul de l'INS-C de pouvoir se faire référencer pour faciliter l'information des établissements et professionnels de santé. Désormais, sur le site :

---

[448] Article 25 de la 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 (1) (Titre résultant de la décision du Conseil constitutionnel n° 2007-546 DC du 25 janvier 2007). JO n° 27 du 1er février 2007. P. 1937- 1941. NOR: SANX0500266L. Cet article insère l'article L. 1111-8-1 au Code de la santé publique.

[449]CNIL. *Conclusions de la Commission de l'informatique et des libertés sur l'utilisation du NIR comme identifiant de santé*. 20 février 2007. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/NIR/Rapport%20NIR.pdf . Consulté le 19 janvier 2011.

[450] ASIP santé communiqué de presse : *Une première étape pour un identifiant national adapté à l'échange et au partage de données de santé*. Paris, le 9 juin 2010. Http://esante.gouv.fr/sites/default/files/CP_INS_Convention ASIP_CNDA_090610_0.pdf. Consulté le 17 janvier 2011

[451] L'identifiant national de santé est « *calculé localement dans les systèmes de santé en appliquant un algorithme public, choisi par l'ASIP santé avec le support de l'ANSSI, sur les traits d'identités (prénom, date de naissance, NIR) lus en Carte Vitale, éventuellement complétés par l'appel à un télé-service »* Http://esante.gouv.fr/sites/default/files/CP_INS_ConventionASIP_CNDA_090610_0.pdf. Consulté le 19 janvier 2011

[452] ASIP. *Les raisons d'être et le cadre réglementaire de l'INS-C*. Publié le 11 juillet 2010. http://esante.gouv.fr/referentiels/identification/les-raisons-d-etre-et-le-cadre-reglementaire-de-l-ins. Consulté le 19 janvier 2013.

www.cnda-vitale.fr, les établissements et professionnels de santé pourront retrouver la liste des logiciels intégrant le calcul de l'INS-C sur son site Internet[453] la liste de logiciels référencés pour le calcul de l'INS-C, élément indispensable pour l'échange et le partage de données de santé dans un contexte sécurisé et interopérable. L'on attend de l'identifiant national de santé qu'il soit unique (un seul identifiant pour chaque personne tout au long de sa vie), non signifiant (la connaissance de l'identifiant national de santé ne doit pas permettre de déduire des informations sur la personne), sans doublon ni collision. Ce n'est pas un identifiant public ni secret mais il est privé C'est une information personnelle du patient protégée par la loi informatique et libertés, au même titre que le nom et le prénom.

Selon l'entendement de la CNIL, cet identifiant doit présenter les « garanties souhaitables » car, *« certifié selon les procédures déjà éprouvées, reconnues et fiables, actuellement utilisées pour les bénéficiaires de l'assurance maladie, mais transcodé selon des techniques établies d'anonymisation*[454] *»*. La procédure prescrite pour sa création (c'est-à-dire par décret après avis de la CNIL aux termes de l'article L1111-8-1 du code de la santé publique[455]), apparaît comme le gage d'une garantie de sécurité supplémentaire en plus de l'appartenance de la CNIL au Comité de pilotage chargé de sa mise en place. Il est regrettable de constater que cette procédure puisse, également être à l'origine du ralentissement de la mise en œuvre de cet identifiant.

Dans son rapport annuel d'activité pour l'année 2009[456], la Commission rappelle que le décret[457] régissant le choix et les modalités d'utilisation de l'identifiant de santé est l'un des

---

[453] ASIP. INS compatibilité : *Liste des logiciels référencés pour le calcul de l'INS-C.* 13 octobre 2013. Http://esante.gouv.fr/services/referentiels/identification/ins-compatibilite-liste-des-logiciels-references-pour-le-calcul. Consulté le 23 octobre 2013.

[454] CNIL. *Quel identifiant pour le secteur de la santé ? La CNIL propose la création d'un numéro spécifique généré à partir du NIR mais anonymisé*. 20 février 2007. http://www.cnil.fr/la-cnil/actu-cnil/article/article/quel-identifiant-pour-le-secteur-de-la-sante-la-cnil-propose-la-creation-dun-numero-specifiqu/. Consulté le 17 février 2011.

[455] *« 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. »* Cette version est également celle de l'article 5 de la loi du 13 Août 2004 relative à l'assurance maladie, JORF du 17 Août 2004, telle que modifiée par la loi n°2007-127 du 30 janvier 2007.

[456] CNIL. *Rapport annuel d'activités 2009*, édition 2010. P. 87 http://www.cnil.fr/fileadmin/documents/ La_ CNIL/publications/CNIL-30erapport_2009.pdf. Consulté le 17 février 2011.

principaux textes qui doivent lui être soumis pour avis en 2010. Dans sa délibération du 2 décembre 2010, la CNIL présente la solution INS-C comme provisoire *« dans l'attente de la mise en place de l'INS aléatoire prévu à terme*[458] *»*. Mais jusqu'en juin 2014, cette étape n'a pas encore été franchie. Et cela risque de mettre du temps car dans le tableau établi par le rapport[459] annuel du Sénat sur l'application des lois 2010 il apparaît que la mise en œuvre de la loi dont le décret d'application est attendu n'est pas urgente[460]. En attendant, le dossier pharmaceutique possède son propre identifiant : « l'identifiant final et général » de santé. Un patient se voit aujourd'hui attribuer un identifiant de santé différent dans chaque système où il est pris en charge (LGC[461], SIH[462], SIL[463], réseau…). Chaque système d'information adopte son propre code d'attribution et de constitution d'identifiant de santé, limitant ainsi les possibilités d'échanges et de partage d'information entre les acteurs de santé dans les meilleures conditions de sécurité. Des initiatives locales de création d'identifiant de santé régionaux ont été lancées et mises en œuvre sur des concepts propres à chacun des projets, limitant également l'usage de l'identifiant au niveau de la région. Or, l'usage de plusieurs identifiants pour les patients est de nature à constituer « *un frein au développement des applications de partage et d'échanges des données de santé et contribue à augmenter le risque médical pour un patient à qui sont attribuées à tort des données mal identifiées*[464] *»* selon les professionnels en la matière.

---

[457] Décrets d'application de la loi n°2007-127 du 30 janvier 2007 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.

[458] CNIL. *Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel*. http://www.legifrance.gouv.fr/affichCnil.do?oldAction =rechExpCnil&id=CNILTEXT000023308516. Consulté le 17 février 2011.

[459] Senat (Rapporteur : Alain Milon). *Rapport annuel de contrôle d'application des lois 2010*. 11 janvier 2011. http://www.senat.fr/rap/apleg_10/apleg_1044.html. Consulté le 25 juin 2012.

[460] Senat (Rapporteur : Alain Milon). *Rapport annuel de contrôle d'application des lois 2010*. 11 janvier 2011. (Voir le tableau). http://www.senat.fr/rap/apleg_10/apleg_1044.html. Consulté le 25 juin 2012.

[461] Logiciel de gestion de cabinet

[462] Système d'information hospitalière

[463] Système d'information pour laboratoire

[464] ASIP santé. *Programme de relance du DMP et des systèmes d'information partagée de santé : Orientations stratégiques et principes de mise avril 2009*. P. 46. http://esante.gouv.fr/sites/default/files/Programme_de_ relance_DMP_et_SIS_Avril_2009.pdf . Consulté le 18 février 2011.

On ne peut qu'espérer que dans un avenir très proche, les autorités compétentes prennent conscience de ces risques et fassent passer l'application du décret identifiant dans le lot des dossiers urgents et le soumettent pour avis à la CNIL. D'autant plus que la question de l'identification des professionnels de santé n'est pas non plus sans difficultés.

b. L'identification des professionnels de santé

Identifier distinctement des professionnels de santé est nécessaire pour l'interopérabilité des systèmes d'information. Il indispensable de savoir qui est responsable de la qualité de l'information émise et qui en est destinataire pour s'assurer de l'habilitation de ce dernier à la recevoir. Ce rôle d'identification est assigné au système CPS[465] (Carte professionnel de santé) dans le cadre de la transmission de Système d'information pour laboratoire aux organismes d'assurance maladie.

En application du décret[466] 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, le système CPS était mis en œuvre par le groupement d'intérêt public CPS (GIP CPS). Mais le GIP CPS a été dissout par arrêté du 28 novembre 2009[467] portant approbation de la dissolution du GIP CPS, et ses missions sont,

[465] Pour plus d'informations sur la carte CPS, voir *la CPS, carte d'identité électronique pour les professionnels de santé.* Publié le 26 avril 2010. *« La carte CPS est une carte électronique individuelle protégée par un code confidentiel, aujourd'hui diffusée à plus de 650 000 exemplaires auprès des personnels de santé (professionnels de santé et personnels auxiliaires). Elle contient des informations portant sur l'identité du professionnel de santé, sa qualification, ses différentes situations d'exercice. Elle contient aussi des données de facturation pour l'établissement des feuilles de soins électroniques, dans le cadre de l'application SESAM Vitale (plus de 900 millions de FSE réalisées en 2006).* http://esante.gouv.fr/espace-cps/guide/la-cps-carte-d-identite-electronique-des-professionnels-de-sante. Consulté le 25 juin 2012.

[466] 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 n° 113 du 16 mai 2007. p. 9362. Texte 210 sur 413. NOR : *SANP0721653D*

[467] Arrêté du 28 novembre 2009 portant approbation de la dissolution du groupement d'intérêt public « Carte de professionnel de santé » et transfert des biens, droits et obligations à l'Agence des systèmes d'information partagés de santé. JORF n°0277 du 29 novembre 2009. P 20627 texte n° 17. NOR: SASG0925049A. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=569F0B88D35BB3D145A19BD9FDE6FB28.tpdjo16v_1?cidTexte=JORFTEXT000021344759&dateTexte=&oldAction=rechJO&categorieLien=id. Consulté le 25 juin 2012.

aujourd'hui, attribuées à l'ASIP santé. Ce groupement est le résultat de la fusion du GIP DMP[468] et du GIP CPS[469].

La carte CPS est un outil indispensable pour le professionnel de santé. Elle atteste de son identité et de ses qualifications professionnelles auprès des systèmes informatisés de santé. C'est une carte à microprocesseur du modèle des cartes bancaires qui comporte des certificats CPS, de véritables pièces d'identité professionnelles numérisées et certifiées par l'ASIP Santé. Les certificats, fichiers informatiques contenant des informations sur leurs propriétaires et équivalents d'une carte d'identité numérique sont utilisés par leur titulaire en guise de gages de confiance, dans les applications communicantes qui mettent en œuvre des données de santé confidentielles. Employés dans le monde numérique, ils garantissent l'identité d'une entité physique ou morale et permettent également d'échanger de manière sécurisée en mettant en œuvre des mécanismes de chiffrement (ou de cryptage). Ils ont pour rôle de permettre :

- l'identification du professionnel de santé porteur, sans ambiguïté. La reconnaissance sans équivoque de sa personne et de ses aptitudes se fait grâce aux informations professionnelles le concernant recueillies auprès des autorités compétentes (État, ordres, organismes d'assurance maladie) ;
- l'authentification du professionnel de santé, par la vérification de son identité sur la base d'éléments de preuve pour les transmissions sécurisées avec l'assurance-maladie et entre professionnels de santé tout comme, le cas échéant, pour l'accès aux dossiers des patients ;
- la signature électronique de documents ou d'actes, permettant ainsi au porteur de s'engager quant au contenu d'un document échangé et de garantir la non altération des données ;
- le chiffrement des données échangées afin de garantir leur confidentialité. L'échange des informations doit se faire de manière à empêcher les interceptions et leur compréhension par un tiers.

La CPS permet aux professionnels de santé de :

[468]Le gouvernement a approuvé la modification de la convention constitutive du Groupement d'intérêt public du Dossier Médical Personnel, qui emporte son changement de dénomination en « Agence nationale des systèmes d'information partagés de santé » par arrêté du 8 septembre 2009 publié au JORF n° 2013. P. 15096, texte n° 15 du 15 septembre 2009 http://esante.gouv.fr/asip-sante/qui-sommes-nous/une-agence-d-État. Consulté le 15 février 2010.

[469] ASIP santé. *Une agence d'État*. Publié le 08 mai 2010. « *La publication au Journal officiel le 29 novembre 2009 des arrêtés du 28 novembre 2009 a acté la dissolution du GIP Carte de professionnel de santé (CPS) et l'élargissement du périmètre des actions de l'ASIP Santé aux missions attachées à la CPS* ». http://esante.gouv.fr/asip-sante/qui-sommes-nous/une-agence-d-État. Consulté le 15 février 2010.

- s'identifier et d'éviter une usurpation de leur identité (via le processus d'authentification) ;
- apposer la signature électronique sur des documents ;
- transmettre les feuilles de soins électroniques aux organismes d'assurance-maladie obligatoires et complémentaires ;
- créer, alimenter et consulter le dossier médical personnel de leurs patients ;
- réaliser des actes médicaux à distance (télémédecine) ;
- utiliser la messagerie sécurisée des professionnels de santé ;

Grâce à la technologie sans contact, elle peut être utilisée pour d'autres applications comme l'accès à des locaux.

Il existe, désormais, une carte CPS 3[470]. Elle a été distribuée à l'ensemble des professionnels de santé à partir de février 2011. Pour l'accompagnement de la dématérialisation des données médicales la carte a été dotée de nouveaux usages qui vont au-delà du seul domaine de l'assurance maladie, notamment, l'accès au DMP, le développement des messageries sécurisées et la télémédecine. Cette nouvelle carte (déployée depuis 2004 sous la version CPS 2 ter) a été aménagée pour suivre les évolutions de la technologie. Elle est distribuée gratuitement et systématiquement à tout professionnel de santé libéral et hospitalier inscrit au tableau des quatre ordres professionnels que sont les pharmaciens, les sages-femmes, les chirurgiens-dentistes et les médecins. C'est une carte « 3 en 1» c'est à dire :

«- Standard : elle intègre le standard IAS ECC (identification-authentification-signature european-citizen-card), standard choisi pour la mise en place de l'administration électronique et de la future carte nationale d'identité électronique.

- Compatible : elle fonctionne comme la CPS actuelle, sans changement à apporter au logiciel ou au matériel existant. Elle est donc totalement compatible avec le poste de travail d'un professionnel de santé qui aurait déjà une CPS (pas d'impact sur les applications de feuille de soin électronique, ou sur l'accès au service de consultation des droits en ligne, à l'Espace Pro, par exemple).

[470]ASIP santé. *L'essentiel sur la CPS 3.* http://esante.gouv.fr/sites/default/files/Fiche_LEssentielsurla CPS3_020311.pdf et pour en savoir davantage sur l'environnement du CPS 3, lire *La CPS 3, une nouvelle étape pour la e-santé* http://esante.gouv.fr/sites/default/files/DP_CPS.pdf. Consulté le 21 mai 2014.

- *Enrichie : elle propose des fonctionnalités sans contact, qui faciliteront l'usage en situation de mobilité, et permet d'envisager de nouveaux usages, et une nouvelle ergonomie pour l'utilisation de la carte*[471]*. »*

L'article L. 161 - 33 alinéa 4 du code de la sécurité sociale dispose : *« dans les cas de transmission de données 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 fixées par décret en Conseil d'État après avis de la Commission nationale informatique et libertés*[472] ». Cet article précise les cas où la carte CPS doit être utilisée tout comme l'article L. 1110 - 4[473] du code de la santé publique. Les deux textes renvoient au décret « confidentialité » ayant pour rôle de déterminer les cas où l'utilisation de la carte est obligatoire. Il s'agit de la transmission électronique des actes ou prestations remboursables par l'assurance-maladie aux termes de la loi et de l'accès ou de la transmission électronique de données de santé par les professionnels de santé selon le décret « confidentialité ». Il semblerait donc que le décret admette un champ d'utilisation plus large (accès ou transmission) que la loi (transmission) ; ce qui pose un problème de conflit de normes. En principe, la loi étant au-dessus du décret, et ce dernier étant pris en application de la première, ce règlement ne peut que définir les modalités d'application de la norme supérieure et non en modifier le champ. Il arrive souvent qu'à la faveur d'innovations administratives, la législation existante soit déformée. Dans le cas d'espèce, Caroline ZORN-

[471] Asip santé. *Qu'est-ce que la carte CPS?*. 23 octobre 2013. http://esante.gouv.fr/services/espace-cps/qu-est-ce-que-la-carte-cps. Consulté le 23 octobre 2013.

[472]Article créé par l'ordonnance n° 96-345 du 24 avril 1996- article. 8 II, IV JORF n° 98 du 25 avril 1996. P. 6311. NOR: TASX9600042R relative à la maîtrise médicalisée des dépenses de soins. http://www.legifrance.gouv.fr/affichCode.do;jsessionid=BB2F9D891ED2F5EC8C8F9564730276C2.tpdjo04v_2?idSectionTA=LEGISCTA000006172510&cidTexte=LEGITEXT000006073189&dateTexte=vig. Consulté le 23 octobre 2013.

[473] Code de la santé publique. Article L. 1110-4, alinéa 4 : *« 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'État 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. »* http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006685746. Consulté le 23 octobre 2013.

MACREZ[474] estime que les professionnels n'utilisant pas la carte lors de la transmission d'informations médicales seraient fondés à invoquer l'exception d'illégalité pour demander au juge que l'acte ne leur soit pas applicable, ou plus radicalement, à attaquer l'éventuelle décision de déconventionnement en recours pour excès de pouvoir pour faire annuler l'acte[475].

L'article R. 2213-1-2[476] du code général des collectivités prévoit un autre cadre d'utilisation de la carte CPS : c'est lorsque le médecin ayant constaté un décès doit se faire identifier avant d'établir un certificat sur support électronique.

Cette identification peut permettre l'interopérabilité des systèmes d'information mais il est également indispensable que les échanges soient normalisés.

2. La normalisation et la sécurisation des échanges

La normalisation est une *« activité propre à établir, face à des problèmes réels ou potentiels, des dispositions destinées à un usage commun et répété, visant à l'obtention du degré optimal d'ordre dans un contexte donné*[477]*. »* La norme est déterminante dans le processus d'interopérabilité et M. PAQUEL d'affirmer qu' *« ... à l'heure de la communication, la normalisation est une contrainte certes, mais une nécessité absolue*[478] *».*

Dans le langage courant, une norme (du latin «*norma, equerre*») est une règle à suivre. Dans le domaine informatique, c'est un référentiel[479] commun et documenté destiné à

[474] Caroline ZORN-MACREZ est docteur en droit privé de l'université de Nancy et actuellement chercheur au CNRS.

[475] ZORN-MACREZ Caroline. *Données de santé et sécurité partagée : pour un droit de la personne à la protection de ces données de santé partagée*. Presses universitaires de Nancy. Collection « santé, qualité de vie et handicap ». Nancy, octobre 2010. 502 pages. P. 269. ISBN : 978 - 2 - 8143 - 00 25 - 5. Thèse en droit privé et sciences criminel remaniée, soutenue le 5 décembre 2009 à l'université de droit de Nancy.

[476] L'article R. 2213 -1-2 du code général des collectivités territoriales est issu du décret n° 2006 - 938 du 27 juillet 2006 relatif au certificat de décès : « le médecin ayant constaté le décès établit sur support électronique un certificat après s'être identifié au moyen d'une carte professionnelle de santé ou d'un dispositif d'authentification individuel offrant des garantie similaires et agréé par le groupement d'intérêt public mentionné à l'article R. 161 - 54 du code de la sécurité sociale. »

[477] AFNOR. *Lexique*. http://www.afnor.org/lexique/%28lettreid%29/n

[478] PAQUEL, Norbert. *Interopérabilité des systèmes, le syndrome de la tour de Babel*. TLM n° 31 avril 1998. Informatique de santé : enjeux, formation continue. http://www.tlmfmc.com/site/dossiers_detail.tpl?sku=305082874372600&sku2=305082906273448. Consulté le 22 mai 2014

[479] C'est une référence que l'on utilise pour décrire un mouvement.

harmoniser les activités du secteur[480]. La norme est réalisée par des organismes spécialisés, la plupart du temps, des organismes privés sans but lucratif [481] en relation avec les pouvoirs publics. En France, le statut réglementaire de la normalisation est régi par la loi n°41-1987 du 24 mai 1941 relative à la normalisation[482] qui prévoit son décret d'application. Aujourd'hui, le texte de référence est le décret[483] n° 2009-697 du 16 juin 2009, transposant la directive[484] 98/34/CE du 22 juin 1998 du Parlement européen et du Conseil.

Aux termes de l'article 1er de la directive, on entend par *« «norme» une spécification technique approuvée par un organisme reconnu à activité normative pour application répétée ou continue, dont l'observation n'est pas obligatoire et qui relève de l'une des catégories suivantes :*

- *norme internationale : norme qui est adoptée par une organisation internationale de normalisation et qui est mise à la disposition du public,*

[480] Il ne faut pas confondre norme et standard comme c'est le cas en anglais où le terme « standard » désigne norme et standard. Le dernier est une convention fondée sur un consensus plus restreint que pour la norme, généralement élaboré entre des industriels au sein de forums ou de consortiums. Alors que la norme est produite par un organisme officiel, le standard est un référentiel publié par une entité privée autre qu'un organisme de normalisation nationale ou internationale non approuvé par un de ces organismes pour un usage national ou international. Lorsqu'une méthode ou une technologie est adoptée par une majorité d'industriels et d'utilisateurs et qu'elle est considérée comme « standards », on parle de standard de fait (standard de facto). Le standard est dit ouvert lorsqu'il est librement diffusé. http://fr.wikipedia.org/wiki/Normes_et_standards_industriels et lexique AFNOR http://www.afnor.org/lexique. Consulté le 23 octobre 2013

[481] Les organismes de normalisation sont des organismes dont le rôle est de valider les normes que les industries utiliseront comme support pour rendre leurs services ou produits interopérables. Il s'agit, notamment, de :
- ISO : Organisation internationale de normalisation
- ANSI : American national standards Institute
- AFNOR : Association française de normalisation.
- CEN : Comité européen de normalisation
- ITU : Unité internationale des télécommunications
- CENELEC : Comité européen de normalisation électronique
- CNISAS : Commission de normalisation de l'informatique de santé et de l'action sociale.

Conformément au décret relatif à la normalisation du 16 juin 2009, AFNOR anime le système central de normalisation qui est composée de 25 bureaux de normalisation sectoriels des pouvoirs publics et de 20 000 experts. Au sein du CEN et de l'ISO, AFNOR représente la France et assume les responsabilités y afférents.
En Allemagne, l'organisme similaire à l'AFNOR est le DIN (Deutsches Institut für Normung), le BSI (British Standard Institute) au Royaume-Uni et l'ANSI (American National Standard Institute) aux États-Unis.

[482] JORF du 28 mai 1941 p. 2219

[483] Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation JORF n° 0138 du 17 juin 2009 p. 9860. Texte n° 6 NOR: ECEI0909907D.

[484] Directive 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. JOCE n° L 204 du 21/07/1998 p. 0037 – 0048. Disponible sur: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0034:FR: HTML. Consulté le 23 octobre 2013

- norme européenne : norme qui est adoptée par un organisme européen de normalisation et qui est mise à la disposition du public,

- norme nationale : norme qui est adoptée par un organisme national de normalisation et qui est mise à la disposition du public ;[485] *»*

Il importe de spécifier la notion de norme dans le processus d'échange de données car cela permet de différencier la notion de « compatibilité » de celle d'« interopérabilité ». En effet, il y a un glissement sémantique qui conduit de la notion de compatibilité à celle d'interopérabilité connue aujourd'hui. La notion de compatibilité utilisée dans les années 90 caractérise la capacité de deux composants informatiques à fonctionner ensemble, notamment les logiciels et les systèmes d'exploitation. L'interopérabilité est davantage fondée sur l'échange de données et sa construction est étroitement liée à l'émergence des normes : des systèmes d'information sont interopérables s'ils sont capables de se communiquer des données grâce à un protocole de transmission commun. L'interopérabilité ne vaut que pour les fonctions couvertes par la norme commune. Ainsi, les postes informatiques sont désormais interopérables en termes d'affichage des pages Internet, quelles que soient la taille et la définition de leur écran, grâce aux fonctionnalités du langage HTML. Par contre, une fonction qui n'est pas encore couverte par une norme ne peut donner lieu à aucune interopérabilité réelle entre les systèmes d'information. Certes, il est toujours possible d'échanger des fichiers selon un format convenu (correspondant par exemple à un standard de fait, tel que celui d'Adobe Acrobat pour la visualisation des textes avec la mise en page), mais il convient plutôt de parler de « convergence » des systèmes d'information que d'« interopérabilité », puisqu'il est nécessaire d'installer un logiciel spécifique (Adobe Acrobat Reader dans l'exemple choisi) pour utiliser les documents transmis[486].

[485] Article 1er de la directive 98/34/CE.

[486] Extrait du rapport d'information de la Commission des affaires culturelles, familiales et sociales sur le dossier médical personnel présenté par M. Jean-Pierre DOOR le 29 janvier 2008. http://www.assemblee-nationale.fr/13/rap-info/i0659.asp#p34_266743. Consulté le 02 mars 2011
Voir également : DGCIS snitem. *Elaboration d'une politique de normalisation en France pour l'interopérabilité des dispositifs médicaux*. 1er Novembre 2010. On peut dire qu'il y a compatibilité quand deux produits ou systèmes peuvent fonctionner ensemble et interopérabilité quand on sait pourquoi et comment ils peuvent fonctionner ensemble. Autrement dit, on ne peut parler d'interopérabilité d'un produit ou d'un système que si on en connaît intégralement toutes ses interfaces. http://www.industrie.gouv.fr/portail/chiffres/tic-et-sante/politique-de-normalisation-vf.pdf. Consulté le 02 mars 2011.

Le rapport de M. JEGOU[487], du 17 Octobre 2007, indiquait que les agents (automate ou utilisateur final) intervenant dans les systèmes d'information doivent avoir un niveau minimum requis pour interpréter convenablement les contenus échangés pour rendre l'interopérabilité opérationnelle. Dans un système de communications multilatérales, ce niveau minimum est déterminé par l'opérateur doté du plus bas niveau de compréhension. En France, dans le domaine de la santé, tous les opérateurs s'exprimant en français, ils n'éprouvent pas la nécessité de recourir à un interprète, sauf exception. Pour la Direction générale de la modernisation de l'État (DGME), l'élévation du niveau de compréhension repose nécessairement sur une approche conceptuelle du système d'information en vue d'obtenir des outils et des vocabulaires ayant une portée universelle. L'élaboration de référentiels métiers est la traduction concrète de cette approche conceptuelle.

Pour mener à bien sa mission, qui consiste à favoriser le développement de l'interopérabilité des systèmes d'information, l'ASIP Santé[488] a mis sur pied un Cadre d'interopérabilité des systèmes d'information de santé (CI SIS). Ce référentiel spécifie les standards (le plus souvent internationaux) à utiliser dans les échanges et lors du partage de données de santé. Il oblige les utilisateurs à la mise en œuvre de ces standards par des spécifications d'implantation destinées à faciliter le déploiement de l'interopérabilité entre systèmes d'information de santé dans le respect des conditions de sécurité et de confidentialité adéquates. Il permet ainsi une interopérabilité reproductible et efficiente entre systèmes d'information de santé.

L'article 17 du décret relatif à la normalisation dispose que les normes sont en principe, d'application volontaire. Toutefois, elles peuvent être rendues obligatoires par arrêté

[487] *JEGOU, 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 (2007-2008) le 17 octobre 2007. http://www.senat.fr/notice-rapport/2007/r07-035-notice.html. Consulté le 26 mai 2014

[488] ASIP santé. *Présentation du répertoire national des référentiels (RNR).* L'ASIP Santé élabore et maintient un certain nombre de ces référentiels en concertation étroite avec les instances représentatives des acteurs concernés (industriels et professionnels de santé). Elle est aussi amenée à sélectionner des référentiels existants, gérés par des organismes externes (institutions où agences nationales, organismes de normalisation internationaux...). L'ASIP Santé privilégie l'emploi de standards internationaux quel que soit le domaine du référentiel (sécurité, interopérabilité, identification...) dont l'utilisabilité a pu être démontrée après une large pratique et sélectionne ou réalise des adaptations de ces standards au contexte français (traductions, restrictions, extensions, spécialisations). Le répertoire national des référentiels (RNR) est l'infrastructure commune de gestion et de mises à disposition du public (industriels, professionnels établissements de santé, institutions) des référentiels nationaux maintenus ou sélectionnés par l'ASIP Santé. http://esante.gouv.fr/referentiels/rnr/presentation-du-repertoire-national-des-referentiels-rnr. Consulté le 21 avril 2014

signé du ministre chargé de l'industrie et du ou des ministres intéressés. Les normes rendues obligatoires sont consultables gratuitement sur le site[489] Internet de l'association française de normalisation (AFNOR). L'application obligatoire d'une norme est marquée par la référence à la norme dans un texte réglementaire comme moyen unique pour satisfaire aux exigences du texte. Dès lors, pour des usages particuliers et pour un certain type d'administrés, les pouvoirs publics peuvent adopter des textes distincts du champ du décret précité pour conférer à une norme, ou une partie de celle-ci, un caractère obligatoire en tenant compte d'éléments particuliers propres au contexte. Il peut s'agir d'un motif d'ordre public impérieux, comme des impératifs de moralité publique, d'ordre public, de sécurité publique, de protection de la santé et de la vie des personnes et des animaux ou de préservation des végétaux. Cela est possible que la norme soit d'origine nationale, européenne ou internationale. Généralement, ce sont des normes portant sur des méthodes d'essais ou d'analyse. La confiance dans les échanges internes ou extérieurs à la communauté européenne se trouve renforcée par l'usage de telles normes. Les normes telles qu' X. 500, X. 509, ISO 9594 - 8, ou ISO 9834 – 1, etc… qui ont été appliquées dans le cadre des cartes CPS ne sont pas des normes d'application obligatoire. Elles sont soit, internationales, soit européennes et françaises[490]. L'aspect international est à mettre à l'actif des normes servant de référence à l'interopérabilité des systèmes d'information de santé. La norme est bien souvent le résultat de conventions entre les parties qui reposent sur une obligation minimale d'atteinte d'un niveau donné de la technique. La pérennité de l'interopérabilité ne pourra être garantie que si elle repose autant que possible sur les normes internationales car les normes nationales peuvent être plus riches mais peuvent conduire à des incompatibilités lors d'échanges internationaux. Les normes sont évolutives pour suivre l'évolution des technologies ; les risques de divergence, au fil du temps, de la part des industriels et des éditeurs de logiciels ne sont pas exclus[491].

[489] http://www.boutique.afnor.org/ . Voir la rubrique « accéder à l'offre de normes et de livres en ligne ».

[490] Les spécificités de ces normes sont précisées sur le site de l'AFNOR: http://www.boutique.afnor.org/.

[491] JEGOU, 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 (2007-2008) le 17 octobre 2007. http://www.senat.fr/notice-rapport/2007/r07-035-notice.html. Consulté le 26 mai 2014

La réglementation des normes, toutes disciplines confondues, prévoit des normes conférant une présomption de conformité (Résolution[492]). Les pouvoirs publics peuvent, par un texte, conférer cette présomption au respect de tout ou partie d'une norme.[493]

Outre la normalisation, la sécurisation des échanges est une disposition essentielle à prendre pour la mise en œuvre de l'interopérabilité. Après avoir authentifié les intervenants dans le processus, il faut recourir aux outils de chiffrement (c'est-à-dire la cryptographie[494] qui fera l'objet d'une analyse plus approfondie dans la seconde partie de cette étude). Ce mécanisme de protection des fichiers dont la libéralisation a mis du temps à se faire en France[495], permet de préserver autant la confidentialité que l'authenticité des données échangées. Seul le destinataire voulu doit pouvoir y accéder et aucune modification ne doit pouvoir être apportée auxdites données pendant l'échange.

Les conditions ainsi réunies doivent, en principe, permettre l'interopérabilité des systèmes d'information mais la mise en œuvre, en matière de santé, connaît encore des limites.

---

[492] Résolution du Conseil (85/C136/01) du Conseil de l'Europe du 7 mai 1985 relative à une nouvelle approche en matière d'harmonisation technique et de normalisation - JOCE C 136 du 4 juin 1985. p. 1-9. La directive 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 en est une des mesures d'application. Elle a été modifiée par la directive 98/48/CE. JOCE L 217 du 5 Août 1998. http://eur-lex.europa.eu/LexUriServ/LexUriServdo?uri= OJ:L:1998:217:0018:0026:FR:PDF Consulté le 26 mai 2014.

[493]Pour plus d'information sur la réglementation des normes, voir le guide d'utilisation des normes sur le site de la DGCIS. http://www.industrie.gouv.fr/portail/pratique/guide_juin09.pdf. Consulté le 26 mai 2014

[494] La cryptographie, *« l'art d'écrire en éléments secrets est la dissimulation du contenu d'une information par un procédé connu des seuls utilisateurs »*. Le secteur de la santé a été le premier à mettre en œuvre le mécanisme de la cryptographie à grande échelle à travers la transmission électronique des feuilles de soins qui fait intervenir plusieurs acteurs comme le ministère de la santé, les caisses d'assurance-maladie et l'ordre des médecins. Le volume des transactions, les enjeux financiers, les problèmes liés à l'éthique et au secret médical ont induit de très fortes contraintes de sécurité sur le réseau, les logiciels applicatifs et les dispositifs (à des professionnels de santé et à des patients).
CAMPANA Mireille. Groupe d'études société de l'information et vie privée. *La cryptographie* in La protection de la vie privée dans la société d'information. Chapitre 10. Tome 2. PUF. 2000. pp. 54 et 61.

[495]Deux décrets n° 99-199 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation et n° 99-200 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable du 17 mars 1999 ont servi au gouvernement à libéraliser l'utilisation de la cryptologie dont le seuil est passé de 40 à 128 bits. Ces décrets ont été abrogés par le décret n°2007-663 du 2 mai 2007 (Article 22). JORF du 4 mai 2007. p. 7865 texte n°1. NOR: PRMD0751412D. L'abrogation concerne également le décret n°98-101 du 24 février 1998 qui définit les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie avec la précision selon laquelle *« les déclarations souscrites avant la date d'entrée en vigueur du présent décret demeurent régies par les dispositions du décret n° 98-101 du 24 février 1998. »*

Paragraphe 2 : Les limites de l'interopérabilité

Les systèmes d'information de santé connaissent aujourd'hui d'énormes difficultés pour être effectivement interopérables, mais la France et l'Europe sont engagées dans la mise en œuvre d'une politique de construction de cette interopérabilité.

A. Les difficultés de mise en œuvre de l'interopérabilité

Les difficultés de mise en œuvre de l'interopérabilité des systèmes d'information de santé peuvent être classées en deux groupes : les difficultés d'ordre technologiques et celles d'ordre sociologiques.

1. Les difficultés d'ordre technique

Comme nous l'avons indiqué plus haut l'interopérabilité n'est possible que si les échanges se font dans le respect des normes requises dans le domaine. Des travaux réguliers dits « de normalisation syntaxique[496] » s'imposent. Selon le rapport DOOR du 29 janvier 2008, *« dans le domaine de la santé, la normalisation syntaxique demeure un défi, en raison de la richesse du vocabulaire médical et de la complexité de la prise en charge thérapeutique. De plus, le socle central de ce mouvement est le protocole HL7, dont le développement est entravé depuis près de dix ans par un conflit méthodologique[497]».* Ce rapport de 2008 indiquait que les normes qui fondent l'interopérabilité des systèmes d'information de santé ne sont pas stabilisées et couvrent les besoins des services spécialisés de manière encore

[496] Ces travaux consistent à définir un vocabulaire et une grammaire commune aux types de données utilisées dans un secteur d'activité donné. *Rapport DOOR* précité. Disponible sur : http://www.assemblee-nationale.fr/13/rap-info/i0659.asp

[497] Rapport d'information n° 659 du 29 janvier 2008 présenté par M. Jean-Pierre DOOR au nom de la Commission des affaires culturelles, familiales et sociales sur le dossier médical personnel. Disponible sur: http://www.assemblee-nationale.fr/13/rap-info/i0659.asp

incomplète. Par exemple, la norme HL7[498] n'était pas fonctionnelle alors qu'elle a vocation à décrire les actes de soins, toutes spécialités confondues. Ce qui est de nature à montrer le caractère précaire des initiatives privées de normalisation alors même que les organismes publics peinent à conduire, à long terme, ces projets. La version 3 de la norme HL7 a eu du mal à être admise par les autorités françaises et européennes du fait de la lourdeur de sa mise en œuvre qu'on lui reprochait et des difficultés éventuelles d'adaptation. La version 3, même plus substantielle, n'a pas connu beaucoup de succès auprès de ces industriels qui, auraient subi un coût trop élevé vu ce qu'ils avaient déjà investi dans la version 2. Ceux-ci ont préféré poursuivre leurs travaux sur la base de cette version 2 dans le cadre de l'initiative IHE[499] (Integrating the health entreprise). Ce forum est l'occasion de répondre à deux questions techniques fondamentales relatives à l'interopérabilité : d'un côté, si les normes existantes couvrent tout le périmètre des fonctions concernées par les échanges de données prévus, et

[498] HL7 (Health Level Seven) est une organisation internationale à but non lucratif produisant des normes d'interopérabilité pour les échanges entre applications du domaine de la santé. Les normes d'HL7 sont produites dans un cadre de gouvernance strict garantissant l'établissement d'un consensus. Ces standards deviennent de facto des standards ANSI (American National Standards Institute). Certains d'entre eux sont ensuite soumis à l'ISO TC 215 en vue d'une adoption en tant que normes ISO. L'utilisation des normes HL7 est libre de droit**.** En revanche, l'accès à la documentation de ces normes est réservé aux adhérents d'HL7 Inc ou aux adhérents de ses affiliés internationaux, parmi lesquels l'affilié français HL7 France H'. IHE fournit des guides d'implémentation des normes HL7. http://www.mediboard.org/public/HL7. Consulté le 26 mai 2014.
HL7 est tiré de « Healthcare », et « Level 7 » renvoie au septième niveau du modèle de communication de l'Organisation internationale de normalisation (ISO) pour l'interconnexion des systèmes ouverts (OSI) – le niveau application. Sa principale fonction est de transmettre la signification des renseignements échangés entre les systèmes de soins de santé et elle est essentielle à l'interopérabilité. *Guide de l'unité collaborative de normalisation*. P. 22. https://www.infoway-inforoute.ca/flash/lang-fr/scguide/docs/StandardsCatalogue_fr.pdf. Consulté le 26 mai 2014.

[499] IHE est une initiative des professionnels de la santé en vue d'améliorer les performances des logiciels d'échange d'informations dans le domaine. Dans cette optique, l'IHE préconise l'utilisation coordonnée de standards établis comme DICOM et HL7 pour résoudre les problèmes récurrents d'intégration de la multitude de logiciels en matière de santé. L'objectif final est donc de favoriser une meilleure interopérabilité entre les systèmes qui utilisent les solutions IHE. En France, IHE a été créé en 2001 par la SFR (Société Française de Radiologie) et par le GMSIH (Groupement pour la modernisation du système d'information hospitalier). IHE-France a organisé les premiers Connectathons (plate forme de tests et d'intégration autour de laquelle se réunissent les industriels du domaine) en Europe. L'initiative IHE est intégrée, depuis 2009, aux activités de l'association « interop'santé » et est soutenu par :

- des associations d'utilisateurs : SFR, SFIL (Société Française d'Informatique de Laboratoire), l'ADICAP (Association pour le Développement de l'Informatique en Cytologie et en Anatomie Pathologiques), PHAST (Association de Pharmaciens Hospitaliers), SDB (Syndicats des Biologistes), FNI (Fédération Nationale des Infirmiers), EDISANTE (échange de données informatisées dans le secteur de la santé) devenu EDESS:(échange de données dans l'espace sanitaire et sociale) le 22 janvier 2014.
- des institutionnels comme l'ASIP Santé, l'INRIA (Institut National de Recherche en Informatique et en Automatique),
- des syndicats d'industriels : LESISS (Les Entreprises des Systèmes d'Information Sanitaires et Sociaux).

IHE-France organise des réUnions de travail pour la définition des spécificités françaises, de nouveaux profils ou de domaines comme le laboratoire et l'anatomopathologie. http://www.interopsante.org/412_p_15685/ihe-en-france.html. Consulté le 26 mai 2014.

d'un autre côté, si celles-ci sont suffisamment fiables pour une utilisation professionnelle permettant l'automaticité des procédures[500].

Un autre souci d'ordre technique est causé par la multiplicité d'opérateurs logiciels. Le potentiel d'interopérabilité permis par les techniques se voit handicapé par des « *difficultés à assurer une gestion unifiée de l'information sur les structures et à l'absence de normalisation des concepts ou faute d'opérateur unique expressément habilité en la matière, chaque acteur développe son propre système, incapable de communiquer avec les autres*[501]. » Bien que certains secteurs arrivent à inter opérer en s'appuyant sur les normes et standards du marché (c'est le cas des applicatifs spécialisés qui ont imposé leurs standards comme le Sesam-Vitale[502] pour la communication des feuilles de soins électroniques, des domaines spécialisés comme la cancérologie ou la diabétologie), un blocage se crée dès que l'on étend le champ de l'interopérabilité à l'ensemble des acteurs. Les applications informatiques restent assez propriétaires et peu communicantes ; ce qui provoque un faible niveau de compatibilité des logiciels informatiques entre les hôpitaux. Ce problème a également été soulevé par M.

[500] Pour la Commission des affaires des affaires culturelles, familiales et sociales, ce sont des questions qui relèvent majoritairement de la compétence du vendeur de logiciel. Mais elle encourage « *l'État à se donner les moyens d'identifier les besoins d'échanges correspondant à ses ambitions en matière d'interopérabilité et s'engager effectivement dans le développement des normes y répondant* ». Rapport d'information n° 659 du 29 janvier 2008 présenté par M. Jean-Pierre DOOR au nom de la Commission des affaires culturelles, familiales et sociales sur le dossier médical personnel. http://www.assemblee-nationale.fr/13/rap-info/i0659.asp. Consulté le 26 mai 2014.

[501] Avis n° 1971 du 6 novembre 2009 présenté au nom de la Commission des affaires sociales sur le projet de loi de finances pour 2010 (numéro 1946) tome II Santé et système de soins par M. Rémi DELATTE, Député. Enregistré à la présidence de l'Assemblée nationale le 14 octobre 2009. 75P. Disponible sur: http://www.assemblee-nationale.fr/13/budget/plf2010/a1971-tii.asp#P338_62675. Consulté le 26 mai 2014.

[502] Le GIE SESAM-Vitale a été créé pour assurer la mise en œuvre et la supervision opérationnelle d'une infrastructure d'échanges mutualisée prenant en compte dans les meilleures conditions économiques et opérationnelles :

- la grande diversité des catégories de Professionnels de Santé : médecins généralistes et spécialistes, pharmaciens, dentistes, infirmières, laboratoires, auxiliaires médicaux, etc.
- la diversité des organisations d'Assurance Maladie Obligatoire *(régime général, régime agricole, régimes spéciaux, etc.)* et Complémentaire *(mutuelles, assurances, institutions de prévoyance...)* ;
- l'exigence d'un moyen d'identification pratique commun à l'ensemble des assurés.

Le lancement du programme SESAM-Vitale s'est appuyé sur un choix fondateur stratégique : diffuser des cartes à puce individuelles comme support d'identification et d'authentification des assurés et des Professionnels de Santé. La France est ainsi devenue le précurseur de la généralisation à grande échelle de cette technologie appliquée au monde de la santé. L'infrastructure mutualisée SESAM-Vitale gère aujourd'hui plus d'un milliard de transactions par an en relation avec 270 000 Professionnels de Santé. Initialement dédiée aux flux de remboursements de soins dans le secteur libéral, l'infrastructure s'ouvre aux Etablissements *(hôpitaux, cliniques)* et a vocation à sécuriser l'accès aux nouveaux services en ligne de l'Assurance Maladie. *Rapport annuel 2009 du GIE SESAM-VITAL*. P.4. http://www.sesam-vitale.fr/nous-connaitre/docs/rapportannuel2009.pdf. Consulté le 26 mai 2014.

Philippe CHOSSEGROS, président de la coordination nationale des réseaux de santé, au sujet des dossiers médicaux. Il faisait remarquer que *« la décision de mise en œuvre du DMP se confronte à un équipement très hétérogène des professionnels libéraux et hospitaliers avec une multiplicité de logiciels plus ou moins récents et actualisables qui se caractérisent par leur incompatibilité ».* [503]

Le rapport de la Cour des Comptes de septembre 2007 indique que «*le parc de logiciels est atomisé»* tant au niveau des systèmes de gestion des dossiers médicaux des médecins de ville que de ceux des unités de production de soins installés dans les établissements hospitaliers. En effet, une étude réalisée en 2003 a montré que sur un ensemble de 18 établissements hospitaliers 16 logiciels différents étaient utilisés[504]. Dans les cabinets de radiologie et les laboratoires où les systèmes d'information sont couplés à des équipements techniques, notamment d'imagerie médicale, le faible nombre de constructeurs de tels matériels rend le parc logiciel moins atomisé.

L'avis[505] présenté par M. DELATTE relève que la CPS est très peu diffusée en milieu hospitalier. D'une part, la CPS n'est pas suffisamment utilisée du fait de l'absence d'une véritable politique de sécurité des systèmes d'information au sein des établissements ; ce qui provoque un faible développement au sein des systèmes d'information hospitaliers des infrastructures de sécurité (annuaires des personnels, gestion personnalisée des habilitations...). La CPS présente donc peu d'intérêt en l'absence d'applications pour en exploiter les avantages. Surtout, contrairement au secteur libéral, l'utilisation de la CPS des professionnels de santé n'est pas nécessaire pour la facturation des prestations aux organismes d'assurance maladie. D'autre part, certains modes de fonctionnement des centres hospitaliers ne sont pas adaptés à l'utilisation de la carte. Le dispositif de lecture «avec contact» dont est équipée la CPS nécessite que la carte soit insérée dans le lecteur pendant la durée de l'exécution d'un traitement. Cette formule est difficile à appliquer pour les praticiens des

[503] Le rapport de M. DOOR du 29 janvier 2008 p. 34 reprend cette intervention de M. CHOSSEGROS Philippe dans son article *Le DMP : plus d'un simple outil technique à optimiser.* http://www.assemblee-nationale.fr /13/pdf/rap-info/i0659.pdf. Consulté le 26 mai 2014.

[504] Rapport de la Cour des Comptes relatif à la sécurité sociale. *Chapitre X : le partage de données entre les systèmes d'information de santé*. Septembre 2007. P 316

[505] Avis n° 1971 du 6 novembre 2009 présenté au nom de la Commission des affaires sociales sur le projet de loi de finances pour 2010 (numéro 1946) tome II Santé et système de soins par M. Rémi DELATTE, Député. Enregistré à la présidence de l'Assemblée nationale le 14 octobre 2009. 75p http://www.assemblee-nationale.fr/ 13/budget/plf2010/a1971-tii.asp#P338_62675. Consulté le 27 mai 2014.

hôpitaux qui utilisent des postes partagés ou qui doivent utiliser successivement plusieurs postes. La nouvelle carte CPS 3 qui intègre les technologies de lecture « sans contact » permettra de résoudre ce problème. En outre, la loi dite «HPST[506]» autorise des solutions alternatives[507] comme les supports mobiles. L'avis donne l'exemple des «*clés USB*» tout comme les initiateurs du projet. Sous l'impulsion de certains députés dont M. Jean-Pierre DOOR, depuis décembre 2008, dans le cadre de l'examen du projet de loi de financement de la sécurité sociale pour 2009[508], a été annoncé un dossier médical portable. Mais l'amendement le proposant n'a été adopté par l'Assemblée nationale qu'en mars 2010 et l'expérimentation a été prévu pour, au plus tard, le 31 décembre 2011 et jusqu'au 31 décembre 2013 («le temps de laisser le Sénat réfléchir à la question») avec des dossiers de patients atteints d'affections de longue durée (ALD)[509]. Pour la Commission des affaires sociales, ce support permettra aux professionnels de santé qui travaillent, ou choisiront de travailler, dans les SISA[510] ou les maisons de santé d'avoir un meilleur outil de partage d'informations, la meilleure circulation de l'information étant nécessaire pour la qualité de coordination de soins.

---

[506] La loi hôpital, patients, santé et territoires ou encore loi Bachelot. 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 texte n° 1. NOR : SASX0822640L. Le texte adopté le 23 juin 2009 à l'Assemblée nationale et le 24 juin 2009 par le Sénat, institue une territorialisation de politique de santé et porte une réforme globale qui doit permettre aux institutions de structures de s'adapter aux nouveaux besoins de la population. Cette réforme a également pour objectif de ramener les hôpitaux publics à l'équilibre budgétaire en 2012. http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020879475&categorieLien=id. Consulté le 27 mai 2014.

[507] Article 132 de la loi HPST: *« Le quatrième alinéa de l'article L. 1110-4 du code de la santé publique est ainsi modifié :*
1° A la seconde phrase, les mots : « carte professionnelle de santé » sont remplacés par les mots : « carte de professionnel de santé », et après les mots : « la sécurité sociale », sont insérés les mots : « ou un dispositif équivalent agréé par l'organisme chargé d'émettre la carte de professionnel de santé »;
2° Il est ajouté une phrase ainsi rédigée : « 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. » http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020879475&categorieLien=id. Consulté le 27 mai 2014.

[508] Article 35 bis. Examen des articles L. 161-36-1, L. 161-36-2 et L 161-36-3-2 du nouveau code de la sécurité sociale. Expérimentation d'un dossier médical sur support mobile. http://www.senat.fr/rap/l08-083-7/l08-083-78.html#toc54. Consulté le 27 mai 2014.

[509] Aux termes de l'article 12 bis (nouveau) du rapport fait au nom de la Commission des affaires sociales sur la proposition de loi adoptée par le Sénat 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, dite loi FOURCADE (ou HPST).

[510] Société interprofessionnelle de soins ambulatoires. Le 9 février 2011, la Commission des affaires sociales du Sénat a adopté une définition de la SISA, société interprofessionnelle de soins ambulatoires. Les SISA constituent les cadres juridiques pour la pratique regroupée des professionnels de santé exerçant en mode libéral. Les SISA seront des sociétés civiles de personnes physiques qui exercent une profession de santé, des sociétés comportant au moins deux médecins et un auxiliaire médical. Infirmiers.com.. *Une "société interprofessionnelle de soins ambulatoires" pour les professionnels de santé libéraux*. 18 décembre 2012. http://www.infirmiers.com/

L'avis[511] présenté par M. Rémi DELATTE citait également l'absence d'identifiant commun du patient comme un « *obstacle majeur à l'interopérabilité orientée patient* » tout comme l'identifiant unique des professionnels de santé. Il estimait que l'interopérabilité des systèmes d'information en santé ne pouvait être satisfaite en l'absence de référentiels communs et d'unicité des identifiants.

2. Les limites d'ordre sociologique

Les obstacles d'ordre sociologiques s'apprécient dans les rapports entre professionnels et dans la politique menée par les pouvoirs publics pour améliorer l'interopérabilité des systèmes de santé. Il faut souligner que « *la volonté de partage de l'information n'est pas suffisamment admise, ni au niveau des principes, ni, a fortiori, au niveau de la nature des informations qu'il serait utile d'échanger » selon le rapport JEGOU.*

Dans les échanges entre professionnels, le coût du matériel est capital dans la décision de communiquer électroniquement. M. JEGOU n'a pas manqué de le relever en ces termes : « *la pratique de l'interopérabilité suppose que les acteurs de santé concernés adoptent une attitude volontariste pour échanger de l'information. Mais l'appréciation par ces derniers du degré d'utilité de l'interopérabilité est à rapprocher du coût qu'ils sont prêts à y consentir et du profit qu'ils en attendent. Le jeu « gagnant-gagnant », entre émetteurs et récepteurs d'information, n'est semble t-il pas assuré, ni au plan pécuniaire, ni au plan des avantages espérés dans l'exercice de leur activité*[512]*».* Ainsi, les moyens traditionnels restent les plus usités. Selon le rapport de la Cour des comptes de septembre 2007, les échanges formalisés entre les professionnels de santé sont limités[513]. Soit, les informations sont transmises dans les carnets de santé traditionnels, soit par des dossiers sur support papier, notamment le document

votre-carriere/ide-liberale/une-societe-interprofessionnelle-de-soins-ambulatoires-pour-les-professionnels-de-sante-liberaux.html Consulté le 28 avril 2014.

[511] Avis n° 1971 du 6 novembre 2009 présenté au nom de la Commission des affaires sociales sur le projet de loi de finances pour 2010 (numéro 1946) tome II Santé et système de soins par M. Rémi DELATTE, Député. Enregistré à la présidence de l'Assemblée nationale le 14 octobre 2009. 75p. Disponible sur: http://www.assemblee-nationale.fr/13/budget/plf2010/a1971-tii.asp#P338_62675. Consulté le 27 mai 2014.

[512] JEGOU, Jean-Jacques. *Système d'information de santé : le diagnostic est posé, le traitement s'impose.* Rapport d'information n° 35 (2007-2008) fait au nom de la Commission des finances, déposé le 17 octobre 2007. http://www.senat.fr/rap/r07-035/r07-035_mono.html#fn30. Consulté le 27 mai 2014.

[513] Rapport de la Cour des comptes de septembre 2007. P. 317. op cit.

médical de synthèse[514] ou encore sous la forme de lettre de sortie adressée au médecin traitant (médecin référent). En clair, il n'y a pas vraiment de transmission électronique pour prétendre à une quelconque interopérabilité entre systèmes d'information. De plus, le rapport déplore que les textes ne soient pas plus explicites et plus larges quant au type d'information échangeable et à la forme de la transmission. Tout cela contribue à limiter l'interopérabilité car son développement ne peut permettre d'autres échanges que ceux prévus par les textes.

L'interopérabilité entre les systèmes d'information est également freinée par le respect du secret médical. Les articles 58, 59 et 60 du code de déontologie médicale impose au médecin de ne transmettre l'information médicale d'un patient qu'après avoir informé ce dernier ou après avoir obtenu son autorisation. Des exceptions sont admises dans des cas prévus par l'article L. 1110-4[515] du code de la santé publique et l'article 64[516] du code de déontologie médicale. Le respect du secret médical ne pose pas de problème au sein des hôpitaux car la circulation des données médicales se fait dans le cadre d'échanges d'informations entre les membres d'une équipe soignante. En revanche, il constitue une contrainte certaine pour la médecine de ville où les échanges entre les systèmes d'information des professionnels de santé ne peuvent s'opérer qu'avec l'autorisation ou l'information du patient. Le rapport de la Cour des comptes relève ainsi un conflit d'intérêts entre une nécessité d'ordre technique et une valeur fondamentale du droit de la santé : le secret médical. Cette situation amène à analyser plus sérieusement la réflexion faite par M. JEGOU au sujet de

[514] Le document médical de synthèse a remplacé le dossier médical de suivi (institutionnalisé pour les praticiens du secteur privé par la loi du 18 janvier 1994 pour favoriser la continuité des soins) après l'abrogation de celui-ci par ordonnance du 24 avril 1996. Ce dossier doit être tenu par le médecin ayant fait le choix de l'option conventionnelle prévue à l'article L. 162 du code de la sécurité sociale dit « médecin référent ». Le document médical de synthèse a été institué par la convention nationale des médecins généralistes du 26 novembre 1998 approuvée par arrêté ministériel le 4 décembre 1998. JORF n° 282 du 5 décembre 1998, p.18329. La convention est entrée en vigueur jusqu'au 7 décembre 2002. BENSSOUSSAN, Alain et MOLE, Ariane. *Guide juridique du dossier médical informatisé*. P. 14.

[515] Article L. 1110-4[515] du code de la santé publique, alinéa 3 « *Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. 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* ». http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006685746. Consulté le 27 mai 2014.

[516] Article 64 (article R.4127-64 du code de la santé publique) *« 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 »*. http://www.web.ordre.medecin.fr/deonto/decret/codedeont.pdf. Consulté le 27 mai 2014.

l'interopérabilité comme posant en elle-même un dilemme. Autant il est nécessaire de mettre dans un échange fluide des informations, autant il est dangereux de laisser libre cours à la circulation des informations. *« L'interopérabilité suppose un cadre réglementaire, qui en fixe les règles d'usage, car elle ne doit pas conduire à un partage universel et incontrôlé de l'information. Il faut donc lui associer des outils de régulation qui permettent d'en contrôler, voire, d'en interdire l'usage*[517] *»*. Il faut noter que le problème ne fait qu'être déplacé avec cette solution car elle propose toujours une limite d'accès. On se retrouve finalement dans un cercle vicieux et nous nous demandons s'il y a bien une solution qui pourrait préserver la confidentialité des informations du patient sans limiter l'interopérabilité.

Au niveau de l'organisation des pouvoirs publics, le rapport de M. JEGOU rappelle que le constat fait par le référé[518] de la Cour des Comptes sur l'interopérabilité des systèmes d'information santé le 15 septembre 2006 demeure d'actualité. Le pilotage organisé par l'État n'est pas suffisamment efficace du fait du trop grand nombre[519] de directions ou de structures

[517] C'est le même principe que celui du réseau Internet sur lequel, même conçu pour assurer l'interopérabilité entre les systèmes, il existe la notion de sous réseaux privés inaccessibles de l'extérieur et généralement dotés de dispositifs anti intrusion (pare-feux), de sécurité et de confidentialité, ainsi que des outils permettant d'interdire l'accès à certains sites (outils de type proxy, gestion de sites de confiance, listes de sites interdits, etc.). *JEGOU, 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 (2007-2008) le 17 octobre 2007. http://www.senat.fr/notice-rapport/2007/r07-035-notice.html. Consulté le 27 mai 2014.

[518] Cour des Comptes. Référé n° 46 485 délibéré le 15 septembre 2006, sixième section première chambre. Ce référé avait pour objet d'apprécier les progrès effectués en matière d'interopérabilité des systèmes d'information en santé au cours des dernières années, notamment, en vue de favoriser la mise en œuvre du dossier médical personnel. Annexe I du rapport JEGOU. http://www.senat.fr/rap/r07-035/r07-035_mono.html#toc44 Consulté le 27 mai 2014.

[519] Le domaine de la santé se caractérise par un grand nombre de systèmes d'information interdépendants, mais dont les projets sont pilotés par des structures différentes. Deux structures ont donc été créées en 1997 auprès du ministère de la santé pour renforcer la coordination de la démarche d'informatisation du système : le Conseil supérieur des systèmes d'information de santé (CSSIS) et la mission pour l'informatisation du système de santé (MISS). En dehors de ces deux entités la DHOS, le GMSIH, la MAINH, l'ATIH, PERNNS pour le secteur hospitalier et le FAQSV et du DNDR pour la médecine de ville.

- DHOS : Direction de l'hospitalisation et de l'organisation de soins. Par un décret et par arrêté le 15 mars 2010, la DHOS est devenue DGOS pour promouvoir une prise en charge globale du patient en ville et à l'hôpital.
- GMSIH : Groupement pour la modernisation du système d'information hospitalier, créé en 2000 sous la forme d'un groupement d'intérêt public auprès duquel la DHOS assure la fonction de Commissaire du gouvernement. Tous les établissements de santés publiques et privées en sont automatiquement membres.
- MAINH : Mission nationale d'appui à l'investissement hospitalier. Elle est chargée d'accompagner techniquement le programme de rénovation hospitalier. La compétence de la MAINH. a été étendue aux systèmes d'information hospitaliers par arrêté du 1er juillet 2005.
- ATIH : Agence technique de l'information sur l'hospitalisation. Créé par décret le 26 décembre 2007 un établissement public administratif placé sous la tutelle du ministère de la santé. Elle assure la collecte auprès des établissements de santé de données relatives aux PMSI (programme de médicalisation des systèmes d'information) et contribuer à la constitution de nomenclature notamment la classification commune des actes médicaux (CCAM) et la classification internationale des maladies (CIM).

périphériques au ministère de la santé impliquées dans le projet, et de la mauvaise organisation (y compris la mauvaise organisation des tâches) de ces structures. La maîtrise d'ouvrage des projets, comme le DMP ou la tarification à l'activité (T2A) dans les établissements de santé, n'est pas suffisamment coordonnée. La Cour des Comptes avait, d'ailleurs, critiqué le rattachement administratif et budgétaire de la mission nationale d'appui à l'investissement hospitalier (MAINH) à l'agence régionale de l'hospitalisation de l'Ile-de-France, ainsi que son positionnement auprès du ministère et non auprès de la direction de l'hospitalisation et de l'organisation de soins (DHOS). D'un autre côté, la chambre des communes britannique, lors d'une mise au point[520] relative à l'état d'avancement de l'équivalent anglais du DMP (Electronic Patient Record) a souligné combien la France était loin d'assurer l'interopérabilité des systèmes d'information de santé et de mettre effectivement en place le dossier médical personnel en se basant, par exemple, sur le nombre limité de systèmes d'imagerie numérique dans les hôpitaux français (seulement 1/3 d'entre eux en dispose).

Face à toutes ces difficultés de mise en œuvre de l'interopérabilité des systèmes d'information de santé, on a été amené à penser qu'il y a un réel manque de volonté politique d'amélioration du système. Mais, l'initiative prise par la ministre de la santé, de la jeunesse et des sports permet de croire que les autorités publiques comptent, désormais, améliorer la situation. Consciente de la nécessité d'entreprendre des réformes d'envergure pour rendre le système d'information de santé interopérable, la ministre Roselyne BACHELOT-NARQUIN, à l'occasion de l'examen du projet de loi de financement de la sécurité sociale pour 2008 a exprimé sa volonté de « reprendre en main[521] » le chantier du DMP et celui du pilotage des systèmes d'information de santé en général.

- PERNNS : Pole d'expertise et de référence nationale de nomenclatures de santé.
- FAQSV : Fonds d'aide à la qualité des soins de ville. La gestion du FAQSV est assuré par les Unions régionales des caisses d'assurance-maladie (URCAM) que par la caisse nationale d'assurance-maladie (CNAMTS)
- DNDR : Dotation nationale de développement des réseaux.

[520] House of Commons, Health committee. *The electronic Patient Record*, sixth report of session 2006-2007. Volume 1, ordered by the House of commons to be printed 25 july 2007. P. 21. HC 422, published on the 13 September 2007. http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422.pdf

[521] BACHELOT-NARQUIN Roselyne, Ministre de la santé de la jeunesse et des sports. Propos recueillis lors de l'examen de l'article 36 du projet de loi de financement de la sécurité sociale pour 2008. Compte rendu des débats du Sénat de la séance du 15 novembre 2007. JORF n° 66 S (C.R) du 16 novembre 2007. P. 4846-4847 http://www.senat.fr/seances/s200711/s20071115/s20071115.pdf. Consulté le 26 mai 2014.

Par ailleurs, le directeur de cabinet de la ministre, M. Georges-François Leclerc avait annoncé lors de l'audition du 16 octobre 2007 des réformes de structures qui se tiendraient en 2008. Le ministère avait décidé de ne plus rattacher budgétairement certaines agences, notamment, la mission d'appui à l'investissement hospitalier (MAINH) et la mission d'expertise et d'audit hospitalier (MEAH) à l'agence régionale de l'hospitalisation (ARH) d'Ile - de - France[522].

Ces initiatives sont corroborées, depuis 2009, par des projets et des réformes tant organiques que techniques qui militent en faveur d'une véritable politique des autorités françaises et européennes de construction de l'interopérabilité entre les systèmes d'information de santé.

B. La politique de concrétisation de l'interopérabilité

Les travaux de la Cour des Comptes relatifs au partage des données entre les systèmes d'information de santé ayant relevé des failles dans la politique de pilotage des systèmes d'information en santé par le ministère, la ministre de la santé et des sports a défini une stratégie globale de développement. Cette politique de « e-santé » tourne autour de 2 axes principaux présentés le 9 avril 2009 par la ministre lors du colloque sur la relance du DMP : unifier la maîtrise d'ouvrage et renforcer le pilotage des systèmes de santé.

1. La construction de l'interopérabilité en France

Dans un souci de rationalisation et de renforcement de la maîtrise d'ouvrage, la ministre a mis en place un nouvel opérateur de système d'information de santé : un regroupement de diverses structures déjà existantes pour obtenir de nouvelles agences aux compétences complémentaires. Ainsi, instituée par la loi HPST, a été créée l'ASIP santé

[522] Annexe 2 du rapport d'information faite au nom de la Commission des finances, du contrôle budgétaire et des comptes économiques de la nation (1) sur le suivi du référé de la Cour des Comptes concernant l'interopérabilité des systèmes d'information de santé, par M. Jean-Jacques JEGOU 17 octobre 2007. P.113 à 118 http://www.senat.fr/rap/r07-035/r07-0351.pdf. Consulté le 26 mai 2014

(Agence des systèmes d'information partagée de santé) par arrêté du 8 septembre 2009[523]. L'ASIP est le résultat du regroupement des missions GIP-DMP[524], GIP CPS[525] et de la mission interopérabilité du GMSH. Elle a pour mission de favoriser le partage des données de santé en assurant l'interopérabilité et la sécurité des systèmes d'information intervenants. L'agence, aussi responsable de la mise en œuvre du DMP est celle à qui le ministère de la santé a confié la maîtrise d'ouvrage opérationnelle des grands référentiels que sont l'identifiant national de santé, les répertoires nationaux de professionnel et de structures, les normes et standards d'interopérabilité, les référentiels de sécurité et confidentialité des données de santé. A ce titre, l'ASIP est impliquée dans la plupart des projets internationaux, nationaux ou régionaux entrant dans son champ de compétence. Elle est à pied d'œuvre pour corriger les problèmes soulevés par les rapports sus-cités à partir de référentiels mis en place pour l'interopérabilité des systèmes d'information de santé.

L'agence a fait le point de la situation, en précisant les évolutions et le niveau de maintenance le 8 février 2011 à l'occasion de la cinquième journée nationale des industriels[526]. Elle a, notamment annoncé que « *les fondements pour assurer l'interopérabilité des systèmes d'information et garantir la confiance des patients et de tous les acteurs de santé sont disponibles et mis en œuvre au plan national dans le DMP*[527]». Il s'agit de « *l'identification unique des patients dans la sphère santé (INS), l'agrément des hébergeurs de données de santé à caractère personnel (PIAHDS) et du cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) validé par les instances représentatives des industriels*[528]».

[523] Cet arrêté portant approbation de la modification de la convention constitutive du GIP-DMP en ASIP Santé a été publié au JORF n° 0213 du 15 Septembre 2009, P. 15096, texte n°15.
La création de l'ASIP santé était une des mesures recommandées par le rapport GAGNEUX d'avril 2008 sur la relance du DMP et reprise par un autre rapport GAGNEUX de mai 2009 relatif à la gouvernance des systèmes d'information de santé. *Avis DELATTE précité*. http://www.assemblee-nationale.fr/13/budget/plf2010/a1971-tii.asp#P338_62675. Consulté le 26 mai 2014

[524] Groupement d'intérêt public du dossier médical personnel.

[525] Groupement d'intérêt public carte de professionnel de santé.

[526]La présentation par l'ASIP santé des référentiels publiés dans le RNR est disponible sur le lien suivant : http://esante.gouv.fr/sites/default/files/110208_JNI_JFP_PGSSI_Referentiels_1.pdf. Consulté le 26 mai 2011.

[527]ASIP santé. *Référentiels pour les SI de santé : Point de situation, Evolutions, maintenance*. 8 février 2011. http://esante.gouv.fr/sites/default/files/110208_JNI_JFP_PGSSI_Referentiels_1.pdf. Consulté le 26 mai 2011.

[528] Idem

Le cadre d'interopérabilité des SIS[529] a été créé le 27 février 2009 et sa dernière mise à jour date du 16 novembre 2010. La version courante du référentiel CI-SIS est la version 1.0.1 publiée le 18 novembre 2010. Elle apporte un lot de corrections éditoriales dans les spécifications et dans les exemples.[530] Le référentiel cadre d'interopérabilité des systèmes d'information de santé vise à 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 télé santé. Quant à l'identifiant unique, même si ses bases ont bien été avancées en 2010, son décret d'application est encore attendu. Ce retard s'explique par le fait que les professionnels effectuent encore des tests pour s'assurer que l'identifiant répondra aux attentes une fois lancé[531]. Pour rappel, le fondement strictement légal, lui, existe déjà à travers l'article L1111-8-1[532] du code de la santé publique qui impose l'utilisation d'un Identifiant National de Santé (INS). En attendant, l'ASIP se montre rassurant quant aux moyens à mettre en place pour sa bonne marche. Dans un communiqué de presse[533] du 18 octobre 2010, l'agence indique que plus de 35 logiciels de professionnels de santé de 22 éditeurs ont intégré les fonctionnalités de

[529] ASIP Santé. *Cadre d'interopérabilité des SIS, document chapeau*. 16 novembre 2010. 16 p. http://esante.gouv.fr/sites/default/files/CI-SIS_Document_Chapeau_v1.0.1.pdf. Consulté le 30 mai 2011.

[530]ASIP santé. *Cadre d'interopérabilité des systèmes d'information de santé*. 3 février 2001. http://esante.gouv.fr/referentiels/interoperabilite/cadre-d-interoperabilite-des-systemes-d-information-de-sante-ci-sis. Consulté le 18 août 2009.

[531] Dans une interview accordée à Charles COPIN par deux représentants de l'ASIP santé : Jeanne BOSSI, secrétaire générale et Jean- François parquet, responsable du pôle architecture, référentiel et sécurité et RSSI ASIP santé, Mme Bossi explique que le retard est volontaire et qu'une fois l'INS bien défini, ils s'attacheraient à en établir les éléments d'application dans le cadre d'un décret. COPIN, Charles. *Où en est-on de l'identifiant santé ?* Idem magazine, avril 2011. http://www.wmaker.net/menaces/idem-magazine/archives/2011/4 /. Consulté le 30 août 2011.

[532] *« Un identifiant de santé des personnes prises 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. » http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=6504FC539045862B0ADB9A7A01953EB1.tpdjo12v_1?idArticle=LEGIARTI000006685788&cidTexte=LEGITEXT000006072665&categorieLien=id&dateTexte=20071221.* Consulté le 30 août 2011.

[533] Communiqué de presse du 18 octobre 2010. *L'identifiant national de santé (INS) prend ses marques et progresse sur le marché des logiciels de santé.* http://esante.gouv.fr/sites/default/files/CP_INS_PointreferencementsCNDA_181010.pdf. Consulté le 30 août 2011.

l'INS. C'est un des pré-requis techniques indispensables pour l'échange et le partage des données personnelles de santé.

Instituée également, par la loi HPST, l'ANAP (Agence nationale d'appui à la performance des établissements de santé et médico-sociaux) a vu le jour par arrêté du 16 octobre 2009[534] à partir du regroupement de 3 entités : le GMSIH[535], la MAINH[536] et la MEAH[537]. La mission[538] de l'ANAP est d'appuyer les établissements de santé et médico-sociaux et les ARS Agences régionales de santé) afin d'améliorer leur performance. L'ANAP leur apportera donc son aide pour optimiser leurs investissements, moderniser leurs systèmes d'information et leurs procédures (avec le soutien financier du plan «hôpital 2012[539]») et développer les bonnes pratiques de gestion et d'organisation.

Une convention de partenariat[540] a été signée entre ces deux agences qui, visant des objectifs complémentaires, ont voulu mettre en commun leurs efforts de modernisation du

---

[534] Arrêté du 16 octobre 2009 publié au JORF n° 0246 du 23 Octobre 2009. p. 17737, texte n° 26 NOR: SASH0923114A. et portant approbation de la convention constitutive du groupement d'intérêt public « Agence nationale d'appui à la performance des établissements de santé et médico-sociaux **».** http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=0659546A1E9A2925B9AA545B745E28DA.tpdjo08v_1?cidTexte=JORFTEXT000021187453&dateTexte=&oldAction=rechJO&categorieLien=id**.** Consulté le 30 août 2011.

[535] Groupement pour la modernisation du système d'information hospitalier.

[536] Mission nationale d'appui à l'investissement hospitalier.

[537] Mission nationale d'expertise et d'audit hospitaliers.

[538] Article 18, alinéa 2 de la loi HPST: *« L'agence a pour objet d'aider les établissements de santé et médico-sociaux à améliorer le service rendu aux patients et aux usagers, en élaborant et en diffusant des recommandations et des outils dont elle assure le suivi de la mise en œuvre, leur permettant de moderniser leur gestion, d'optimiser leur patrimoine immobilier et de suivre et d'accroître leur performance, afin de maîtriser leurs dépenses. A cette fin, dans le cadre de son programme de travail, elle peut procéder ou faire procéder à des audits de la gestion et de l'organisation de l'ensemble des activités des établissements de santé et médico-sociaux. » Disponible sur:* http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020879475&categorieLien=id. Consulté le 30 août 2011.

[539] « *Lancé dès le mois de juin 2007, le plan Hôpital 2012 s'inscrit dans la continuité du volet investissement du plan Hôpital 2007 et a pour objet de maintenir durant la période 2007-2012 un niveau d'investissement équivalent à celui de la période précédente et nécessaire à la réalisation des schémas régionaux d'organisation des soins de troisième génération, au développement des systèmes d'informations et à certaines mises aux normes de sécurité* ». Ministère de la santé. Présentation des opérations retenues au titre du plan hôpital 2012. Dossier de presse, 10 février 2010. http://www.sante.g du mercredi 10 févrierouv.fr/IMG/pdf/Dossier_de_presse_100210-Hopital2012.pdf. Consulté le 30 août 2011.

[540] Communiqué de presse du 20 mai 2010. *Signature de convention de partenariat entre l'ASIP Santé et l'ANAP*. http://esante.gouv.fr/sites/default/files/CP_ASIPSante_ANAP_200510.pdf. Consulté le 28 avril 2014.

système de santé et du secteur médico-social. Dans le cadre de cette convention, des domaines de coopération ont été identifiés et les directeurs des deux agences ont convenu de se rencontrer régulièrement afin de partager leur programme de travail et les problématiques communes de leurs chantiers respectifs. La convention de partenariat est conclue pour une durée d'un an renouvelable tacitement ; ce qui contribuera énormément au renforcement du pilotage des systèmes d'information de santé.

A la demande de la ministre, M. GAGNEUX, Inspecteur général des affaires sociales, a fait en mai 2009[541] un rapport sur le renforcement du pilotage et de la gouvernance des systèmes d'information de santé. Ce rapport formulait des propositions parmi lesquelles la création d'une instance nationale de haut niveau dénommée « Conseil national des systèmes d'information de santé » qui aurait pour objectif d'élaborer une stratégie nationale, d'en définir les priorités et d'en assurer le suivi. Celle-ci a été retenue par la ministre qui a, par ailleurs, chargé le secrétaire général des ministères responsables des affaires sociales de la mission d'assurer le pilotage et la coordination des actions en matière de systèmes d'information, en liaison avec les caisses d'assurance maladie et la caisse nationale de solidarité pour l'autonomie (CNSA). Une « délégation à la stratégie des systèmes d'information de santé » issue d'une évolution et d'un renforcement de la mission pour la formation de ce système de santé servira d'appui au secrétaire général dans cette tâche. L'action de la Délégation sera recentrée sur les fonctions de pilotage stratégique et de prospective. Elle assurera le secrétariat du Conseil national des systèmes d'information de santé et en préparera les travaux. Le décret portant création de cette délégation a été pris le 5 mai 2011[542]. Il en précise les missions[543]. Celles-ci, efficacement menées avec tous les

[541] GAGNEUX. Jean-Michel. Rapport du 3 mai 2009. *Refonder la gouvernance du système d'information de santé*. http://www.sante.gouv.fr/IMG/pdf/Rapport_FINAL_.pdf. Consulté le 27 mai 2014.

[542] Décret n° 2011 - 496 du 5 mai 2011 portant création d'une stratégie à la délégation des systèmes d'information de santé auprès des ministères chargés de la santé, de la sécurité sociale, de solidarité et de la cohésion sociale. JORF n° 0105 du 6 mai 2011. Texte n° 31.NOR : ETSG1106711D. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023950748&dateTexte=&categorieLien=id. Consulté le 31 août 2011.

moyens intellectuels, financiers et industriels pourraient, à terme, propulser la France « *comme leader de la télémédecine et du développement des systèmes d'information médicale partagée*[544]. »

Finalement, force est de constater que les initiatives prises par la ministre pour favoriser l'interopérabilité des systèmes d'information de santé entrent bien dans le cadre des recommandations de la Cour des comptes dans son rapport du 12 septembre 2007[545]. Mais cela n'exclut pas des actions à l'extérieur des frontières françaises pour un partage plus fluide entre systèmes français et systèmes étrangers. C'est l'objectif visé par les projets européens de construction de l'interopérabilité.

---

[543] «*La délégation à la stratégie des systèmes d'information de santé a pour missions, en liaison avec les autres services de l'administration centrale des ministères chargés des affaires sociales :*
1° D'animer le travail d'élaboration des orientations et des priorités nationales dans le domaine des systèmes d'information de santé et médico-sociaux et des technologies numériques appliquées à la santé ;
2° De participer aux organes de pilotage mis en place au niveau national en matière d'informatisation de la santé et du secteur médico-social, de contribuer à la préparation de leurs délibérations et décisions et de mettre en œuvre, dans son domaine de compétence, leurs orientations et leurs décisions ;
3° De préparer les décisions du Conseil national de pilotage des agences régionales de santé en matière de systèmes d'information et de veiller à leur mise en œuvre ;
4° De coordonner les actions des services de l'État, des organismes d'assurance maladie, des agences et organismes intervenant dans le domaine de la santé, des services et des établissements de santé, des services et établissements médico-sociaux et de la Caisse nationale de solidarité pour l'autonomie, en vue de la mise en œuvre de la politique nationale d'informatisation du système de santé et médico-social ;
5° D'assurer la tutelle sur le groupement d'intérêt public dénommé « Agence des systèmes d'information partagés de santé » ;
6° D'orienter et de coordonner l'action à l'échelle européenne et internationale des services des ministères chargés de la santé et des affaires sociales ainsi que des organismes placés sous leur autorité, dans les domaines des technologies numériques et des systèmes d'information ;
7° D'assurer la maîtrise d'ouvrage stratégique des systèmes d'information des services centraux et déconcentrés des ministères chargés des affaires sociales ; à ce titre, elle valide les orientations stratégiques du schéma directeur de ces structures et elle contribue à la définition et à la mise en œuvre d'une politique d'audit.»
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023950748&dateTexte=&categorieLien=id. Consulté le 3 septembre 2011.

[544] C'est la vision d'un certain nombre d'acteurs engagés dans le processus dont le rapporteur pour avis, M. DELATTE. Avis n° 1971 du 6 novembre 2009 présenté au nom de la Commission des affaires sociales sur le projet de loi de finances pour 2010 (numéro 1946) tome II Santé et système de soins par M. Rémi DELATTE, Député. Enregistré à la présidence de l'Assemblée nationale le 14 octobre 2009. 75p http://www.assemblee-nationale.fr/13/budget/plf2010/a1971-tii.asp#P338_62675. Consulté le 3 septembre 2011.

[545] « *35. Réduire le nombre d'opérateurs des systèmes d'information en santé et renforcer le pilotage stratégique par la tutelle.*
36. Apporter sans tarder des solutions opérationnelles aux questions d'identification, de normes et de standard qui conditionnent l'interopérabilité. » http://www.ccomptes.fr/fr/CC/documents/RELFSS/Chap10-partage-donnees-systemes-infos-sante.pdf Consulté le 3 septembre 2011.

2. La construction de l'interopérabilité en Europe

Au plan européen et international, l'interopérabilité des systèmes de santé se heurte au principe de subsidiarité[546] dans la politique de santé que mènent les gouvernements. A l'occasion de la table ronde[547] sur l'interopérabilité médicale dans l'Union européenne, organisée par le Conseil national de l'ordre des médecins, plusieurs intervenants avaient dénoncé le fait que les États membres restent « *maître de leur politique de santé*[548] » et aient *« du mal à harmoniser les systèmes d'échange de données*[549] *»*. Les médecins et autorités gouvernementales français ont pris à bras-le-corps le problème de l'interopérabilité des systèmes de santé en Europe en organisant une table ronde sur l'interopérabilité médicale en Europe. Cette rencontre a eu pour objectif de réfléchir aux dispositions à prendre pour rendre les systèmes européens interopérables sachant que les systèmes de soins et d'information de santé qui coexistent dans l'Union sont différents. Pour eux, l'interopérabilité implique deux domaines distincts mais complémentaires : l'échange entre systèmes et le partage de l'information. « *L'interopérabilité dans le domaine de l'échange entre les systèmes d'information de santé a pour but de faciliter la communication (notamment en matière d'organisation des soins) au sein d'un hôpital, d'un réseau de santé, d'un pays, voire entre des*

---

[546] **«** *Le principe de subsidiarité consiste à réserver uniquement à l'échelon supérieur, ici la Communauté européenne (CE), ce que l'échelon inférieur, les États membres de la CE, ne pourrait effectuer que de manière moins efficace. Ce principe a été introduit dans le droit communautaire par le traité de Maastricht (art. 5 du traité instituant la Communauté européenne-TCE). »* Direction de l'information légale et administrative. Vie publique. *Qu'est-ce que le principe de subsidiarité ?* http://www.vie-publique.fr/decouverte-institutions/Union-europeenne/fonctionnement/france-ue/qu-est-ce-que-principe-subsidiarite.html. Au nom de ce principe, la Commission européenne ne peut dicter de politique de santé aux États membres, elle ne peut que structurer et supporter leurs actions et, parfois, faire des recommandations qui se limitent à des lignes directives qu'ils sont libres d'interpréter et de mettre en œuvre en fonction de leurs propres contraintes. COMYN. Gérard, chef d'unité NTIC pour la santé à la Commission européenne. *Compte rendu de la table ronde du 5 décembre 2008.* P. 21. http://www.eu2008.fr/webdav/site/PFUE/shared/import/1205_Interoperabilite_medicale/Interoperabilite_medicale_compte_rendu_(FR).pdf . Consulté le 21 mars 2011.

[547] Table ronde tenue au Conseil national de l'ordre des médecins dans le cadre de la présidence française de l'Union européenne le 5 décembre 2008. *Compte rendu de la réunion*. 51 p: http://www.eu2008.fr/webdav/site/PFUE/shared/import/1205_Interoperabilite_medicale/Interoperabilite_medicale_compte_rendu_(FR).pdf. Consulté le 21 mars 2011.

[548] Droit médical.com. Interopérabilité des systèmes informatiques de santé européens. 10 décembre 2008. http://droit-medical.com/actualites/4-evolution/322-interoperabilite-systemes-informatiques-sante-europeens#ixzz1OaO7KMqX . Consulté le 21 mars 2011

[549] Idem

pays frontaliers. L'interopérabilité dans le domaine du partage des données médicales place le patient, et a fortiori le dossier médical, au cœur du débat : cette démarche met en lumière des approches et des ontologies variées, parfois complémentaires, parfois divergentes[550]. »

La table ronde a permis de mettre en lumière certains préoccupations et projets concernant l'interopérabilité des systèmes de santé. Au titre des préoccupations, M. COMYN a attiré l'attention de l'auditoire sur un détail important, à savoir, la formation des médecins aux nouvelles technologies. Selon, lui, le contexte dans lequel ils travaillent rend difficile leur accommodation avec les ordinateurs ; c'est pourquoi il a incité les agences régionales à y veiller[551]. En ce qui concerne le partage d'informations entre médecin de pays différents, s'il existe une convention entre l'État du médecin et celui où est stocké le dossier médical du patient, le médecin pourra être autorisé à consulter à distance les informations relatives à la santé du patient. Pour cela, il est « *indispensable que soit mis en place un système de communication par réseau sécurisé qui permette à tout médecin de se connecter sur son serveur national et de laisser ce serveur faire le travail d'interopérabilité par rapport au pays voisin pour aller chercher les informations sur le patient qu'il doit soigner*[552] ». Mais, cette solution est entravée par un préalable qu'il faut absolument construire : pour qu'un médecin puisse consulter en ligne un dossier médical, il faut que celui-ci soit accessible. Or, en France et dans la plupart des pays de l'Union, le chantier des dossiers médicaux informatisés n'est pas encore achevé. Dès lors, si au sein d'un même pays, un médecin ne peut pas consulter électroniquement le dossier d'un patient, comment cela serait-il possible hors des frontières. Jean-Jacques FRASLIN propose que les États membres bâtissent d'abord, en leur sein des systèmes nationaux d'information efficients[553].

---

[550] Droit médical.com. *Interopérabilité des systèmes informatiques de santé européens*. 10 décembre 2008. http://droit-medical.com/actualites/4-evolution/322-interoperabilite-systemes-informatiques-sante-europeens#ixzz1OaO7KMqX. Consulté le 15 février 2009.

[551] Compte rendu de la table ronde. P. 50. http://www.eu2008.fr/webdav/site/PFUE/shared/import/ 1205_ Interoperabilite_medicale/Interoperabilite_medicale_compte_rendu_(FR).pdf. Consulté le 21 mars 2011.

[552] Idem

[553] FRASLIN Jean-Jacques. *Interopérabilité médicale : La France aux abonnés absents.* 13 janvier 2009. http://www.i-med.fr/spip.php?article280. Consulté le 17 octobre 2011

Une recommandation[554] relative à l'interopérabilité transfrontalière a été adoptée en 2008. Son objectif est de permettre aux médecins des États membres d'avoir accès aux informations essentielles de leurs patients quel que soit l'État où les données de ceux-ci sont stockées. La recommandation indique « *qu'elle a pour but de contribuer à la mise en place de l'interopérabilité totale dans le domaine de la santé en ligne en Europe d'ici à la fin de 2015*[555]. » Dans la mise en application de ce texte, un certain nombre d'États membres[556] participent à un projet cofinancé par l'Union européenne dénommé epSOS (Smart Open Service for European Patients)[557], lancé en juillet 2008. Ce projet s'intéresse non seulement aux barrières techniques mais aussi aux frontières politiques et administratives de l'interopérabilité. Il est destiné à garantir la compatibilité des informations médicales quelles que soient les différences linguistiques ou technologiques sans qu'il soit indispensable de créer un système de santé européen commun. L'interopérabilité va permettre de favoriser la mobilité des patients en Europe ; de garantir la sécurité de leur soin ; d'accroître l'efficacité et la rentabilité des soins transfrontaliers et de fournir un service médical sûr et sécurisé dans chaque pays et à travers l'Europe.

Le réseau Calliope (Call for InterOperability in Europe) en est un complément. Il a pour principal objectif d'engendrer de bonnes pratiques qui conduisent, à terme, à une

---

[554]Recommandation 2008/594/CE de la Commission du 2 juillet 2008 *sur l'interopérabilité transfrontalière des systèmes des dossiers informatisés de santé*. Notifié sous le n° C(2008) 3282. JOUE du 18 juillet 2008. Pp. L 190/37- L 190/43. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:190:0037:0043:FR:PDF. Consulté le 22 mai 2014.

[555] Recommandation 2008/594/CE de la Commission du 2 juillet 2008 *sur l'interopérabilité transfrontalière des systèmes des dossiers informatisés de santé* (9) P. L 190/ 38 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:190:0037:0043:FR:PDF. Consulté le 22 mai 2014.

[556] 12 États dont : Allemagne, Autriche, Danemark, Espagne, France, Grèce, Italie, Pays-Bas, République Tchèque, Royaume Union, Slovaquie, Suède,

[557] Pour plus d'information sur ce projet, voir le site internet qui lui est dédié : http://www.epsos.eu/france/le-projet-epsos.html. « Le projet epSOS ne vise pas à fournir uniquement un ensemble de recommandations, de spécifications fonctionnelles et techniques, de modèles d'organisation, d'outils techniques visant à améliorer l'*interopérabilité* entre les pays**.** Le projet epSOS vise aussi, de manière très concrète, à conduire une opération pilote dans plusieurs régions européennes.
De janvier 2011 à décembre 2011, dans plusieurs pays européens, des sites pilotes epSOS vont permettre de tester l'échange de données de santé via les services *Patient Summary* et e-Prescription / e-Dispensation. Pour la première fois, les patients européens auront la chance de bénéficier de ces nouveaux services de *e-Santé*.
Les pays participant à l'opération pilote ont sélectionné les sites pilotes de manière à optimiser les cas d'utilisation. Ces sites sont situés dans des grandes villes, dans des régions touristiques ou proches des frontières. Six scénarios (envoi ou réception du *Patient Summary*, de la e-Prescription ou de la e-Dispensation) ont été retenus et doivent être testés pendant l'opération pilote, chaque site pilote implémentant l'un ou l'autre de ces scénarios. » http://www.epsos.eu/france/loperation-pilote-france.html

interopérabilité transfrontalière efficace et standardisée. C'est *un réseau européen de coordination, d'échange d'expériences et de savoir-faire pour la mise en œuvre de services et d'infrastructures interopérables dans le domaine de la e-santé. Par cette plate-forme, les organismes chargés de mettre en place les programmes de e-santé dans l'Union européenne collaborent entre eux. Le projet comprend, à ce jour, les pouvoirs publics de plus de 20 pays et 13 organisations européennes représentant les médecins, les pharmaciens d'officine, les patients, les industriels de la e-santé et les assureurs santé*[558].

Une autre initiative allant dans le même sens est celle de l'ehealth-interop[559]. C'est un programme de travail de normalisation visant, à terme, à définir et à recommander les normes à adopter dans l'Union européenne pour des systèmes d'information interopérables dans le domaine de la e-santé. Il a été lancé en Février 2008 à l'initiative de la Commission européenne qui en a confié la réalisation à 3 organisations européennes de normalisation : le CEN[560], le CENELEC[561] et l'ETSI[562] en mars 2007. Ces organisations devront fournir un ensemble cohérent de standards d'interopérabilité globale pour les systèmes d'information et de communication en e-santé. L'aboutissement du projet ehealth-interop est prévu pour la fin 2012[563].

A l'occasion du Conseil de l'Union européenne du 1er décembre 2009, les ministres de la santé ont unanimement admis l'importance d'une e-santé à l'échelle européenne ; c'est pourquoi, les ministres et secrétaires d'États des 27 pays de l'Union européenne ont adopté la

---

[558] ASIP santé. *Calliope : mettre l'interopérabilité en partage*. http://esante.gouv.fr/dossiers/calliope-mettre-linteroperabilite-en-partage. Consulté le 21 mai 2014.
Le projet a débuté le 1er juin 2008 et devrait s'achever à la fin de l'année 2010. Financé par la direction générale société de l'information et médias (DG Infso) à hauteur de 250 000 euros (sur les 500 000 euros du projet), la gouvernance de Calliope a été confiée à un organisme grec, l'ICCS (*Institute of Communication and Computer Systems*).

[559] Site internet de ehealth-interop. http://www.ehealth-interop.nen.nl/

[560] Comité européen de normalisation.

[561] Comité européen de normalisation en électronique et en électrotechnique.

[562] Institut européen des normes de télécommunication.

[563] ASIP Santé. *Ehealth-interop veut normaliser la e-santé européenne*. 13 juillet 2010. Pour plus de développement sur le sujet. http://esante.gouv.fr/dossiers/ehealth-interop-veut-normaliser-la-e-sante-europeenne.
L'Union européenne soutient plusieurs autres projets de e-santé comme le Netcards et le Stork qui visent à permettre de garantir la continuité des soins dans toute l'Europe. Voir à ce sujet, *L'Union européenne investit dans la e-santé de ses États membres.* ASIP Santé. 21 juin 2010. http://esante.gouv.fr/dossiers/l-Union-europeenne-sinvestit-dans-la-e-sante-de-ses-États-membres#comments. Consulté le 15 décembre 2012.

déclaration : « European co-operation on ehealth[564] ». Celle-ci a pour but d'organiser le développement de la e-santé en Europe fondé sur 5 points[565] essentiels dont « le travail sur l'interopérabilité et la coopération entre les acteurs ». Dans ce cadre, l'initiative de collaboration a été concrétisée par l'Asip santé et la FIEEC. Conformément à sa mission de promotion et de défense des industries électriques, électroniques et de communication pour développer de façon pérenne leur rôle central dans l'économie, la FIEEC[566] collabore avec l'Asip santé pour promouvoir un développement cohérent des technologies de l'information et de la communication dans les secteurs de la santé. La FIEEC avait encouragé en 2008, un approfondissement des conditions d'industrialisation de la télésanté en France. L'analyse, inspiré d'un constat établi à l'occasion du rapport publié en juin 2008 relatif à une stratégie industrielle pour les marchés du futur, fixait 3 conditions : l'établissement d'un cadre juridique réglementaire et approprié ; le renforcement de l'interopérabilité des systèmes ; l'évolution des pratiques et des mentalités. L'Asip santé et la FIEEC ont décidé de mener une étude[567] télémédecine et télésanté réalisée à partir de l'analyse des dix expériences européennes réussies, dans le prolongement du rapport du député Pierre LABORDES : « *la télésanté : un nouvel atout au service de notre bien-être* », remis en décembre 2009 à Mme Roselyne BACHELOT, alors ministre de la santé et des sports. Cette étude a cherché à capitaliser sur les meilleures pratiques de déploiement, en vue d'une industrialisation de la télémédecine et de la télésanté en France.

---

[564] La déclaration en version anglaise (« *final Conference* Declaration ») est disponible à l'adresse suivante : http://esante.gouv.fr/sites/default/files/eHealthConferenceDeclarationFulltext_0.pdf. Consulté le 15 décembre 2012.

[565] Les 4 autres points sont :

- L'engagement politique et stratégique
- La mise en place de l'espace de confiance
- L'encadrement réglementaire
- La protection des données médicales à caractère personnel

http://esante.gouv.fr/dossiers/l-Union-europeenne-sinvestit-dans-la-e-sante-de-ses-États-membres. Consulté le 15 décembre 2012

[566] La FIEEC est une fédération industrielle représentant les entreprises des industries électriques, électroniques et de communication (les technologies de l'énergie et du numérique) auprès des instances nationales et européennes.

[567] Asip santé et FIEEC. *Étude sur la télésanté et télémédecine en Europe*. Mars 2011. www.esante.gouv.fr.

Section 2 : La télésanté

« *Dans cinq ans, la télétransmission sera devenue un réflexe naturel*[568] » écrivait M. WORMS, alors, Président du Conseil supérieur des systèmes d'information de santé, en 2000. Aujourd'hui, en France, cette prévision se réalise avec l'émergence de la télésanté. A partir de la «télétransmission», M. WORMS annonçait, consciemment ou non, l'ère nouvelle de la télésanté. En effet, selon le dictionnaire Robert[569], la télétransmission est le fait de « *transmettre des informations à distance par le réseau télématique (Internet)* ». Les médecins et les pharmaciens par exemple télétransmettent les feuilles de soins des patients à la Sécurité sociale. C'est donc un terme au champ large dans lequel pourrait s'insérer toute transmission d'informations, y compris médicales, comme celles auxquelles M. WORMS faisait allusion.

Comment définit-on la télésanté et quel est son statut juridique ?

Paragraphe 1 : La notion de télésanté

La télésanté offre de nombreux atouts dont l'amélioration de la prise en charge médicale des patients, l'assurance d'une meilleure continuité des soins, la diminution des dépenses[570], le développement de l'activité économique et la diminution des déplacements. Autant d'avantage qui font de la télésanté un enjeu majeur, mais elle n'a pas été définie par le droit positif alors même qu'il dispose d'un vaste champ de déploiements possibles. La télésanté n'a pas de définition légale en France ; cela est parfois source de confusion avec des termes voisins.

[568] WORMS, Gérard. Le quotidien du médecin. N° 6629 du 24 janvier 2000. p. 8 et10.

[569] Le nouveau petit Robert de la langue française 2010. Paris : le Robert, Dalloz 2009. P. 2522.

[570] Selon l'étude prospective de PWC « *Socio-économic impact of m-health* », publié en septembre 2013, le déploiement de la technologie mobile dans le domaine de la santé permettrait d'économiser 99 milliards d'euros en Europe d'ici 2017. Les économies réalisées faciliteraient l'accès aux soins de 24,5 millions de patients supplémentaires, améliorant l'état de santé des citoyens. Par ailleurs, le PIB de l'Union européenne pourrait augmenter de 93 milliards d'euros. Asip santé. *La m-health permettrait d'économiser 99 milliards d'euros en Europe en 2017*. [en ligne]. 3 octobre 2013. Disponible sur: http://esante.gouv.fr/actus/services/la-m-health-permettrait-d-economiser-99-milliards-d-euros-en-europe-en-2017. Consulté le 17 mai 2014.

A. La définition de la télésanté

La télésanté n'a pas de définition légale en France. Par ailleurs, les différentes propositions émanant des acteurs nationaux et internationaux impliqués dans sa mise en œuvre, créent une confusion entre cette notion et d'autres qui lui sont proches.

1. L'absence de définition légale

A défaut de définition légale française, la référence en la matière est celle donnée par l'OMS en 1997. E-health pour les anglo-saxons, la « télématique de santé », c'est l'ensemble des « *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*[571] ». Le Directeur général adjoint de l'OMS en donne une définition plus synthétisée en considérant, par rapport à la télémédecine, que la télésanté est « *l'intégration des systèmes de télécommunication dans la pratique de la protection et de promotion de la santé*[572] ». Il explique qu'ainsi, *« La télésanté est donc plus en relation avec les activités internationales de l'OMS dans le domaine de la santé publique*[573]*. Elle porte, en effet, sur l'éducation pour la santé, sur la santé, sur l'épidémiologie*[574] *alors que la télémédecine est plus orientée vers l'aspect clinique. »*

---

[571] Cette définition a été proposée par le groupe spécialisé sur la télématique de santé de l'organisation mondiale de la santé (OMS) en décembre 1997 pour la préparation du rapport sur la télématique dans le cadre de la politique de santé pour tous au XXIe siècle. Rapport de la Consultation internationale de l'OMS du 11 au 17 décembre 1997. Genève. Publication WHO/DGO/98.1 1998. Document EB 101/INF. DOC/9.

[572] Déclaration faite par le Docteur Fernando ANTEZANA en décembre 1998 à Genève. http://www.antel.fr/doc/Rapport_final_Telemedecine.pdf. Consulté le 27 février 2011.

[573] Santé publique : « *connaissances et techniques propres à prévenir les maladies, à préserver la santé, à améliorer la vitalité et la longévité des individus par une action collective (mesures d'hygiène et de salubrité, dépistage et traitement préventif des maladies, mesures sociales propres à assurer le niveau de vie nécessaire) »*. Dictionnaire le Petit Robert édition 2009.

[574] « *Etude des rapports existant entre les maladies ou tout autre phénomène biologique, et divers facteurs (mode de vie, milieu ambiant ou social, particularités individuelles) susceptibles d'exercer une influence sur leur fréquence, leur distribution, leur évolution »*. Dictionnaire le Petit Robert. Édition de 2009.

La loi 83 du Québec propose une acception beaucoup plus étoffée. On entend par « *service de télésanté une activité, un service ou un système lié à la santé ou aux services sociaux, pratiqué à distance au moyen des technologies de l'information et des communications, à des fins éducatives, de diagnostic ou de traitement, de recherche, de gestion clinique ou de formation. Toutefois, cette expression ne comprend pas les consultations par téléphone*[575] *»*. Il apparaît donc que la télésanté est une activité basée sur une relation tripartite entre un site émetteur permettant de saisir, de traiter et de stocker un contenu (sons, images, données alphanumériques), un moyen de transférer ce contenu (les TIC) et un site récepteur, un mécanisme pour recevoir et afficher le contenu. Ce qui ouvre sur un large éventail de pratiques médicales et socio-médicales à distance au moyen des TIC. Mais la dernière phrase (« *cette expression ne comprend pas les consultations par téléphone »)* suscite des doutes quant à la considération de la téléconsultation comme activité de télésanté si l'on se base sur cette définition.

Le document de travail portant sur le plan opérationnel pour la télésanté au Québec de février 2006[576], admet que les pratiques de télémédecine et de téléconsultation entrent dans le cadre de la télésanté[577]. Pourtant, sachant que la téléconsultation est un acte médical pratiqué à distance au moyen de systèmes de télécommunication comme la visioconférence, les messageries, les sites web et même la téléphonie, la définition de la loi 83 du Québec l'en exclut implicitement. On se demande alors dans quelle catégorie de pratique le législateur québécois classe la consultation par téléphone au Québec ou encore, si cela y est légal ?

---

[575] L'article 56 – 108.1, alinéa 3 du projet de loi n° 83 du Québec modifiant *la loi sur les services de santé et les services sociaux et d'autres dispositions législatives*. (2005, chapitre 32). Adopté le 25 novembre 2005 et adopté le 30 novembre 2005. http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2005C32F.PDF.
Actuel article 108.1 de la *loi sur les services de santé et les services sociaux et d'autres dispositions législatives*. Chapitre S-4.2. http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/S_4_2/S4_2.html Consulté le 21 avril 2014.

[576] PICOT, Jocelyne. *Plan opérationnel pour la télésanté au Québec*. Document de travail préparé par la Direction générale des services de santé et médecine universitaire du Ministère de la santé et des services sociaux et présenté à inforoute santé du Canada. 2 février 2006. Volume 1. P. 7-8. http://www.medicine.mcgill.ca/ruis/docs/telesante/plan_op_telesante.pdf. Consulté le 22 mai 2014.

[577] « *Les pratiques suivantes sont donc à considérer dans cette définition : La télémédecine et la téléconsultation, soit entre spécialiste et omnipraticien ou infirmière, soit entre deux professionnels de la santé ou directement entre patient et professionnel de la santé.* » PICOT, Jocelyne. *Plan opérationnel pour la télésanté au Québec*. 2 février 2006. Volume1. P. 7-8. http://www.medicine.mcgill.ca/ruis/docs/telesante/plan_op_telesante.pdf. Consulté le 22 mai 2014.

En réalité, selon l'esprit de cette loi, si la consultation par téléphone est exclue du champ de la télésanté, celle qui se fait par visioconférence est bien légale. Des lignes directives[578] relatives aux activités de télésanté ont été élaborées sous l'impulsion du ministère de la santé et des services sociaux (MSSS) dans le cadre du soutien et au développement des pratiques professionnelles multidisciplinaire au Québec, notamment la télésanté. En application de la loi sur les services de santé et des services sociaux, ces lignes directives servent de guide de conduite dans la réalisation des projets de télésanté. Elles reconnaissent comme comptant au nombre des activités pour lesquelles s'applique la télésanté, la téléconsultation avec le patient et la téléconsultation sans patient. Elles en précisent les définitions[579].

Au plan européen, une étude menée sur la télésanté et la télémédecine en Europe en mars 2011 définit la télésanté comme l' *« utilisation dans le secteur de la santé de l'ensemble des technologies numériques de communication permettant d'offrir de nouveaux services aux patients, d'améliorer la circulation d'informations entre professionnels (dématérialisation et partage de documents cliniques) ou de réaliser certains actes médicaux à distance dans le cadre de la télémédecine[580]. »*

En novembre 2008, un rapport élaboré par des conseillers généraux des établissements de santé de France présentait la télésanté comme englobant « *toutes les applications, sites, portails, que l'on trouve sur Internet et qui sont, tout ou partie, liés à la santé. Ces sites, bien connus des patients et des professionnels de santé, proposent des prestations nombreuses : conseils, recommandations avant voyage, articles, forums, bulletins d'information voire, pour*

[578] MSSS. *Lignes directives relatives aux activités de télésanté RUIS UL.* Version-3.1. Août 2013. 23p. http://www.csssalphonsedesjardins.ca/fileadmin/CSSSAD/PDF/Centres_d_expertises_et_services_r%C3%A9gionaux/Lignes_directrices_RUIS-UL_V_3_1_finale.pdf. Consulté le 21 avril 2014.

[579] La téléconsultation avec le patient est la consultation en présence de l'usager effectué par un professionnel de la santé située au centre dispensateur par visioconférence. Cette activité clinique permet l'évaluation, la réévaluation de l'état physique ou mental de l'usager pour : une confirmation diagnostique, ou une seconde opinion, pour l'élaboration, ou la révision d'un plan d'intervention, ou toute autre activité clinique. Quant à la téléconsultation sans patient, elle consiste en une consultation en l'absence de l'usager par visioconférence concernant son état de santé. Cette activité permet de tenir une discussion de cas pour confirmer un diagnostic, obtenir une seconde opinion, élaborer ou réviser un plan d'intervention ou toute autre activité clinique. MSSS. *Lignes directives relatives aux activités de télésanté RUIS UL.* Version-3.1. Août 2013. p.9. http://www.csssalphonsedesjardins.ca/fileadmin/CSSSAD/PDF/Centres_d_expertises_et_services_r%C3%A9gionaux/Lignes_directrices_RUIS-UL_V_3_1_finale.pdf. Consulté le 21 avril 2014.

[580] ASIP Santé et FIEEC. Études sur la télésanté et télémédecine en Europe. Mars 2011. Cette étude a été pilotée par l'ASIP santé et la fédération des industries électriques et électroniques de la communication (FIEEC). Ils en ont présenté les principaux enseignements au cours d'une conférence de presse le 29 mars 2011. http://esante.gouv.fr/sites/default/files/Etude_europeenne_Telesante_FIEEC_ASIPSante.pdf. Consulté le 21 avril 2014

certains d'entre eux, des dossiers médicaux en ligne ».[581] Cette conception de la télésanté la limitait aux seules informations médicales que l'on recueille sur Internet en omettant ses aspects cliniques. La question se pose alors de savoir si l'on peut concevoir une télésanté sans actes cliniques ?

La réponse semble négative pour l'association médicale mondiale qui en a une autre opinion : « *la télésanté consiste à utiliser les technologies de l'information et de la communication pour délivrer des soins de santé et des informations sur de grandes et petites distances*[582] ». L'association retient un contenu plus étendu pour la télésanté qui « *fait entrer en jeu la gamme complète d'actions contribuant à la bonne santé du patient et du public : la prévention, la promotion, le diagnostic et le traitement, tous des domaines où les médecins jouent un rôle important.*[583]».

Le rapport LASBORDES[584] d'octobre 2009 rejoint davantage les définitions proposées par l'OMS et l'AMM[585] en indiquant que *« la télésanté est l'utilisation des outils de production, de transmission, de gestion et de partage d'informations numérisées au bénéfice des pratiques tant médicales que médico-sociales*[586]. » C'est un système dont l'enjeu s'étend au delà du cadre de la santé. Madame ALAJOUANINE, Présidente du haut Conseil de la télésanté ou Commission GALIEN affirmait, en effet que : *« la télésanté est certes du domaine de la santé mais tout aussi bien du social, de l'économie, de l'industrie, de l'intérieur, de la défense, du commerce extérieur, ou encore de l'aménagement du territoire. Par exemple : c'est bien le rôle de l'État en tant que premier aménageur du territoire et*

[581]SIMON, Pierre et ACKER, Dominique. Rapport. *La place de la télémédecine dans l'organisation des soins.* Novembre 2008. P. 8/160. Disponible sur: http://www.sante.gouv.fr/IMG/pdf/Rapport_final_ Telemedecine.pdf. Consulté le 28 mai 2014.

[582]Association médicale mondiale. *Prise de position de l'AMM sur les principes directeurs pour l'utilisation de la télésanté dans les soins médicaux*. P. 1. http://www.wma.net/fr/30publications/10policies/t5/index.html. Consulté le 28 mai 2014.

[583] Idem

[584] Rapport LASBORDES. La télésanté: *un nouvel atout au service de notre bien-être*. 15 octobre 2009. http://lesrapports.ladocumentationfrancaise.fr/BRP/094000539/0000.pdf. Consulté le 27 mai 2014.

[585] Association médicale mondiale.

[586] Rapport LASBORDES. La télésanté : un nouvel atout au service de notre bien-être. 15 octobre 2009. P 37/247. http://lesrapports.ladocumentationfrancaise.fr/BRP/094000539/0000.pdf. Consulté le 28 mai 2014.

garant de la sécurité publique, d'assurer un meilleur équilibre territorial pour l'accès aux soins : la Télésanté à travers l'aide au diagnostic à distance va y contribuer largement[587]*. »*

Finalement, aussi diverses soient-elles l'essentiel des définitions de la télésanté retient l'intervention des TIC tant dans les aspects cliniques que dans les aspects médico-sociaux du domaine de la santé. Mais, une confusion persiste dans le vocabulaire employé pour décrire l'utilisation des TIC dans le domaine de la santé.

2. La confusion entre la télésanté, la e-santé et la cybersanté

L'utilisation des TIC dans le domaine de la santé est présentée sous différentes appellations qui ne laissent pas suffisamment transparaître leurs différences. Cela crée un imbroglio entre les notions de télésanté, cybersanté et e-santé en l'absence de définitions homologuées.

La première difficulté réside dans leur traduction du terme « télésanté » de l'anglais au français. Pour certains, e-health, en anglais se traduit télésanté (définition officielle de l'OMS), en français ; pour d'autres, e-health se traduit e-santé en français. C'est le cas de l'Union européenne qui, pour débattre du développement de la e-santé en Europe a organisé « *une conférence e-health* » à Barcelone en mars 2010 et a adopté une déclaration *« European co-operation on eHealth »*[588]. En Suisse, se fondant sur la traduction officielle de l'Union européenne, « cybersanté » est considéré comme l'équivalent français de «e-health »[589]. Dès lors, rien qu'en Europe, e-health peut s'entendre e-santé ou cybersanté ou encore télésanté[590].

---

[587] La revue télésanté. *L'amélioration de l'accès aux soins passe par le déploiement de la télémédecine*. Interview accordée par la Présidente Ghislaine ALAJOUNINE. http://www.jiqhs.fr/wp-content/uploads/2010/12/Résumé-télémédecine_Ghislaine-Alajouanine.docx. Consulté le 29 avril 2014.

[588] http://esante.gouv.fr/dossiers/l-Union-europeenne-sinvestit-dans-la-e-sante-de-ses-États-membres

[589] Office fédéral de la santé publique. Cybersanté (e-health) questions- réponses. 16 octobre 2007. P.4. www.e-health-suisse.ch/faq/00052/index.html?lang=fr&download. Consulté le 16 septembre 2011.

[590] Par le représentant de la CPME (Comité permanant des médecins européens) dans le rapport sur la place de la télémédecine dans l'organisation des soins. Novembre 2008. p. 12/160 « *Il rappelle que la télémédecine ne doit pas être confondue avec la télésanté (eHealth), la télématique, les NTIC, les services de santé sur Internet (Healthnets)* ». http://www.antel.fr/doc/Rapport_final_Telemedecine.pdf. Consulté le 16 septembre 2011.

En dehors des difficultés de traduction, il faut noter que les définitions données par les mêmes acteurs ne permettent pas non plus de différencier les contenus desdites notions.

Le rapport du ministère de la santé français sur la place de la télémédecine dans l'organisation des soins établi par Pierre SIMON et Dominique ACKER emploie e-santé et télésanté comme des synonymes : *«Les technologies du numérique appliquées à la santé couvrent le champ de la e-santé ou télésanté et offrent des possibilités nouvelles d'accès aux soins, des champs nouveaux dans l'organisation des soins, les pratiques professionnelles et la formation des professionnels de santé*[591]*. »*

Autant d'exemples justifiant de la multitude de définitions, de la difficulté de traduction et donc de la confusion qui règne quant à la perception de la notion de « télésanté ». Cependant, force est de constater que des États comme le Canada utilisent des termes qui ont le mérite de permettre une certaine clarté. En effet, « télésanté » se traduit « telehealth» en anglais[592] et non e-health; celui-ci étant réservé à e-santé. Pour clarifier davantage la situation, il serait judicieux d'organiser une rencontre internationale[593] pour préciser la définition, le champ de la télésanté et les nuances entre toutes les notions clés employées pour désigner l'utilisation des TIC dans le secteur de la santé. Une première piste qui pourrait être explorée dans ce cadre serait de voir comme Hachimi Sanni YAYA, qu'il y a une évolution conceptuelle entre les 3 termes. La cybermédecine (cybersanté, pour notre étude) serait le résultat de l'évolution de la télésanté en passant par la e-santé[594]. La e-santé est définie par EYSENBACH comme *« un champ émergeant à l'intersection de l'informatique*

[591] SIMON, Pierre et ACKER, Dominique. Rapport La place de la télémédecine dans l'organisation des soins. Novembre 2008. P. 8/160. http://www.antel.fr/doc/Rapport_final_Telemedecine.pdf. Consulté le 28 mai 2014.

[592] Par exemple, la version anglaise que propose le site dédié à la télésanté au Canada (https://www.infoway-inforoute.ca/about-infoway/approach/investment-programs/telehealth) traduit « télésanté » par « telehealth » (https://www.infoway-inforoute.ca/lang-en/about-infoway/approach/investment-programs/telehealth). Consulté le 28 mai 2014.

[593] Une telle initiative a déjà été prise par le secrétariat du Conseil exécutif de l'OMS au sujet de la normalisation de la cybersanté en 2006. OMS. *Rapport du secrétariat. Cybersanté : terminologie normalisée*. 25 mai 2006. Document EB118/8. p.3 *« en collaboration avec des organisations internationales de normalisation (l'Organisation internationale de Normalisation, le Comité européen de Normalisation ou d'autres organismes, par exemple), l'OMS jouerait un rôle actif dans la fixation de normes et de règles en matière d'information sanitaire, applicables à toutes les terminologies internationales dans le domaine de la santé, telles que l'exhaustivité, la pertinence, le multilinguisme, l'utilité, la fiabilité, la validité, l'interopérabilité et l'amélioration constante de la qualité, ce qui améliorerait l'apport du secteur de la santé à la création de terminologies normalisées »* http://apps.who.int/gb/ebwha/pdf_files/EB118/B118_8-fr.pdf . Consulté le 22 mai 2014.

[594]YAYA, Hachemi Sanni, RAFFELINI, Chiara. *Des souris et des médecins De la télémédecine à la cybermédecine*. Avril 2008. P. 45 – 52.

médicale, la santé publique et l'économie, se référant aux services de santé et aux informations produites ou échangées par le biais d'internet et les technologies proches. Dans un sens plus large, le terme caractérise non seulement un développement technique mais également un état d'esprit, une manière de penser, une attitude et une sorte d'obligation pour les personnes travaillant en réseau d'améliorer les soins de santé localement, au plan régional ou mondialement en utilisant les technologies de l'information et de la communication[595] ». Pour lui, la e-santé («*santé électronique*») renferme le fait de dépasser le simple cadre des soins médicaux ou paramédicaux pour s'intéresser à l'éducation, à la formation, à la prévention, à l'administration et plus généralement à la santé publique. Ce concept associe les patients au processus de soins en les rendant plus actifs. Ils s'informent via internet au sujet de leur santé et échangent sur des forums. C'est ce dernier aspect qui marque le niveau d'évolution de la télésanté à la e-santé.

Dans son rapport[596] sur la santé et les nouvelles technologies remis au Conseil économique et social en 2002, madame Jeannette GROS explique que la e-santé recouvre les activités de publication de sites médicaux en ligne à destination des professionnels de la santé tout comme des internautes. La e-santé comprend les services médicaux en ligne, les lettres d'information, les avis ou conseils médicaux d'ordre général prodigués par des médecins, des bases de connaissances médicales, des sites de presse médicale. Elle porte également sur les sites de publicité en ligne, de e-commerce de santé et d'hébergement de données personnelles de santé. En somme, la e-santé ne s'inscrit pas dans une logique personnalisée de diagnostique ou de thérapie alors que la télésanté, même si elle consiste quelques 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 (la téléconsultation, la téléassistance, la télévigilance, etc).

Le passage de la e-santé à la cybersanté reste plus difficile à démontrer car la cybersanté sous-entendant "santé dans le cyberespace"[597], place les services de santé dans un

---

[595] EYSENBACH G. *What is e-health? In* Journal Medical Internet Research. 2001 April–June, 3(2):E20. Traduction de la définition donnée par Gunther Eysenbach lors d'un discours qu'il a tenu à l'UNESCO à Paris en Juin 2001 à la Conférence internationale sur le progrès médical et l'équité dans le domaine de la santé au XXIème siècle.

[596] GROS Jeannette. Rapport. *Santé et nouvelles technologies de l'information et de la communication*. 10 avril 2002. P. II –9 - 12. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000462/0000.pdf. Consulté le 29 avril 2014.

[597] ROGUE, Evelyne. Dictionnaire pratique de la cybersanté. P. 187 : « *cyberespace : par extension, tous les univers reconstitués de toutes pièces en bits numériques. Autrement dit, il s'agit d'univers virtuels qui n'existent*

univers virtuel et donc dans une position qui dépasse les limites temporelles et spatiales quant au partage des informations de santé ; situation qu'offre la e-santé également. Même si Hachimi Sanni YAYA insiste sur la fin de la couverture spatiale et temporelle, l'accès aux informations médicales par le grand public en dehors des professionnels de santé et l'instauration d'une communication synchronique ou asynchrone[598], nous percevons difficilement cette évolution. Les définitions données par l'OMS au sujet de la télésanté et de la cybersanté corroborent cette difficulté. La télésanté est entendue comme l'ensemble des « *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 »* − alors que « *la cybersanté consiste à utiliser, selon des modalités sûres et offrant un bon rapport coût/efficacité, les technologies de l'information et de la communication à l'appui de l'action de santé et dans des domaines connexes, dont les services de soins de santé, la surveillance sanitaire, la littérature sanitaire et l'éducation, le savoir et la recherche en matière de santé*[599] ». Ici, les détails à partir desquels M. YAYA considère que la e-santé est une évolution de la télésanté se retrouvent dans la définition donnée pour la cybersanté. Tout comme dans la définition d'EYSENBACH, l'on retrouve l'aspect économique, les domaines autres que l'aspect clinique de la santé et les possibilités d'ordre temporaire et spatial offrent les technologies de l'information et la communication. Chacune des deux définitions se retrouve finalement être une reformulation de l'autre.

Il existe des difficultés réelles pour appréhender la notion de télésanté. Sa différentiation avec les termes e-santé et cybersanté n'en n'est pas moins complexe. Cette situation trouve des origines dans la multitude d'application que comporte la télésanté.

---

et ne peuvent exister que grâce aux réseaux informatiques mis en communication les uns avec les autres.On doit ce terme à William GIBSON. A l'origine, ce mot a été créé pour désigner un espace existant entre plusieurs personnes ayant la possibilité de communiquer par réseaux interposés. »

[598] YAYA, Hachemi Sanni, RAFFELINI, Chiara. *Des souris et des médecins De la télémédecine à la cybermédecine*. Avril 2008. P. 49 – 51.

[599] Organisation mondiale de la Santé. Cinquante huitième Assemblée mondiale de la santé, neuvième séance plénière de la Commission sur la cybersanté, WHA58.28. 25 mai 2005. http://apps.who.int/gb/ebwha/pdf_files/WHA58/WHA58_28-fr.pdf. Consulté le 2 Septembre 2011.

B. Les applications de télésanté

Les limites de la technologie sont sans cesse repoussées y compris dans le domaine de la santé. La télésanté comporte plusieurs applications dont le dossier médical personnel, la description électronique, la télémédecine, les outils d'aide à la décision, les technologies et les services de santé en ligne, la réalité virtuelle, la robotique, la chirurgie assistée par ordinateur, les systèmes mobiles et portables de suivi médical (défibrillateur cardiaque), les portails des santés en ligne, la vidéoconférence, etc. Mais le rapport LASBORDES a fait une classification qui comporte deux aspects : l'un, médico-social et l'autre, médical (la télémédecine). C'est cette répartition que nous retiendrons dans le cadre de cette étude car elle nous paraît regrouper l'ensemble des exemples cités ci-dessus.

1. Les applications médico-sociales

« Dans le cas du handicap sensoriel, des solutions émergent pour organiser l'environnement de sorte que les personnes puissent se déplacer librement. Pour les déficiences intellectuelles, on a plutôt tendance à clore le débat, en limitant la marge de manœuvre de la personne. On la place dans des institutions fermées, avec des murs d'enceinte à l'intérieur desquelles il dispose d'une autonomie relative. Le système visé permet de dépasser cette contrainte. Grâce à des terminaux de type « BlackBerry », il est possible de suivre les personnes, et de générer des alarmes. Les professionnels sont équipés, et chacun d'eux est localisable. La particularité de ce système, c'est qu'il fournit une géolocalisation de l'aidant. Un exemple illustrera le propos : Une personne atteinte de troubles autistiques, attend son car pour 5 heures. Le car n'arrive pas. La personne déclenche la balise. Elle va se trouver en relation avec son référent. Le référent lit sur son terminal : « Pierre a un problème ». Il regarde où est ce dernier, ce qu'il veut. L'aidant peut alors faire appel à un cadre de niveau supérieur. Les mesures qui s'imposent peuvent être prises[600]*. »*

[600] PICARD, Robert. PILLET, Didier. *Rapport n° 2010/42/CGIET/ SG: Caractérisation du secteur médico-social pour le développement d'offres TIC.* Décembre 2010. http://www.cgiet.org/documents/Rapport_ Caracterisation_du_secteur_medico_social_pour_le_developpement_d_offres_TIC.pdf. Consulté le 15 Octobre 2011.

L'exemple cité par ce rapport présente un cas de télésanté médico-social (la télévigilance) au service du bien-être d'une personne en situation de handicap. Il en existe plusieurs qui veillent à faire écho de la volonté de la société d'assurer une certaine autonomie aux personnes âgées ou aux personnes handicapées, respecter leur volonté de se faire soigner chez elles et prêts de leur famille tout comme le fait de réduire les frais élevés d'hospitalisation, du séjour en maison spécialisée, etc. d'autres solutions permettent d'informer le patient ou de former les professionnels ou tout simplement d'échanger des informations dans le domaine de la santé. Pour le rapport LASBORDES, *« les applications du domaine médico-social*[601] *vues du patient peuvent être :*

- La téléinformation : Capacité à accéder à un portail grand public sur lequel les usagers/patients et les acteurs du monde médico-social pourront accéder à des informations de prévention et de recommandations sanitaires, à des alertes (situations de crise, épidémie), à des conseils et bonnes pratiques, à des annuaires, des guides d'accompagnement leur permettant d'identifier le point d'entrée qui correspond à leur problématique. Ainsi peuvent se créer des réseaux informationnels[602] très développés comportant les proches, l'hôpital, les soins locaux (le pharmacien, le médecin traitant, le psychologue), les pairs (les sites Internet, les associations de santé).
- La télévigilance : alerte, suivi et accueil téléphonique de personnes utilisant notamment les capteurs dynamiques de positionnement, de comportement, de fonctionnement d'organes vitaux ou d'appareils supplétifs et des outils de géolocalisation (par exemple pour les pathologiques de type Alzheimer). Le programme *« plas'o'soins*[603] *»,* premier projet de télésanté financé par l'Agence nationale de la recherche (ANR) permet une meilleure coordination entre les différents acteurs de la santé et les services à domicile. Le système prend en compte le profil du patient et sa géolocalisation, les prescriptions, les interventions,

[601] Ce qui est relatif à la médecine sociale. La médicine sociale est l'ensemble des connaissances portant sur les conséquences médicales des lois et des phénomènes sociaux (législations sociales, médecine du travail, etc.). Dictionnaire le petit Larousse 2010. P. 632

[602] Analyse faite par des experts (Rémi BASTIDE, Marie-Pierre BES, Adrien DEFOSSEZ) sur la problématique de l'isolement du patient en hospitalisation à domicile : une approche par l'analyse sociologique des réseaux les *cahiers de la télé santé 2009, vers l'âge de raison…* p. 53-57.

[603] LE TARNE, Libre. 8 avril 2011. *Plasosoins, pour une meilleure coordination de l'aide à domicile in Actes de la journée des télés santé 2011 du jeudi 31 mars 2011 en France et en francophonie*. P. 38. Le projet qui est en cours d'élaboration a été présenté par Pierre BARDY, Directeur des soins à domicile pour l'UMT. Mis en place en Midi-Pyrénées, il est porté par plusieurs partenaires dont l'école d'ingénieurs et ISIS de Castres, le centre de génie industriel de l'école des mines Albi Carnaux, la société CGX systèm, les centres hospitaliers des Castres et d'Albi, l'UMT 81.

et leurs évolutions. Ce dispositif peut également faire remonter les messages d'alerte du patient vers un service d'urgence, un médecin ou un proche. Ce système permet également de vérifier la cohérence et la traçabilité des interventions et la constitution d'un tableau de bord permettant d'apprécier la qualité du service rendu.

- Le télémonitoring : enregistrement de divers paramètres physiologiques sur un patient et transmission aux professionnels concernés (médecins, sages-femmes, infirmières…) souvent dans le cas de pathologies chroniques : enregistrement de la tension artérielle, surveillance des insuffisances respiratoires chroniques, surveillance des grossesses à risque. Par exemple, une PME fondée en 2004 par Philippe SALAMITOU SRETT offre un service de télémonitoring pour le suivi des patients atteints de BPCO (Broncho- pneumopathie chronique obstruante) traités par oxygénothérapie long terme. Pour ce faire, SRETT a mis au point un petit boîtier qui s'intercale entre la source d'oxygène et le patient. Le boîtier renferme un capteur, un micro-contrôleur, un émetteur qui transmet les données par voie radio et une pile. Il mesure la fréquence respiratoire du patient pendant toute la durée de l'oxygénothérapie. Ces données transmises sans fil vers le centre de données permettront de connaître avec précision la façon dont a été pratiqué le traitement et la durée exacte de son utilisation puis d'effectuer en permanence un suivi de ce patient.
- La télécollaboration : outils d'animation de communautés et de réseaux de santé, plates-formes collaboratives dédiées.
- Le télémajordome : outils et offres de services permettant à distance de commander ou mettre en œuvre des services d'accompagnement (restauration, aides à domicile…) notamment pour les maladies chroniques, les hospitalisations à domicile, les personnes handicapées.
- La téléanimation : accès à une gamme d'outils interactifs (loisirs, messageries multimédia simplifiées, web conférences…) incitant les usagers/patients à conserver un lien social et un minimum d'activité physique et cérébrale (explosion très significative des jeux électroniques) pour séniors ou expérimentation d'activités physiques assistées réalisées par des kinésithérapeutes dans le domaine de la réadaptation).
- La téléformation : services de télécommunication synchrones ou asynchrones ; téléphonie, visioconférence, messageries, forums, serveurs d'images. Ces services de formation à distance, s'adressant à des étudiants ou à des professionnels de santé, permettent l'accès à un savoir-faire ou à des connaissances, quelle que soit leur localisation (base de données médicales sur le web, modules de e-learning, interventions chirurgicales visualisées à

distance par des internes…). Le développement de ces pratiques facilite l'accès aux formations en matière de santé pour des personnes qui vivent à l'extérieur des centres métropolitains. Plusieurs sites proposent ce type de formation en France ; par exemple, IMAIOS[604], Mediformation[605], l'école de santé publique de Nancy[606], etc…

- La téléprescription : elle permet la dématérialisation des prescriptions médicales et offre d'éviter les déplacements inutiles.[607] » Deux situations sont à distinguer : celle d'un médecin qui reçoit, au sein de son cabinet ou dans le cadre de la continuité des soins des appels téléphoniques de ses patients et celle du médecin régulateur dans le cadre de la permanence de soins. Pour le Conseil de l'ordre des médecins, la téléprescription est admise comme un *« conseil téléphonique à un patient connu et identifié dans les suites d'une consultation avec examen physique, dans le but d'évaluer les effets d'un traitement, adapter une posologie ou procéder à un éventuel changement de médicaments. »* Le médecin doit toujours rechercher si le patient a bien compris ce conseil de prescription. Jusqu'en 2004 l'article R. 5194 du code de la santé publique réfutait implicitement la téléprescription en imposant que la prescription de médicaments ou produits soit rédigée après examen du malade. Mais l'article 34 de la loi du 13 août 2004 relative à l'assurance maladie prescrit désormais que : *« une ordonnance comportant des 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. »* La lettre de cette loi n'évoque pas les appels téléphoniques. Elle se limite à la prescription par courriel, or la pratique ne peut se passer des prescriptions téléphoniques. C'est pourquoi il serait préférable de revoir la rédaction de cette réglementation dans le sens d'une prise en compte de la globalité de la question[608]. Le Conseil de l'ordre des médecins tout

[604] http://www.imaios.com/fr: Formation médicale en ligne pour les professionnels.

[605] http://www.mediformation.com/: Mediformation est le spécialiste des formations et préparations aux concours dans le domaine de la santé par e-learning en partenariat avec infirmiers.com.

[606] http://www.sante-pub.u-nancy.fr/elearning/ de l'université Henri Poincaré de Nancy I. Consulté le 8 mai 2014.

[607] Rapport LASBORDES. La télésanté : un nouvel atout au service de notre bien-être. 15 octobre 2009. p. 37. http://lesrapports.ladocumentationfrancaise.fr/BRP/094000539/0000.pdf. Consulté le 8 mai 2014.

[608] En tout état de cause, la prescription effectuée par le médecin devra être confirmée sur un support écrit identifiable, quel que soit sa forme, et le médecin devra s'assurer de sa bonne compréhension. Il pourra s'avérer

comme leurs homologues européens s'opposent à la prescription téléphonique ou par courriel lorsque le patient n'est pas connu et identifié. Ils préconisent que la réponse téléphonique à un patient inconnu et non identifié se limite à une simple information de caractère général suivie le cas échéant, d'une invitation à se rendre au cabinet d'un médecin.

Les applications médico-sociales de télésanté se diversifient et se développent de jour en jour mais la législation française n'a pas encore établi de cadre juridique spécifique à ce domaine contrairement aux applications médicales.

2. Les applications médicales : la télémédecine

Selon une étude[609] Sofres commandée par le Conseil national de l'ordre des médecins, 91% des français estimaient déjà en 2009 que la télémédecine leur sera nécessaire pour assurer leur suivi médical. Pierre TRAINEAU, Directeur général du CATEL[610] a, quant à lui, recensé 280 applications de télémédecine qui fonctionnent déjà en France[611]. La télémédecine est de plus en plus pratiquée et sous diverses formes mais, il persiste encore des zones d'ombre quant à ses aspects juridiques surtout lorsqu'elle est transfrontalière.

---

utile pour le médecin de reporter les conditions dans lesquelles il a effectué cette prescription dans le dossier médical du patient. Cette prescription devrait porter la mention « téléprescription ».
Le Comité Permanent des Médecins Européens a publié des lignes conductrices pour la correspondance par e-mail entre un médecin et un patient. Il fait clairement état de l'utilisation du courrier électronique vis-à-vis des seuls patients connus du praticien et de la nécessité d'une identification des partenaires, notamment par la voie de la signature électronique. La correspondance e-mail fait partie du dossier médical du patient et doit être archivée. Le CPME recommande de vérifier que cette correspondance est couverte par l'assurance en responsabilité civile du praticien et conforme à la réglementation en vigueur. Ces dernières recommandations sont bien évidemment également valables pour les échanges téléphoniques. Conseil national de l'ordre des médecins. Docteur Xavier DEAU. *L'activité médicale auprès du médecin : peut-on admettre la prescription téléphonique et à quelles conditions ?* Rapport adopté à la session du Conseil du 15 Octobre 2004. http://www.Conseil-national.medecin.fr/system/files/activitemedicaletelephonique.pdf?download=1 disponible le 15 novembre 2011.

[609]Sondage TNS Sofres pour le CNOM sur l'informatisation de la santé 03/06/2009 http://www.Conseil-national.medecin.fr/article/sondage-tns-sofres-pour-le-cnom-sur-l-informatisation-de-la-sante-656 Consulté le 29 avril 2014.

[610] Club des acteurs de la télésanté. C'est un club (une association née en 1997) de réflexion sur les questions liées à la santé à distance. Pour plus de renseignements sur le CATEL, http://www.catel.pro/

[611] CATEL. Rapport d'activités 2010-2011. *Aux bons soins de la télémédecine*. p. 37. http://www.catel.pro/documents/Rapport-Activites-2010-2011-CATEL.pdf . Consulté le 29 avril 2014.

a. Les formes de télémédecine

Myriam Le GOFF-PRONOST écrivait : *« la pratique de la télémédecine bouscule les fondements mêmes de l'acte médical traditionnel et oblige à ouvrir de nouvelles réflexions théoriques pour tenir compte de ces changements. Avec la télémédecine, l'acte médical ne s'exécute plus uniquement dans le cadre d'un colloque singulier « médecin/patients », mais il fait intervenir des tiers médecins qui ne sont pas forcément en contact direct avec le patient. Et pourtant, ces tiers sont appelés à participer à la décision diagnostique et thérapeutique. (...) La mise en place des projets de télémédecine va se traduire principalement par le passage d'une relation d'agence traditionnelle où le patient est le principal et le médecin, l'agent, vers une relation d'agence commune qui implique un patient et plusieurs médecins, une relation plus collective et coordonnée, fondée sur le partage de l'information et de l'expertise »*[612]. Les experts nous assurent qu'avec la télémédecine on ne va pas assister à terme, à la disparition de la consultation avec les médecins en chair et en os, à la déshumanisation des soins rien qu'en se penchant de plus près sur ce qu'est la télémédecine. *Le terme « télémédecine » signifie littéralement « médecine à distance » et a été inventé dans les années 70. Autour du concept initial de télémédecine sont ensuite apparus des termes tels que « télésanté » et « télésoins*[613] *».*

L'article 78 de la loi "hôpital, patients, santé territoires" définit « la télémédecine » comme constituant *« une forme de pratique médicale artiste à distance utilisant les technologies de l'information et la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. Elle permet d'établir le 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*

[612] LE GOFF-PRONOST, Myriam. *TIC, télémédecine et accès aux services : une approche économique***.** Thèse de doctorat. : Sciences économiques: UBO, Institut Télécom-Télécom Bretagne : 2003, p. 276-277.

[613] ONU en partenariat avec l'IUT (Union internationale des télécommunications). *Les télécommunications et la santé in* les télécommunications en action, chapitre 2. http://www.regency.org/t_in_act/pdf/french/health.pdf . Consulté le 29 avril 2014.
Les télésoins sont une sphère d'activité nouvelle associant délivrance de soins à distance et soutien communautaire.

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[614]*.»*

Il arrive que télémédecine et télésanté soient utilisées indifféremment comme si ces deux termes étaient synonymes. Mais il faut noter avec l'ex directeur général de l'OMS[615], que l'appellation « télémédecine » est réservée aux seules actions cliniques et curatives de la médecine utilisant les systèmes de télécommunications[616]. Le Conseil national de l'ordre des

[614] 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 textes n°1. NOR : SASX0822640L.

[615] L'actuel Directeur général de l'OMS se nomme Margaret CHAN. Elle a été élue à ce poste par l'Assemblée mondiale de la santé le 9 novembre 2006.

[616] Dr ANTEZANA Fernando, en décembre 1998 à Genève. SIMON, Pierre et ACKER, Dominique. Rapport final relatif à *la place de la télémédecine dans l'organisation des soins*. Novembre 2008. P. 8/160.
Ce rapport établit également l'histoire de la télémédecine aux pages 95 – 96/160 : *« L'histoire de la télémédecine débute dans les années 60 aux États-Unis, avec notamment la mise en réseau de programmes de téléconsultation et de télé éducation autour du Nebraska.*
Psychiatric Institute. Deux autres dates symboliques peuvent aussi servir de points de repère à l'émergence de la télémédecine : en 1965 la première visioconférence en chirurgie cardiaque entre les États-Unis et la Suisse, en 1973 le premier congrès international sur la télémédecine au Michigan, lequel est l'occasion du lancement de nombreux projets. Ces projets de télémédecine sont dès lors conçus et mis en œuvre. Mais, globalement, la littérature spécialisée constate un échec de la majorité d'entre eux ou du moins des résultats incertains et pour la plupart non évalués, en raison, notamment, des faibles performances technologiques, des coûts élevés et surtout d'une mauvaise organisation des réseaux mis en place. Il n'y a pas eu beaucoup d'études médico-économiques sur cette première génération de projets et sur la faisabilité technique. Grâce aux liaisons par satellites, la télémédecine va se développer vers la fin des années 1970 par le biais de programmes de recherche instruits par des organisations et/ou institutions spécialisées qui sont elle-même confrontées directement au problème de l'accès aux soins de personnes situées dans des lieux inaccessibles ou difficilement accessibles. Par exemple, la NASA va mettre en place des programmes de télémédecine pour ses astronautes et l'armée américaine des systèmes de téléassistance pour délivrer les premiers soins aux blessés sur les champs de bataille du Vietnam. Les stations d'étude et de recherche en Antarctique, ainsi que les stations d'exploitation pétrolière dans les océans vont réfléchir au développement de technologies appliquées la télémédecine. Enfin, l'US NAVY va développer des programmes d'expérimentation de la télémédecine. La renaissance officielle de la télémédecine date de la fin des années 1980 en Scandinavie, en particulier en Norvège, avec le déclenchement d'un programme intitulé « access to health care services ». Une technologie plus évoluée et des coûts moindres ont permis des succès dans les différents projets de télémédecine mis en place. Ces projets se concentrent sur un certain nombre d'applications de téléconsultation « en temps réel » en radiologie, dermatologie, cardiologie, psychiatrie et oto-rhino-laryngologie. Cinq raisons expliquent le succès de cette troisième génération de la télémédecine: un besoin clinique clair, un partenaire de télécommunication dynamique, une technologie appropriée, un montage financier solide, un projet moins coûteux. Devant le succès des projets norvégiens et la vulgarisation d'Internet, d'autres pays vont développer des programmes de télémédecine, notamment les États-Unis, l'Australie, le Royaume-Uni, la Nouvelle Zélande, Hongkong ou encore la France. Deux grands types de projets voient alors le jour: d'une part, des projets qui concernent certaines activités médicales (exemples de la télé radiologie, de la télé dialyse), d'autre part, des projets dont les débouchés commerciaux favorisent l'implication forte de partenaires financiers dynamiques. Aujourd'hui, les plus grandes expérimentations se tiennent aux États-Unis, même si l'Europe met en œuvre elle aussi de nombreux projets. On assiste depuis 1995 à un important développement de la télémédecine aux États-Unis, celle-ci se voulant porteuse de trois objectifs : permettre un meilleur accès aux services de santé, améliorer la qualité et enfin réduire les coûts de ces services. Deux champs d'expérimentations ont été privilégiés aux États-Unis: dans les prisons, et notamment au Texas, dans le but de réduire les coûts de transport et d'améliorer la sécurité, et dans les zones rurales mal desservies, en particulier dans l'État de Géorgie confronté aux même difficultés que la Norvège pour attirer des médecins dans des secteurs géographiques isolés. » http://www.antel.fr/doc/Rapport_final_Telemedecine.pdf . Consulté le 8 mai 2014.

médecins ajoute que la télémédecine constitue un sous-ensemble spécifique de la télésanté dont la principale particularité tient à ce qu'elle concerne des activités exercées par des professions réglementées[617].

Le décret du 19 octobre 2010[618] relatif à la télémédecine reprenant la distinction faite par le rapport LASBORDES un an plus tôt à défini comme actes de télémédecine les applications suivantes :

- *« la téléconsultation qui a pour objet de permettre à un professionnel médical de donner une consultation à distance à un patient. Un professionnel de santé peut être présent auprès du patient et, le cas échéant, assister le professionnel médical au cours de la téléconsultation* ». Elle s'exerce dans 2 types de situations : le cas le plus répandu concerne la régulation médicale lorsque le patient prend contact, par téléphone, avec un centre où le médecin régulateur établit le diagnostic de gravité et prend la décision d'orientation du patient. Cette pratique fait déjà appel à des protocoles de bonne pratique et peut s'appuyer sur des systèmes experts. Un autre type de téléconsultation consiste en ce qu'un médecin est consulté à distance par le patient près duquel se trouve un autre médecin ou un autre professionnel de santé. Cette pratique est en œuvre en France surtout en gériatrie : « *aidé par le personnel de la maison de retraite où il séjourne, un patient entre en relation, par visioconférence, avec un gériatre qui se trouve dans un service hospitalier. A distance, en questionnant le patient et en observant ses réactions, le spécialiste peut réaliser un bilan mémoire et un bilan nutritionnel, poser un diagnostic et faire une prescription, qu'il envoie à la maison de retraite via une liaison Internet sécurisée*[619] ».
- *« La téléexpertise qui a pour objet de permettre à un professionnel médical de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux en raison de leurs formations ou de leurs compétences particulières, sur la base des informations médicales liées à la prise en charge d'un patient*. » La téléexpertise n'est pas de nature intrinsèquement différente de la consultation spécialisée ou du deuxième avis. Elle ne s'en distingue que parce qu'elle s'effectue par la transmission électronique de données cliniques, biologiques et/ou d'imagerie

[617] Conseil national de l'ordre des médecins. *Les préconisations du Conseil national de l'ordre des médecins*. Télémédecine Janvier 2009. P. 5. http://www.Conseil-national.medecin.fr/sites/default/files/telemedecine2009.pdf. Consulté le 29 avril 2014.

[618] Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine. JORF n°0245 du 21 octobre 2010. Texte n° 13. NOR:SASH1011044D

[619] TRAINEAU, Pierre. Catel, *Notre temps* in rapport d'activités de 2010-2011. p. 38./21. Mai 2011. http://www.catel.pro/documents/Rapport-Activites-2010-2011-CATEL.pdf. Consulté le 29 avril 2014.

et non pas par le déplacement du patient ou du « médecin distant » selon le Conseil national de l'ordre des médecins. Si l'on prend l'exemple des urgences neurovasculaires, le diagnostic précis et la conduite à tenir dépendent d'une analyse des examens radiologiques par un spécialiste et d'une évaluation précise de l'état clinique du patient, le tout dans un contexte d'urgence ou la rapidité de prise en charge influe sur le pronostic. La télé- expertise radiologique et la visioconférence permettent d'assurer cela au-delà des centres d'urgence neurovasculaires[620]. Ou encore, « des médecins de certains centres anticancer de petites villes ont la possibilité d'entrer en relation hebdomadaire par visioconférence avec les cancérologues d'autres établissements qui sont plus importants. Et, ainsi, de discuter des cas compliqués et de prendre des décisions de meilleure qualité »[621].

- « *La télésurveillance médicale qui a pour objet de permettre à un professionnel médical d'interpréter à distance les données nécessaires au suivi médical des patients et, le cas échéant, de prendre des décisions relatives à la prise en charge de ces patients. L'enregistrement et la transmission des données peuvent être automatisés ou réalisés par le patient lui-même ou par un professionnel de santé* ». La télésurveillance se distingue de la téléconsultation en ce sens qu'elle concerne un patient déjà connu par le médecin ou l'équipe soignante. Elle est également différente de la téléassistance « sociale » qui met en œuvre des services à la personne en sécurisant, par exemple, le maintien à domicile, sous la règle du respect de la protection de la vie privée. Le Dr Agnès CAILLETTE-BEAUDOIN, neurologue et directrice de l'association CALYDIAL à Lyon explique que depuis 2006 la télésurveillance est pratiquée pour certains de leurs patients insuffisants rénaux qui réalisent des dialyses péritonéales à domicile. Trois ou quatre fois par jour une infirmière vient leur infuser du Liquide de dialyse neuf pour récolter celui qui est saturé à chaque passage, grâce à un stylo caméra et un cahier doté d'une technologie spéciale. Elle inscrit certaines données : le poids de la poche infusée, le poids de la poche récoltée, le poids du patient, sa tension. Le tout est transmis en direct à un centre où se trouve le néphrologue et analysé par un logiciel pour repérer d'éventuels signaux d'alerte. Cela leur permet d'intervenir rapidement[622].

[620] Bertrand, Jean-Marie. *Un cadre juridique pour favoriser le développement de la télémédecine* in Les cahiers de la télésanté 2009, vers l'âge de raison... P. 9

[621] TRAINEAU, Pierre. Catel, rapport d'activité de 2010- 2011. p. 37

[622] Catel, rapport d'activité de 2010- 2011. p. 37- 38.

- *« La téléassistance médicale qui a pour objet de permettre à un professionnel médical d'assister à distance un autre professionnel de santé au cours de la réalisation d'un acte* ». L'application la plus médiatisée, en matière de téléassistance médicale, est représentée par la téléchirurgie[623], domaine dans lequel des équipes françaises s'illustrent régulièrement. Cette pratique se déploie rapidement et favorise même des collaborations entre médecins situés dans des États différents. Par exemple, des médecins québécois et normands travaillent à faciliter la prise en charge des patients à domicile par téléassistance. Initié par le CHU de Sherbrooke au Québec, le projet met en situation une infirmière au domicile du malade. Lorsqu'elle a un doute sur la façon de soigner la plaie, elle sort son téléphone portable et filme la zone à soigner. A l'autre bout du fil, un expert la renseigne en temps réel sur la conduite à tenir[624].

En plus des applications proposées par rapport LASBORDES, le décret sur la télémédecine ajoute en cinquième position « *la réponse médicale qui est apportée dans le cadre de la régulation médicale mentionnée à l'article L. 6311-2 et au troisième alinéa de l'article L. 6314-1 »* du code de la santé publique. Il s'agit donc de téléprescription dans le cadre de la régulation médicale. L'aide médicale urgente est définie à l'article L. 6311-1 du code de la santé publique comme une organisation permettant de faire assurer aux malades les soins d'urgence appropriés à leur état. En février 2009, la haute autorité de santé (HAS) a rédigé des recommandations[625] sur la prescription médicamenteuse par téléphone (ou

[623]La première télé chirurgie a eu lieu le 7 septembre 2001 par le Professeur Jacques MARESCAUX assisté des Professeurs LEROY et GAGNER. « L'intervention chirurgicale s'est déroulée non pas à partir d'un hôpital, mais dans un immeuble de Manhattan. L'équipe chirurgicale était répartie de la manière suivante : le Professeur. J. Marescaux assisté du Professeur. M. Gagner étaient à New York ; le Professeur. J. Leroy et le Dr. M. Smith se trouvaient dans le bloc opératoire du C.H.U. de Strasbourg, prêts à intervenir en cas de besoin. L'intervention s'est déroulée sous anesthésie générale, se conformant aux règles classiques de la chirurgie mini-invasive, avec introduction d'une optique et d'une caméra dans le ventre de la patiente et des deux instruments permettant d'opérer. » IRCAD, France Telecom, Computer Motion. *« Opération LINDBERG » Une première mondiale en télé-chirurgie : le geste chirurgical a traversé l'atlantique*. Conférence de presse 19 septembre 2001. P.3. http://www.ircad.fr/event/lindbergh/lindbergh_presse_fr.pdf. Consulté le 2 mars 2012.

[624] Les cahiers de la télésanté 2010. *Une nouvelle approche du médico-social* in hôpital, patients, santé, territoires : vers plus de mobilité d'autonomie et de bien-être ? p. 31–32.

[625] Recommandations professionnelles portant sur la prescription médicamenteuse par téléphone (ou - téléprescription) dans le cas de la régulation médicale. http://www.has-sante.fr/portail/upload/docs/application/pdf/2009-05/teleprescription-recommandations.pdf. Consulté le 27 octobre 2011.
Ces recommandations concernent la téléprescription dans le seul cadre de la régulation médicale, une situation bien particulière puisque le médecin ne connaît pas le patient et ne l'examine pas. « *Elles précisent les situations où une prescription par téléphone peut être proposée : une demande de soins non programmée qui nécessite un Conseil médical et thérapeutique, hors urgence vitale (nécessitant un examen médical immédiat) ou l'adaptation en urgence d'un traitement déjà prescrit lorsque le médecin traitant n'est pas joignable* », précise le Dr Revel-Delhom. Dans les deux cas, le médecin régulateur doit s'assurer de la bonne compréhension du patient. Les recommandations définissent également les éléments à faire préciser lors de l'interrogatoire, les mentions qui

téléprescription) dans le cadre de la régulation médicale pour encadrer cette pratique. Le décret[626] n° 87-1005 du 16 décembre 1987 abrogé le définissait en son article 3, 5 missions des services d'aide médicale urgente notamment, le fait d' *« assurer une écoute médicale permanente, de déterminer et déclencher dans le délai le plus rapide, la réponse la mieux adaptée à la nature des appels »*. Cette disposition a été reprise par l'article R. 6311 - 2 du code de la santé publique. L'article 49 de la loi hôpital, patients, santé et territoires, précise quant à lui que *« pour l'accomplissement de la mission de service public de permanence des soins, des modalités particulières de prescription sont fixées par voie réglementaire[627].»* En pratique, la prescription médicamenteuse par téléphone dans le cadre de la régulation médicale correspond à trois situations : la rédaction d'une ordonnance à distance, la prescription des médicaments présents dans la pharmacie familiale et l'adaptation d'un traitement prescrit antérieurement par un praticien non joignable.[628]

---

doivent figurer sur l'ordonnance éventuelle et les modalités d'obtention des médicaments, en coordination avec le pharmacien. Les techniques pour assurer la traçabilité de l'entretien téléphonique et pour garantir la confidentialité lors du transfert de l'ordonnance (un courriel plutôt qu'un fax) sont rappelées. Autant de pistes pour guider le prescripteur sur la forme. En revanche, sur le fond, le médecin régulateur demeure seul juge. « *Il prend sa décision de téléprescription ou pas, au cas par cas, en fonction des informations dont il dispose et de son expérience,* insiste le Dr Revel-Delhom*. C'est pourquoi les recommandations ne citent pas de situations cliniques ou de liste de médicaments.*» HAS. *Encadrer la téléprescription dans le cadre de la régulation médicale*. Lettre d'information n° 19 de novembre – décembre 2009. http://www.has-sante.fr/portail/jcms/c_887837/encadrer-la-teleprescription-dans-le-cadre-de-la-regulation-medicale. Consulté le 15 novembre 2011.

[626] Article 3 du Décret n°87-1005 du 16 décembre 1987 relatif aux missions et à l'organisation des unités participant au service d'aide médicale urgente appelées SAMU. NOR: ASEP8701666D. JORF du 17 décembre 1987 p. 14692. Il a été abrogé le 26 juillet 2005. Ce décret «SAMU» a été fondu par le décret n° 2006 - 576 du 22 mai 2006 relatif à la médecine d'urgence et modifiant le code de la santé publique (dispositions réglementaires). Ainsi, les dispositions de l'article 3 du décret SAMU sont-elles reprises par l'article R 6311-2 du code de la santé publique : « *Pour l'application de l'article R. 6311-1, les services d'aide médicale urgente : 1° Assurent une écoute médicale permanente ; 2° Déterminent et déclenchent, dans le délai le plus rapide, la réponse la mieux adaptée à la nature des appels ; 3° S'assurent de la disponibilité des moyens d'hospitalisation publics ou privés adaptés à l'état du patient, compte tenu du respect du libre choix, et font préparer son accueil ; 4° Organisent, le cas échéant, le transport dans un établissement public ou privé en faisant appel à un service public ou à une entreprise privée de transports sanitaires ; 5° Veillent à l'admission du patient.»* .

[627]Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires(1)

[628] Pour le Docteur Sévérine CAHUN-GIRAUD, Médecin régulateur SAMU, il faut retenir que : « *ce mode de prescription nécessite une information précise du patient sur les modalités du traitement et sur les signes à surveiller pour détecter une éventuelle aggravation justifiant un rappel. La prescription est limitée dans le temps et le nord renouvelable. Elle comporte obligatoirement la mention « téléprescription » et est transmise, de préférence par fax, à la pharmacie déterminée avec le patient. Le recueil des informations nécessaires à la prescription peut s'avérer difficile, de même que le choix de la pharmacie de garde. Le suivi de la prescription pourrait être assuré par un rappel du patient par le régulateur, mais n'est actuellement pas réalisable par manque d'effectifs.* CAHUN-GIRAUD, Sévérine. *La téléprescription dans le cadre de la régulation médicale. De nouvelles recommandations*. Mise à jour le 17 juin 2010. http://www.macsf.fr/vous-informer/teleprescription-regulation-medicale.html . Consulté le 27 octobre 2011.

Le rapport LASBORDES a classé la téléprescription comme une application médico-sociale de la télésanté sans faire de distinction entre la situation d'un médecin avec ses patients et celle de la régulation médicale. Le décret a, quant à lui, reconnu cette pratique comme une application médicale mais en retenant uniquement le cadre de la régulation médicale d'urgence. Ce décret semble alors mieux refléter la volonté des médecins car selon un sondage[629] Sofres de mars 2011, 81% des médecins interrogés ne sont pas prêts à donner des conseils médicaux en ligne en dehors de la régulation médicale.

b. Les aspects juridiques de la télémédecine

La loi du 13 août 2004 relative à l'assurance maladie avait introduit, par ses articles 32 et 33, la télémédecine dans la législation française. Le décret[630] d'Octobre 2010 relatif à la télémédecine, tout en offrant un cadre légal plus détaillé a abrogé les articles 32 et 33 précités. Ce texte a ajouté au code de la santé publique un chapitre VI portant sur la télémédecine *« après le chapitre V du titre III de la sixième partie du code*[631]*. »* Il fixe les conditions d'exercice de la télémédecine et en précise les règles d'organisation. Ainsi, tout comme pour la médecine classique, « *les actes de télémédecine sont réalisés avec le consentement libre et éclairé de la personne »* qui peut être exprimée par voie électronique. Sauf en cas d'opposition du patient, *« les professionnels participants à cet acte peuvent échanger des informations la concernant notamment par le biais des technologies de l'information et de la communication*[632] *»*. Pour une question sécuritaire, les professionnels de santé intervenant dans l'acte devront être authentifiés et les patients, identifiés. Les professionnels devront pouvoir accéder aux données médicales du patient nécessaires à la réalisation de l'acte et le patient devra être formé et préparé à l'usage du dispositif de la télémédecine si nécessaire[633]. Par ailleurs, l'organisation des activités de télémédecine devra s'inscrire dans une convention.

[629] Newsletter médecins 8 avril 2011. http://www.Conseil-national.medecin.fr/newsletter/2011/4 Consulté le 30 avril 2014.

[630] Décret d'application de la loi HPST de 2009.

[631] Première disposition du décret

[632] Article R. 6316 - 2

[633] Article R. 6316 - 3

Elle pourra se faire soit dans le cadre d'un programme national, soit par des contrats pluriannuels relatifs à l'amélioration de la qualité des soins et leur coordination, soit par une convention signée entre un organisme qui propose des actes de télémédecine ou un professionnel de santé libéral envisageant cette activité et l'Agence régionale de la santé dont ils dépendent[634]. «*Les contrats déterminent les pénalités applicables aux titulaires de l'autorisation au titre des articles L. 6114-2 et L. 6114-3 en cas d'inexécution partielle ou totale des engagements dont les parties sont convenues. Ces pénalités financières sont proportionnées à la gravité du manquement constaté et ne peuvent excéder, au cours d'une même année, 5 % des produits reçus, par l'établissement de santé ou par le titulaire de l'autorisation, des régimes obligatoires d'assurance maladie au titre du dernier exercice clos*[635] ». La question de la responsabilité est d'autant plus importante que le consentement donné par le patient forme un contrat médical et que la spécificité de la télémédecine induit un plus grand nombre de responsabilités en jeu. En effet, selon le Professeur PENNEAU, « *le médecin, du fait de son installation est en état de pollicitation, et lorsque le patient répond à cette offre et l'accepte, le contrat est formé*[636] ». La difficulté serait de savoir si en matière de télémédecine, le contrat médical lie autant le médecin requérant que le télémédecin (médecin requis) au patient. Quel lien juridique s'instaure entre le patient et le télémédecin ? Quel juge est compétent pour connaître de cette affaire ?

Même si la loi du 13 août 2004 avait déjà reconnu dans son article 32 que l'acte de télémédecine est un acte médical à part entière et qu'il doit, par conséquent être effectué dans le strict respect des règles de déontologie médicale, la législation en la matière n'est pas très fournie. Les questions de responsabilité des acteurs de la télémédecine, notamment, restent floues du fait de l'absence de précision quant à leurs liens légaux. Le recours à un télémédecin lors d'actes de téléconsultation ou de télésurveillance ou de réponse médicale urgente engage inévitablement sa responsabilité en cas d'incident même s'il n'a passé avec le patient, aucun contrat au sens de l'arrêt Mercier. L'article 60 du code de déontologie médicale ne reconnaît pas non plus de contrat médical entre le patient et le référant en l'absence d'accord de volonté.

634 Article R. 6316 - 6

635 Article L 6114-1 du code la santé publique.

636 PENNEAU, Jean. *La responsabilité du médecin*. Paris. Dalloz, 1992. P. 8.
Depuis l'arrêt Mercier du 20 mai 1936 (Cassation civile, 20 mai 1936. Droit pénal 1936, I, p. 88), la Cour de cassation a consacré la formation d'un « véritable contrat » entre le médecin et son patient.

La responsabilité du télémédecin ne serait pas d'ordre contractuel mais plutôt délictuel ; ce qui le rendrait alors plus vulnérable. Compte tenu du caractère médical de leur lien et de l'obligation de moyens qui pèse sur les médecins, il serait également inapproprié de se fonder directement sur l'article 1382[637] du code civil pour engager sa responsabilité d'autant plus que l'article 64[638] du code de la santé publique en prévoit d'office. Pour Me DESMARAIS[639], ce serait aussi une manière de « battre en brèche » le principe du contrat médical posé par l'arrêt Mercier.

Il existe bien une convention entre le médecin requérant et le télémédecin qui pourrait s'analyser comme une stipulation pour autrui au sens de l'article 1121[640] du code civil. C'est ce qu'a retenu le juge dans l'affaire centre nationale de transfusion sanguine et autres du 17 décembre 1954[641] lorsque l'hôpital public a eu recours à une œuvre spécialisée de transfusion sanguine pour procurer du sang à une malade. *« L'assistance publique hospitalière doit être considérée comme ayant stipulé la fourniture de sang au profit de la malade hospitalisée.»* La stipulation pour autrui est une opération juridique par laquelle une personne que l'on appelle le stipulant contracte avec une autre, le promettant, chargée d'exécuter une obligation au profit d'une troisième appelée tiers bénéficiaire, ici le patient. Dans cette logique, le télémédecin s'engage vis-à-vis du patient qui, de ce fait, peut agir en responsabilité contractuelle pour solliciter la réparation des dommages pour inexécution. En revanche, le promettant, ici, le télémédecin peut également opposer à ce dernier les exceptions qu'il aurait opposées au stipulant[642], ici le médecin requérant. En dehors des cas de stipulations pour autrui classiques comme le contrat d'assurance ou de donation, il serait difficile, par exemple, pour un télémédecin de pouvoir exercer ce droit à l'encontre du patient. Il est peu probable que la

---

[637] *«Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer.»*

[638] Article 64 (article R. 4127 - 64 du code de la santé publique) : « *lorsque plusieurs médecins collaborent à l'examen ou au traitement des malades, et doivent se tenir mutuellement informés ; chacun des praticiens assume ses responsabilités personnelles et veilles à l'information du malade. »*

[639] DESMARAIS, Pierre. *La télémédecine, source de nouveaux cas de responsabilité in* communication commerce électronique n° 9, septembre 2011, étude 16.

[640] *«On peut pareillement stipuler au profit d'un tiers lorsque telle est la condition d'une stipulation que l'on fait pour soi-même ou d'une donation que l'on fait à un autre. Celui qui a fait cette stipulation ne peut plus la révoquer si le tiers a déclaré vouloir en profiter.»*

[641] Cassation civile 2ème, 17 décembre 1954. Semaine juridique édition générale 1954, II. 8490.

[642] Cassation civile 1ère, le 29 novembre 1994. N° 92-15.783. Bulletin 1994. I. n° 353. P. 254.

responsabilité du médecin soit atténuée ou le droit à l'indemnisation du patient réduit du fait de son erreur, de sa faute ou de sa négligence.

Le rapprochement du lien existant entre les médecins requérant et le télémédecin de la stipulation pour autrui n'est pas partagé par tous les auteurs. En effet, pour Liliane DUSSERRE et François-André ALLAERT[643], ces relations doivent être représentées sous une forme contractuelle qui, en l'absence de textes réglementaires et de jurisprudence pourrait se reporter, par analogie, aux dispositions qui régissent la collaboration entre laboratoires d'analyses biologiques. Le contrat de collaboration entre laboratoires pourrait donc servir de modèle et fixer les responsabilités de chacun des intervenants, sous réserve de l'appréciation souveraine des tribunaux. Le décret[644] du 15 mars 1993 modifié par celui du 27 décembre 1995[645] prévoit qu'un contrat de collaboration doit être établi et que le patient doit être informé du nom et de l'adresse du laboratoire qui a pratiqué les analyses, ainsi que du nom du directeur ou du directeur adjoint sous le contrôle duquel ces analyses ont été effectuées. La téléexpertise pourrait ainsi aisément être rapprochée de cette situation de collaboration dans le cas de l'anatomopathologie et même dans le cas de plateau médico-technique comme la radiologie. L'intérêt de ce rapprochement résiderait dans le fait que le contexte juridique est déjà établi avec une précision qui clarifie les responsabilités en cas d'erreur ou d'accident. La loi du 27 janvier 1993 a été complétée par l'article L 760 du code de la santé publique qui prévoit un alinéa indiquant que : *« dans le contrat de collaboration, l'analyse est effectuée sous la responsabilité du laboratoire qui a effectué le prélèvement. »* Ainsi, en matière de télémédecine, le patient ne pourrait engager que la responsabilité du médecin requérant en cas de problème ; quitte pour ce dernier à exercer une action récursoire contre le télémédecin. La responsabilité du prestataire électronique est nécessairement subsidiaire dans le cas d'un

[643] DUSSERRE, Liliane, ALLAERT, François-André. *La télémédecine est-elle légale et déontologique* ? in Information médicale : aspects déontologiques, juridiques et de santé publique. Volume 8. Paris, 1996.

[644] Décret n° 93-354 du 15 mars 1993 relatif *aux conditions d'autorisation des laboratoires d'analyses de biologie médicale et au contrôle de bonne exécution de ces analyses et modifiant les décrets numéro 76 - 1004 du 4 novembre 1976 et n° 83-104 du 15 février 1983.* NOR : SANP9300553D. JORF n° 64 du 17 mars 1993. p. 4155.

[645] Décret n° 95-1321 du 27 décembre 1995 modifiant le décret n° 76. 1004 du 4 novembre 1976 fixant les conditions d'autorisation des laboratoires d'analyses de biologie médicale. Décret abrogé mais remplacé par Décret n°2005-840 du 20 juillet 2005 relatif à la sixième partie (Dispositions réglementaires) du code de la santé publique et modifiant certaines dispositions de ce code. NOR: SANP0522707D

recours en responsabilité à l'encontre du médecin, ou du télémédecin, de sorte que ceux-ci ne pourront exercer qu'un recours récursoire à l'encontre de leur prestataire[646].

Le recours à la télémédecine peut conduire à des situations sans précédents en termes de responsabilité et, dans certains cas, engendrer des situations de coresponsabilité. Certes, les juridictions compétentes comme les conseils de discipline des ordres, fixeront les règles en cas de contentieux, et une jurisprudence viendra clarifier l'application des principes déontologiques et juridiques. Cependant, afin de prévenir des appréhensions à cet égard, il convient d'organiser cette pratique dans un cadre législatif et réglementaire formalisé[647]. Le décret de 2010 sur la télémédecine devrait être complété dans ce sens par des règlements ou des référentiels. Les déclarations[648] de la DGOS (Direction générale de l'offre de soins) de la fin de l'année 2010 sur la nécessité d'un cadrage éthique et juridique du déploiement de la télémédecine pourraient aller dans ce sens. La DGOS préconise que l'on approfondisse le décret du 19 octobre 2010 en clarifiant les principes « et non les modalités » relatifs à *« la responsabilité médicale, à la prescription, aux conséquences en termes de degrés de compétences des professionnels de santé, sur la coopération interprofessionnelle et sur la formation, initiale et continue ».*

---

[646] A l'instar des logiciels destinés à être utilisés spécifiquement à des fins diagnostiques ou thérapeutique, le matériel électronique nécessaire à la télémédecine doit s'analyser juridiquement comme un dispositif médical (code de la santé publique, article L. 5211 -), et donc comme un produit de santé, de sorte que le professionnel de santé sera tenu d'une obligation de sécurité de résultat quant au fonctionnement de ce matériel médical (code de la santé publique, article L. 1142 - 1,1). Le professionnel de santé est, bien évidemment, lié par contrat à son prestataire, de sorte qu'il devrait, théoriquement, agir à son encontre sur le fondement de l'article 1147 du Code civil. Toutefois l'action pourrait se heurter à certaines clauses limitatives de responsabilité voire à des clauses plafonnement le montant des indemnités dues, de sorte que l'on pourrait s'interroger quant à une action des professionnels de santé contre le fabricant sur le fondement de la responsabilité du fait des produits défectueux. Ce régime de responsabilité, applicable malgré l'existence de relations contractuelles (article 1386 - 1 du Code civil), présente l'avantage de permettre d'écarter les clauses limitatives de responsabilité (article 1386 - 11 du Code civil). Mais, dans son dernier état, la jurisprudence (CJCE, 4 juin 2009, aff. C-285/08, § 28 : jurisData n° 2009 -007423. Cassation commerciale, 26 mai 2010, numéro 07 - 11. 744 jurisData n° 2010 - 007170.) considère que la réparation d'un dommage causé à une chose destinée à un usage professionnel est utilisée pour cet usage ne relève pas du champ d'application de la directive 85/374/CEE du Conseil, le 25 juin 1985.
DESMARAIS, Pierre. *La télémédecine, source de nouveaux cas de responsabilité in* communication commerce électronique n° 9, septembre 2011, étude 16.

[647] Conseil national de l'ordre des médecins. *Les préconisations du Conseil national de l'ordre des médecins.* Télémédecine Janvier 2009. P. 10.

[648] Ticsanté.com. *La DGOS prépare un plan national de déploiement de la télémédecine*. 1er décembre 2010. http://www.ticsante.com/la-DGOS-prepare-un-plan-national-de-deploiement-de-la-telemedecine-NS_801.html. Consulté le 29 avril 2014.

S'agissant de la compétence juridictionnelle pour trancher la question de la responsabilité des professionnels intervenant dans la pratique de la télémédecine, le décret sur la télémédecine de 2010 n'est pas plus exhaustif. La jurisprudence[649] relative au cumul des responsabilités entre un praticien libéral et un centre de transfusion sanguine a jugé qu'il appartient à la victime de saisir les juges judiciaires et administratifs de façon concurrente afin de les voir se prononcer sur la responsabilité des personnes publiques et privées en cause. Un rapport[650] de l'Assemblée nationale de septembre 2004 sur les nouvelles technologies de l'information et des systèmes de santé recommandait, pour la bonne marche de la télémédecine, qu'une disposition législative prévoie que la compétence juridictionnelle se situe au lieu de consultation du patient.

Au plan européen dans la directive[651] européenne relative à l'application des droits des patients en matière de soins de santé transfrontaliers de mars 2011 pour un certain nombre de questions juridiques relatives à la télémédecine internationale. Ses articles 5 et 16 établissent respectivement les responsabilités des autorités de l'État membre de traitement contre la chaîne du traitement médical et les garanties quant à la qualité et la sécurité médicales qui entoureront la télémédecine transfrontalière. Cependant, plusieurs questions attendent encore d'être clarifiées. Il s'agit de la reconnaissance de la télémédecine par tous les États membres comme un acte médical[652], du problème de la limite de l'application du droit communautaire lorsque les entreprises de télémédecine sont implantées en dehors de l'Union européenne. Certaines questions sont d'ordre formel et concernent le consentement des patients, le contrôle de la qualité des services, la réglementation applicable au remboursement des prestations et les procédures légales adéquates à suivre en cas de conflit à propos des prestations. Une

[649] Tribunal des conflits, 14 février 2000, n° 02929 : jurisData n° 2000 - 111 468.

[650] DIONIS DU SEJOUR, Jean, ETIENNE, Jean-Claude. *Nouvelles technologies de l'information et système de santé : « la nouvelle révolution médicale »*. Septembre 2004. Rapport n° 1686 Assemblée nationale – n° 370 Sénat - consultable sur les sites Internet Assemblée nationale et Sénat. P. 4. http://www.assemblee-nationale.fr/documents/resume-rapport-ntic-sante.pdf. Consulté le 15 novembre 2011.

[651] Directive 2011/24/UE du Parlement européen et du Conseil le 9 mars aux 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers. JOUE L 88 du 4.4.2011, p. 45–65. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32011L0024:FR:NOT. Consulté le 15 novembre 2011

[652] *« Dans certains États membres comme par exemple l'Autriche, la télémédecine ne peut pas être considérée comme un acte médical parce que selon la loi autrichienne, un acte médical implique que le patient et son médecin traitant soient physiquement en présence l'un de l'autre dans une même pièce. Si la télémédecine n'est pas considérée comme un acte médical, cela peut signifier que la protection juridique offerte dans le cadre de procédures médicales ne fonctionne pas ».* PATTYNAMA, Peter M. *Aspects juridiques de la télémédecine transfrontalière.* Les dossiers européens. Juin - juillet 2010 n° 20. Le défi de la télémédecine en Europe. P. 38-39.

harmonisation plus approfondie de la législation européenne et internationale si possible s'impose donc pour le déploiement de la télémédecine transfrontalière. Il faut espérer que cet effort permette de résoudre, par la même occasion, dans une certaine mesure, les problèmes posés par le statut juridique de la télésanté.

Paragraphe 2: Le statut juridique de la télésanté

En l'état actuel du droit positif, le statut juridique général de la télésanté n'a pas encore été expressément établi. En France, la loi "hôpital, patients, santé, territoires", du 21 juillet 2009, constitue une référence en la matière. Mais celle-ci insiste davantage sur le cadre de la télémédecine (article 78) et les dossiers médicaux personnel et pharmaceutique (article 50), des applications de la télésanté plutôt que sur cette dernière avec toutes ses composantes. La télésanté comprend, en effet, plusieurs applications de services à distance ; ce qui peut impliquer des conflits de lois et de juridictions.

A. Un service fourni à distance

La télésanté, ensemble de services en rapport avec le domaine de la santé et fournis à distance, est encadrée par plusieurs législations liées, chacune pour sa part, à une particularité de ces services. La télésanté fait ainsi intervenir le droit international et le droit communautaire, la législation sur les prestations de service à distance, la législation sur la protection des données personnelles et la législation sur la santé publique.

La télésanté est l'utilisation des technologies de l'information de la communication en vue d'offrir des informations, des services et de l'expertise en santé sur de courtes ou longues distances[653]. Si la courte distance fait référence à un échange à l'intérieur d'un même établissement sanitaire ou d'une même ville ou même à l'intérieur des frontières d'un État, la

[653] Conception du ministère de la santé du Canada. CSSSPNQL. *Premières nations du Québec. Plan stratégique de télésanté 2007-2010.* Décembre 2007. p. 9 http://www.cssspnql.com/docs/centre-de-documentation/plan-strat%C3%A9gique-t%C3%A9l%C3%A9sant%C3%A9-pn-2007-10-fr.pdf?sfvrsn=2. Consulté le 29 avril 2014.

longue distance peut aller à l'extérieur d'un État ou même entre deux ou plusieurs continents. Pour régir ce type de relation au plan international, c'est le droit international privé ou même public qui est applicable à ce domaine particulier qui suscite d'ailleurs des interrogations sur son statut juridique.

En tant que *« coopération médicale à distance qui permet d'optimiser les ressources médicales*[654] *»*, la télésanté est une capacité intellectuelle mise à la disposition du patient, du professionnel de santé ou de toute autre personne intéressée. C'est plus un service qu'un simple produit malgré le grand nombre de matériels qui y intervient. C'est l'expertise technologique et médicale qui est déplacée car, comme le disait M. SARRAMON : *« ce n'est plus le patient qui se déplace mais la science médicale qui se regroupe pour aller vers le patient*[655] *»*. Généralement, ce service est reçu en contrepartie d'un paiement d'honoraires du professionnel de santé, du prix de la connexion à internet et/ou encore du prix de l'accès à certains liens en ligne. Sont considérées comme services *« les prestations fournies normalement contre rémunération, dans la mesure où elles ne sont pas régies par les dispositions relatives à la libre circulation des marchandises, des capitaux et des personnes*[656] *»*. Paradoxalement, la directive « services » de l'Union européenne du 12 décembre 2006 relative aux services dans le marché intérieur exclut de son champ d'application les services de soins de santé[657] après avoir défini les services comme étant des activités économique non salariées, exercées normalement contre rémunération.

La directive 2011/24/UE définit les « *soins de santé* » comme « *des services de santé fournis par des professionnels de la santé aux patients pour évaluer, maintenir ou rétablir*

---

654 FERRAUD-CIANDET, Nathalie. *L'Union européenne et la télésanté in Revue Trimestrielle de droit européen.* N° 3 du 1er juillet 2010. P. 544.

655 SARRAMON, J.P. *Médecine: médecin – malade. World congress on telemedecine for the development of the global information society for health.* Toulouse. Du 30 Novembre au 1er Décembre 1995. in L'apport des nouvelles technologies de l'information et de la communication au service de la santé en Afrique dans le cadre du NEPAD. 21 février 2002. p. 24. http://www.asmp.fr/travaux/gpw/nouveltecno/rapport.pdf. Consulté le 30 avril 2014.

656 Traité pour le fonctionnement de l'Union européenne, article 57(ex article 50). Version consolidée au JOUE n° C 326 du 26 octobre 2012.
La directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur du 12 décembre 2006 a repris cette définition en son article 4 : *« toute activité non salariée, exercée normalement contre rémunération, visée à l'article 50 du traité »*.JOUE L /376 P. 36 -68

657 *« La présente directive ne s'applique pas aux activités suivantes : (...) f) les services de soins de santé, qu'ils soient ou non assurés dans le cadre d'établissements de soins et indépendamment de la manière dont ils sont organisés et financés au niveau national ou de leur nature publique ou privée*; » La directive 2006/123/CE du Parlement européen et du Conseil relative aux services dans le marché intérieur du 12 décembre 2006. Article 2.

leur état de santé, y compris la prescription, la délivrance et la fourniture de médicaments et des dispositifs médicaux[658]*. »* La télésanté est donc un service au sens du traité pour le fonctionnement de l'Union européenne et de la directive relative aux droits des patients, qui est caractérisé par la distance géographique entre les prestataires et les bénéficiaires. A ce titre et malgré le caractère particulier des prestations médicales (services d'intérêt général, services sensibles tout comme les services sociaux[659]), elles sont soumises au principe de la libre circulation des services. La Cour de justice des communautés européennes l'a rappelé dans plusieurs arrêts dont l'arrêt Kohll[660] d'avril 1998 et l'arrêt Stamatelaki[661] sans qu'il soit besoin de différencier les services sociaux d'intérêt général (communication du 26 avril 2006[662]) des services de santé transfrontaliers (communication du 26 septembre 2006[663]).

Au plan européen, en plus de la jurisprudence sus-citée, une directive[664] a été adoptée le 9 mars 2011 pour régir les droits des patients en complément de la législation existante[665].

---

[658] Directive 2011/24/UE. Article 3, a) du Parlement européen et du Conseil du 9 mars 2011 *relative à l'application des droits des patients en matière de soins de santé transfrontaliers*. Journal officiel de l'Union européenne du 4 avril 2011. P. L 88/45. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:FR:PDF. Consulté le 02 octobre 2011.

[659] La Commission européenne l'a reconnu dans le livre blanc depuis 2004.

[660] CJCE. Arrêt Kohll, du 28 avril 1998. N° C-158/96. Recueil. P. I-1931. : « *la Cour a constaté que la nature particulière de certaines prestations de services ne saurait faire échapper ces activités au principe fondamental de libre circulation (arrêt du 17 décembre 1981, Webb, 279/80, Rec. p. 3305, point 10).* » http://curia.europa.eu. Consulté le 30 septembre 2011.

[661] CJCE. Arrêt Stamatelaki du 19 avril 2007. N°C-444/05. JOUE C 96/14 du 28 avril 2007. *« Il convient de rappeler que, selon une jurisprudence constante, les prestations médicales fournies contre rémunération relèvent du champ d'application des dispositions relatives à la libre prestation des services, sans qu'il y ait lieu de distinguer selon que les soins sont dispensés dans un cadre hospitalier ou en dehors d'un tel cadre (arrêt du 16 mai 2006, Watts, C-372/04, Rec. p. I-4325, point 86 et jurisprudence citée) ». http://curia.europa.eu*. Consulté le 30 septembre 2011.

[662] Communication de la Commission. *Mettre en œuvre le programme communautaire de Lisbonne. Les services sociaux d'intérêt général dans l'Union européenne*. Bruxelles, le 26 avril 2006. {SEC(2006) 516} ou COM(2006) 177. http://ec.europa.eu/employment_social/social_protection/docs/com_2006_177_fr.pdf. Consulté le 02 Octobre 2011.

[663] Communication de la Commission. *Consultation concernant une action communautaire dans le domaine des services de santé*. Bruxelles, le 26 septembre 2006. SEC (2006) 1195/4. http://ec.europa.eu/health/ph_overview/co_operation/mobility/docs/comm_health_services_comm2006_fr.pdf

[664] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 *relative à l'application des droits des patients en matière de soins de santé transfrontaliers*. JOUE du 4 avril 2011. P. L 88/45. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:FR:PDF Consulté le 02 octobre 2011.

[665] La directive européenne 2011/24/UE rappelle ces textes en son article 2

De prime abord, cette directive préconise l'extension de la libre prestation des services de santé « ordinaires » aux services de santé en ligne. En effet, à son point 26, elle précise que : « *la Cour de justice a jugé que les dispositions du traité relatives à la libre prestation des services incluent la liberté pour les bénéficiaires de soins de santé, notamment les personnes qui ont besoin de recevoir un traitement médical, de se rendre dans un autre État membre pour y bénéficier de ces soins. Il devrait en être de même pour les bénéficiaires de soins de santé désireux de bénéficier de soins de santé dispensés dans un autre État par d'autres moyens, par exemple les services de santé en ligne ».* En outre, les patients sont autorisés à accéder à distance à leur dossier médical ou de disposer d'au moins une copie de celui-ci dans la limite des mesures nationales prises pour l'exécution des dispositions de l'Union relatives à la protection des données personnelles[666].

Partant du principe qu'il est essentiel pour un patient bénéficiant de soins de santé transfrontaliers de savoir à l'avance quelle réglementation lui sera applicable, la directive a pour objet de prévoir des règles qui visent à faciliter l'accès à des soins de santé transfrontaliers sûrs et de qualité élevée et encourage la coopération en matière de soins de santé entre les États membres, dans le plein respect des compétences nationales en matière d'organisation et de prestations de soins de santé. La directive tend également à clarifier les liens avec le cadre existant relatif à la coordination des systèmes de sécurité sociale, le règlement (CE) n° 883/2004, en vue de l'application des droits des patients[667]. Ce texte fonde ses bases sur un certain nombre de législations existantes en matière de relations contractuelles. Ce sont, notamment, le règlement (CE) n° 593/2008 du Parlement européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome 1)(2), le règlement (CE) n° 864/2007 du Parlement et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome 2) (3) et d'autres règles de droit international privé de l'Union notamment celles relatives à la compétence judiciaire et au droit applicable[668]. La directive rappelle que la réglementation applicable aux soins de santé transfrontaliers devrait être celle figurant dans la législation de l'État membre de traitement, étant donné que conformément à la tête de 168, paragraphe 7, du traité sur le fonctionnement de l'Union européenne l'organisation et la prestation de services de santé et de soins médicaux

[666] Directive 2011/24/UE. Article 5. d)

[667] Directive 2011/24/UE. Article 1er

[668] Directive 2011/24/UE. Article 1er, (q)

relèvent de la responsabilité des États membres. Il faut entendre par *« État membre de traitement », « l'État membre sur le territoire duquel les soins de santé sont effectivement dispensés aux patients. Dans le cas de la télémédecine, les soins de santé sont considérés comme dispenser dans l'État membre où le prestataire de soins de santé est établi*[669] *»*. Pour la directive cette disposition devrait aider le patient à prendre une décision en connaissance de cause et devrait permettre d'éviter les interprétations erronées et les malentendus. Elle devrait également instaurer une relation de confiance d'un niveau élevé entre le patient et le prestataire de soins de santé[670].

Cette législation ne résout pas véritablement le problème des disparités entre les États membres quant aux systèmes de règlement des soins de santé en général et en matière de télésanté en particulier. Mais elle prévoit un dispositif qui vise à organiser les conditions de remboursements des soins transfrontaliers. L'État membre d'affiliation peut imposer à des personnes assurées désireuses de bénéficier de remboursements de coûts des soins de santé transfrontaliers, y compris des soins de santé reçus par les moyens de la télémédecine, les mêmes conditions, critères d'admissibilité et formalités réglementaires et administratives - que celles-ci soient fixées à un niveau local, régional ou national - que ceux qu'il imposerait si ces soins de santé étaient dispensés sur son territoire. Cela peut inclure une évaluation par un professionnel de santé ou un administrateur de la santé fournissant des services pour le système de sécurité sociale obligatoire ou le système de santé national de l'État membre d'affiliation, tel que le médecin généraliste ou le prestataire de soins de santé primaire auprès duquel le patient est inscrit, si cela s'avère nécessaire pour déterminer le droit d'un patient aux soins de santé, à titre individuel[671].

La directive 2011/24/UE a pour objectif de tout mettre en œuvre conformément aux principes établis par la Cour de justice, et sans compromettre l'équilibre financier des systèmes de soins de santé et de sécurité sociale des États membres, d'assurer une plus grande sécurité juridique en matière de remboursement des coûts de soins de santé pour le patient et pour les professionnels de santé, les prestataires de santé et les institutions de sécurité sociale[672]. Par cette directive, l'Union européenne soutient et facilite la coopération et

[669] Directive 2011/24/UE. Article 3

[670] Directive 2011/24/UE. Point 19

[671] Directive 2011/24/UE. Article 7. 7.

[672] Directive 2011/24/UE. Point 27

l'échange d'informations des États membres dans le cadre d'un réseau constitué sur la base du volontariat reliant les autorités nationales chargées de la santé en ligne désignées par les États membres. Elle contribue activement, notamment à l'interopérabilité des systèmes de santé au sein de l'Union. Certes la télésanté n'est pas expressément (littéralement) visée par cette directive, mais nous pourrons considérer que les références à la télémédecine et à la santé en ligne visent implicitement tous les cas de télésanté.

Que ce soit une relation entre professionnels de santé et patient ou entre professionnels de santé, cette prestation de services, dans le cadre de la télésanté, peut engendrer des conflits juridictionnels ou des conflits de lois.

B. Les conflits de lois et de juridictions en matière de télésanté

Au plan international, les problèmes de conflits juridictionnels ou de conflits de lois en matière de télésanté ne semblent pas encore avoir trouvé de solution internationale. Si le problème posé en matière de télésanté sur un plan international relève du droit international privé et/ou public, le droit applicable à cette discipline est des moins aisés à déterminer. La télésanté peut mettre en relation des particuliers dont un professionnel de santé et son patient, ou des professionnels ou encore, faire intervenir un organisme social d'un État. En cas de litige laquelle des juridictions du lieu d'exercice du professionnel de santé ou du lieu de résidence du patient serait-elle compétente pour connaître de l'affaire ? Faut-il appliquer le droit du lieu d'exercice du professionnel de santé ou celui de résidence du patient ?

La télésanté permet d'offrir des services de santé personnalisés à distance impliquant généralement le consentement libre et éclairé des parties et, surtout celui du patient qui est préalablement informé des conditions d'accomplissement desdits actes. Une convention expresse ou tacite est donc systématiquement signée entre les partenaires, qui concourt à une clarification des droits et devoirs incombant à chaque acteur. Vu sous cet angle, les actes de télésanté sont considérés comme tout acte ou fait juridique engageant la responsabilité d'une des parties vis-à-vis de l'autre ou des autres dans un rapport contractuel ou extra contractuel. Myriam Le GOFF-PRONOST a écrit : « *Afin d'étudier les effets de la télémédecine sur les asymétries d'information qui sont marquées dans le domaine de la santé, tout particulièrement les relations entre médecin-patient d'une part, et médecin-expert et médecin-*

demandeur d'autre part, il faut se référer aux modélisations issues de la théorie des contrats[673]. » En outre, il faut relever que les services de télésanté sont dispensés à partir de TIC ; ce qui les rapproche[674] davantage d'actes de commerce électronique[675]. Dès lors, nous nous inspirerons de la législation internationale en la matière pour trouver une réponse à la problématique du droit applicable à une télésanté comportant un ou des éléments d'extranéité.

La jurisprudence française affirme que *« tout contrat international est nécessairement rattaché à la loi d'un État*[676] *»* mais laquelle serait la bonne en matière de télésanté *?* Les règles de droit international privé applicables aux conflits de lois exigent que l'on détermine le lieu d'exercice des services de santé litigieux. Tout dépendra encore de la spécificité de la télésanté et de la spécificité de chaque application de télésanté. En effet, dans un contexte de télémédecine par exemple, pour juger la négligence du médecin l'on doit se référer aux règles ordinaires applicables aux conflits de lois alors que pour déterminer la juridiction compétente pour connaître de cette affaire, on devra d'abord déterminer si l'acte médical est réputé avoir été posé au lieu où se trouve le patient ou au lieu où se trouve le médecin.

---

[673] LE GOFF-PRONOST, Myriam. *TIC, télémédecine et accès aux services : une approche économique***.** Thèse de doctorat. : Sciences économiques: UBO, Institut Télécom-Télécom Bretagne : 2003, P. 276-277

[674] Bien sûr, il ne faut pas omettre que l'article 19 du code de déontologie médicale (article R. 4127 - 19 du code de la santé publique) exclut la médecine du champ du commerce. Le « contrat de soins » qui est à la base de la responsabilité médicale (article 69) n'est pas une convention commerciale, ni un marché. C'est un contrat tacite ou ce qu'apporte l'un n'est pas l'équivalent de ce qu'apporte l'autre. Les médecins s'engagent à donner des soins adéquats (article 32) qui ne sont pas définis par avance et qui diffèrent selon les circonstances.

[675] La loi française pour la confiance dans l'économie numérique (LCEN) n° 2004 - 575 du 21 juin 2004 (JORF du 22 juin 2004 texte 2. NOR : ECOX0200175L) définit en son article 14 le commerce électronique comme l'activité par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services**.** Bien sûr, la directive européenne de 2000 sur le commerce électronique précise en son considérant n° 18 qu'il y a des activités qui de par leur nature ne peuvent pas être réalisées à distance ou par voie électronique telles que le contrôle légal des comptes d'une société ou la consultation médicale requérant un examen physique du patient. Mais, la télésanté ne se limite pas à une consultation médicale en ligne mais consiste également en des services médico-sociaux et d'autres applications médicales (Voir infra sur les applications de télésanté). D'ailleurs, l'alinéa suivant de l'article 14 ajoute qu' « *Entrent également dans le champ du commerce électronique les services tels que ceux consistant à fournir des informations en ligne, des communications commerciales et des outils de recherche, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent. »* Des applications comme la téléinformation, la télévigilance, etc, entrent bien dans ces cadres. http://www.legifrance.gouv.fr

[676] Messageries Maritimes, Cour de cassation, chambre civile, section civile. 21 juin 1950, Revue. Critique. 1950. P.609, note Batiffol. Dalloz 1951. P. 749, note Hamel Joseph. JCP 1950. II. 5812, note Levy Jean Philippe.

En ce qui concerne la résolution des conflits de lois, les dispositions de la Convention de Rome de 1980[677] sur la loi applicable aux obligations contractuelles (pour le principe de la loi du pays du fournisseur de la prestation caractéristique) semblent fournir un certain nombre de solutions. En effet, les parties au contrat sont libres de définir le droit applicable à leur convention. Mais, le cas échéant, l'article 4[678] de la Convention de Rome prévoit que le contrat est régi par la loi du pays avec lequel il présente les liens les plus étroits c'est-à-dire le pays avec lequel la partie qui doit fournir la prestation caractéristique a, au moment de la conclusion du contrat, sa résidence habituelle ou son administration centrale (pour une personne morale, une association). La prestation caractéristique selon Marie-Elodie ANCEL est *« la seule prestation principale dans les contrats à titre gratuit et les actes neutres ; elle est la prestation « pour laquelle le paiement est dû » dans les contrats de fourniture rémunérée ; elle est la prestation finale, qui lie les intérêts des contractants dans les contrats dits d'intérêts communs*[679] ». La question se pose alors de savoir : quelle est la prestation caractéristique dans des actes de télésanté ? Pour notre part, il faut considérer que la prestation caractéristique est constituée par l'ensemble des consignes, soins et conseils délivrés par le professionnel de santé. En matière de télémajordome par exemple, ce sera l'accompagnement, pour la téléinformation, la diffusion d'information et la téléconsultation, la consultation faite à distance. A moins que les parties aient choisi expressément la loi de leur relation, la loi

[677] Convention de Rome n° 80/934/CEE du 19 juin 1980 sur la loi applicable aux obligations contractuelles. JOCE n° C 027 du 26 janvier 1998. P. 0034 - 0046. Publiée par décret n° 91-242 du 28 février 1991, JOCE du 3 mars 1991.

[678] *« Article 4: loi applicable à défaut de choix*

1. *Dans la mesure où la loi applicable au contrat n'a pas été choisie conformément aux dispositions de l'article 3, le contrat est régi par la loi du pays avec lequel il présente les liens les plus étroits. Toutefois, si une partie du contrat est séparable du reste du contrat et présente un lien plus étroit avec un autre pays, il pourra être fait application, à titre exceptionnel, à cette partie du contrat de la loi de cet autre pays.*
2. *Sous réserve du paragraphe 5, il est présumé que le contrat présente les liens les plus étroits avec le pays où la partie qui doit fournir la prestation caractéristique a, au moment de la conclusion du contrat, sa résidence habituelle ou, s'il s'agit d'une société, association ou personne morale, son administration centrale. Toutefois, si le contrat est conclu dans l'exercice de l'activité professionnelle de cette partie, ce pays est celui où est situé son principal établissement ou, si, selon le contrat la prestation doit être abordée par un établissement autre que l'établissement principal, celui où est situé cet autre établissement. (...)*
5. *L'application du paragraphe 2 est écartée lorsque la prestation caractéristique ne peut pas être déterminée. Les présomptions des paragraphes 2,3 et 4 sont écartées lorsqu'il résulte de l'ensemble des circonstances que le contrat présente des liens plus étroits avec un autre pays. »*

L'article 17 de la loi pour la confiance dans l'économie numérique renchérit cette position en précisant que le commerce électronique est soumis *à la loi de l'État membre sur le territoire duquel la personne qui l'exerce est établie sous réserve de la commune intention de cette personne et de celle à qui sont destinés les biens ou services.* La loi pour la confiance dans l'économie numérique désigne donc subsidiairement et impérativement la loi du prestataire alors que le règlement de Rome I en fait une présomption.

[679] ANCEL, Marie-Elodie. La prestation caractéristique du contrat. P. 371.Paris, Économica 2002.

applicable est celle du lieu d'établissement[680] du professionnel de santé qui fournit les soins ou autres services médicaux ou médico-sociaux à distance. Cette solution peut faire craindre que des patients ou des internautes puissent subir des dommages du fait des différences qui existent entre les systèmes de santé des États. En effet, se fondant sur sa connaissance de sa loi nationale en matière de santé publique et notamment l'étendue de la responsabilité des professionnels de santé, une personne peut s'engager en croyant le faire en toute connaissance de cause et être surprise par les limites qui vont être opposées à ses droits par la loi de l'État où est établi son « téléinterlocuteur ». Pour la sécurité des patients et des intéressés à la télésanté en général, il est souhaitable d'harmoniser la législation internationale en matière de santé. En attendant, des initiatives de loi type[681] du genre de celle portant sur le commerce électronique de 1996[682] sont à encourager.

S'agissant des difficultés liées aux conflits de juridiction, le règlement 2000[683] remplaçant la Convention de Bruxelles de 1968 donne compétence de principe au tribunal du défendeur. Son article 18 propose également des mécanismes extrajudiciaires dont la

---

[680] La directive européenne sur le commerce électronique définit le lieu d'établissement en son considérant 19 : *« Le lieu d'établissement d'un prestataire devrait être déterminé conformément à la jurisprudence de la Cour de justice, selon laquelle le concept d'établissement implique l'exercice effectif d'une activité économique au moyen d'une installation stable et pour une durée indéterminée. Cette exigence est également remplie lorsqu'une société est constituée pour une période donnée. Le lieu d'établissement d'une société fournissant des services par le biais d'un site Internet n'est pas le lieu où se situe l'installation technologique servant de support au site ni le lieu où son site est accessible, mais le lieu où elle exerce son activité économique. Dans le cas où un prestataire a plusieurs lieux d'établissement, il est important de déterminer de quel lieu d'établissement le service concerné est presté. Dans les cas où il est difficile de déterminer, entre plusieurs lieux d'établissement, celui à partir duquel un service donné est fourni, le lieu d'établissement est celui dans lequel le prestataire a le centre de ses activités pour ce service spécifique ».* Directive européenne 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »). JOUE n° L 178 du 17 juillet 2000. P. 0001–0016. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L 00 31:FR:HTML. Consulté le 30 avril 2014.

Par analogie, lire Cassation commerciale, 19 Octobre 2010 n° 09-69.246. Bulletin 2010, IV, n° 154, Société JFA chantier naval c/ société Kerstholt teakdecksystems BV. Pour plus d'analyses sur les conflits de lois et de juridictions, lire également Fabienne Jault-Seseke. *Droit international privé*. Dalloz 2011. P 1374.

[681] C'est une loi modèle, un prototype de loi sur une matière spécifique, proposé aux États membres de l'ONU par la CNUCID (Commission des nations unies pour le droit commercial international) modifications dans leur ordre juridique national. Une loi type est incorporée dans une loi interne selon ses besoins et sa structure légale.

[682] Loi type de la CNUCID sur le commerce électronique et guide pour son incorporation 1996 avec l'article 5 bis tel qu'adopté en 1998. 91p. ISBN: 92-1-233323-0. http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf . Consulté le 30 avril 2014.

[683] Règlement (CE) n° 44/2001/ du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale. JOUE du 16 janvier 2001, n° L 012. P. 0001-0023.

médiation ou l'arbitrage. Pour les différends en matière de commerce électronique, ce texte prévoit qu'un consommateur peut demander justice au tribunal du lieu de son domicile si le professionnel avec lequel il a contracté dirige son activité vers le pays où il réside. L'activité du professionnel est considérée comme « dirigée » vers l'État membre dans lequel réside le consommateur contractant si, avant la conclusion éventuelle du contrat, il ressort de son site internet et de l'activité globale du professionnel qu'il envisageait de commercer avec des consommateurs domiciliés dans cet État membre. Dans les affaires Peter Pammer et Hotel Alpenhof GesmbH[684], la Cour de justice des communautés européennes qui fait cette interprétation de l'article 15 du règlement de 2000, donne une liste[685] non exhaustive d'indices pour déterminer la volonté du professionnel de diriger son activité. La doctrine[686] a craint que ces dispositions ne soient préjudiciables au consommateur car, il ne pourra demander justice au tribunal de son domicile qu'à la condition que le professionnel y mène son activité. Et dans le cas échéant, qu'adviendra-t-il de ce droit reconnu au consommateur ? Il aurait été préférable que le consommateur puisse saisir son tribunal en toutes circonstances à cause de sa vulnérabilité. Si l'on ne trouve pas de solution plus favorable pour le patient ou tout intéressé à la télésanté, cette solution pourra y être transposée avec les mêmes risques.

---

[684] CJUE, grande chambre, 7 décembre 2010, Peter Pammer. n° C-585/08 et C-144/09. Document n° 62008CJ0585. http://curia.europa.eu/juris/celex.jsf?celex=62008CJ0585&lang1=en&lang2=MT&type=NOT &ancre=. Consulté le 30 avril 2014.

[685] « *Il peut s'agir, d'abord, d'éléments manifestant une volonté expresse de démarcher des consommateurs étrangers. Tel serait le cas d'une mention précisant que le professionnel propose ses biens ou ses services dans des pays nommément désignés (pts 80 et 81). De même, une telle volonté serait caractérisée par un engagement de dépenses dans un service de référencement sur Internet auprès de l'exploitant d'un moteur de recherche afin de faciliter l'accès du site aux consommateurs étrangers (pt 81). Mais dans la plupart des cas, la Cour reconnaît que la volonté est moins clairement affichée, nécessitant la combinaison de plusieurs indices que sont : la nature internationale de l'activité en cause (comme des activités touristiques) ; la mention de coordonnées téléphoniques avec l'indication du préfixe international ; l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État membre où le commerçant est établi ou l'utilisation d'un nom de domaine neutre (.com ou .eu) ; la description d'itinéraires géographiques d'un État membre vers celui où le professionnel est établi ; la mention d'une clientèle internationale composée de clients domiciliés dans différents États membres (comme la présentation de témoignages de tels clients) ; ou encore la langue utilisée ou la monnaie si l'un et l'autre ne sont pas ceux du pays où le commerçant est établi (pt 83). En revanche, sont expressément écartées par la Cour de justice les informations neutres comme les coordonnées téléphoniques, électroniques ou postales qui ne sont pas caractéristiques, d'autant plus que ces informations sont rendues obligatoires par la législation européenne (Dir. n° 2000/31/CE, 8 juin 2000, sur le commerce électronique). De même, comme l'a précisé la déclaration conjointe du Conseil et de la Commission, la langue ou la monnaie ne constituent pas en soi des informations pertinentes*.» AUBERT de VINCELLES, Carole. *Compétence internationale en matière de cyberconsom mation : précision sur la notion d'activité dirigée in revue des contrats* n° 2 du 1er Avril 2011. LGDJ. Lextenso éditions. p. 515.

[686] BLAISE Jean-Bernard, HUET Jérôme, *Commerce électronique et code de commerce* in le bicentenaire du code de commerce. Université de Paris II. Dalloz 2008. p. 9/24.

Dans tous les cas, il n'y a pas vraiment de risque de « vacuum juris[687] » car l'article 5-2[688] de la Convention de Rome accorde la possibilité de se prémunir des dispositions impératives de la loi de son lieu de résidence habituelle en cas de différend [689]; position partagée par la loi[690] pour la confiance dans l'économie numérique en son article 17. En effet, le 1° de cet article dispose que l'alinéa précédent donnant compétence au tribunal du lieu du domicile du professionnel n'a pas pour objet de priver un consommateur ayant sa résidence habituelle sur le territoire national de la protection que lui assurent les dispositions impératives de la loi française relative aux obligations contractuelles conformément aux engagements internationaux souscrits par la France.

Certes, ces textes régissent les rapports à l'intérieur de l'Europe mais nous pensons que leurs dispositions peuvent inspirer le droit international privé quant aux règlements des conflits internationaux de télésanté.

Finalement, en état embryonnaire ou inexistant dans les États en développement, la télésanté tient une place de choix dans les pays industrialisés du fait du vieillissement de la population et de l'allongement de l'espérance de vie. Elle a beaucoup évolué en une décennie, mais beaucoup reste à faire pour dépasser le cap des expérimentations et assurer une couverture totale du territoire national. Des questions éthiques et juridiques restent encore en suspend, mais la détermination des États développés, notamment, la France et toute l'Union européenne à faciliter l'accès aux soins est certaine. Pour ces États, l'information personnelle du patient et du professionnel fait partie des priorités et c'est ce qui justifie la politique mise en place par le gouvernement français pour le déploiement du dossier médical personnel outil indispensable à l'efficacité de la télésanté.

---

[687] Vide juridique

[688]« Nonobstant les dispositions de l'article 3, le choix par les parties de la loi applicable ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle :
- si la conclusion du contrat a été précédée dans ce pays d'une proposition spécialement faite ou d'une publicité, et si le consommateur a accompli dans ce pays les actes nécessaires à la conclusion du contrat ou,
- si le cocontractant du consommateur ou son représentant a reçu la commande du consommateur dans ce pays (...) »

[689] Règlement de Rome I article 6.1, a.

[690] Loi n° 2004-575 pour la confiance dans l'économie numérique. JORF n° 143 du 22 juin 2004. P. 11168. Texte n°2. NOR: ECOX0200175L.

CHAPITRE II : LE DOSSIER MEDICAL PERSONNEL : UN OUTIL CAPITAL DE MISE EN ŒUVRE DE LA TELESANTE

Le 5 janvier 2011, à l'occasion de sa conférence annuelle, l'ASIP santé annonçait l'ouverture nationale du service DMP. Son déploiement[691] sur l'ensemble du territoire prévu pour toute l'année 2011 intervient au terme d'une phase pilote qui a eu pour objet de tester la fiabilité et la robustesse des systèmes mis en œuvre et de les valider, après évaluation scientifique, sur la base de référentiels techniques établis à l'échelon national suivant la politique mise en place par le gouvernement [692]. Cette annonce était attendue depuis la mi-2007[693]. Mais, depuis sa création décidée par la loi[694] du 13 août 2004 relative à l'assurance maladie, dans le prolongement des dispositions introduites par la loi[695] de 2002 relative aux droits des malades, des inquiétudes d'ordre technique et juridique soulevées n'avaient pas encore reçu de réponse satisfaisante. A ce jour, d'énormes progrès ont été faits afin de permettre cette mise en route du DMP. L'ASIP santé fait avancer le pilotage, notamment en ce qui concerne l'interopérabilité des systèmes d'information de santé. Pourtant, alors que les raisons qui justifient sa création (Section 1) ont été relativement claires dès le départ, les

[691] « *Le déploiement du Dossier Médical Personnel (DMP), lancé en janvier 2011 par l'ASIP Santé s'organise en effet progressivement, par territoire géographique et par filières de soins dans un grand nombre de régions françaises. Il bénéficie pour ce faire de l'appui de « maîtrises d'ouvrage régionales » (MOAR), structures chargées de développer et coordonner sur le terrain les initiatives locales dans le champ de la santé électronique (ou « e-santé »). Ces dernières proposent des actions d'information, de formation et d'accompagnement de l'ensemble des acteurs concernés (médecins de ville et hospitaliers, directeurs d'hôpitaux, associations de patients, éditeurs de logiciels, SSII…) pour favoriser l'usage du DMP sur leur territoire.* » ASIP, *Déploiement du DMP: l'ASIP Santé apporte son soutien à 33 établissements*. http://esante.gouv.fr/actus/dmp/deploiement-du-dmp-l-asip-sante-apporte-son-soutien-a-33-etablissements-mise-a-jour. Consulté le 30 avril 2014.

[692] Observations du gouvernement sur le recours exercé contre la loi relative à l'assurance maladie. JORF du 17 août 2004. P. 14666

[693] Aux termes de l'article L. 161- 36 - 2 du code de la sécurité sociale, le dispositif d'accès et d'écriture dans le dossier médical personnel pour chaque professionnel auquel le patient fait appel, après autorisation de ce dernier, entrera en vigueur à compter du 1er juillet 2007.

[694] Loi n° 2004-810 du 13 Août 2004 relative à l'assurance maladie. Parue au JORF du 17 Août 2004 mais rectifiée au JORF n° 276 du 27 novembre 2004. P 20151 et suivant. NOR : *SANX0400122Z*

[695] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (1). JORF n° 54 du 5 Mars 2002. Texte n°1. p 4118 et suivants NOR: MESX0100092L **.**

garanties de la confidentialité (Section 2) des données médicales à caractère personnel qu'offre le DMP sont encore en construction.

Section 1: La constitution du DMP

Le rapport de M. DUBERNARD du 24 juin 2004 sur le projet de loi relative à l'assurance maladie faisait remarquer *« une insuffisante coordination des soins, d'abord imputable à une coordination déficiente des professionnels de santé. Le cloisonnement entre les médecins libéraux (peu habitués au travail en groupe ou en réseaux), entre les différents professionnels de santé (avec les clivages spécialistes/généralistes et médecins/professions paramédicales), auquel s'ajoute l'étanchéité entre la médecine de ville et les établissements de santé, a été mis en évidence [696] »*. Cette situation est problématique car elle est à l'origine d'erreurs de diagnostics ou de prescriptions quelquefois fatales aux patients sans oublier les dépenses supplémentaires[697] et pas toujours nécessaires qu'elle peut occasionner. Le dossier médical personnel apparaît ainsi comme un moyen de lutte contre les prescriptions injustifiées ou dangereuses, le nomadisme médical et les redondances d'actes médicaux. Le gouvernement entend utiliser cet instrument pour mieux coordonner les soins et réduire les dépenses de santé[698]. Après analyse du projet, la CNIL demande, dans sa délibération[699] du 10

[696] DUBERNARD, Jean Michel. Rapport n° 1703 sur le projet de loi relatif à l'assurance maladie déposé à l'Assemblée Nationale le 24 juin 2004. http://www.assemblee-nationale.fr/12/rapports/r1703.asp#P278_28212. Consulté le 27 mai 2014.

[697] La préoccupation avait été relevée par M. ROCHEBLOINE François en 2001 qui déplorait le manque de coordination entre établissements de santé et les désagréments personnels et les frais supplémentaires indéniables à cause du fait que le Code de la santé publique n'oblige pas les professionnels de santé au transfert de dossier médical. Assemblée nationale. Question n° 59945 de M. ROCHEBLOINE François, Député (Union pour la démocratie française-Alliance - Loire) au Ministre délégué à la santé. Question publiée au JORF du 16 avril 2001. P. 2224 et réponse au JORF du 6 Août 2001. P. 4601. http://questions.assemblee-nationale.fr/q11/11-59945QE.htm . Consulté le 26 mai 2014.

[698] L'ancien ministre de la santé, Philippe DOUSTE-BLAZY, lors de son audition sur le projet de loi relatif à l'assurance maladie espérait des économies de l'ordre de 3,5 milliards d'euros par an. *Rapport n° 424 (2003-2004) de M. Alain VASSELLE fait au nom de la Commission des affaires sociales*, déposé le 21 juillet 2004 au Sénat. http://www.senat.fr/rap/l03-424-2/l03-424-2_mono.html#toc4. Consulté le 26 mai 2014.

[699] CNIL. Délibération n°2004-054 du 10 juin 2004 portant avis sur le projet de loi relatif à la réforme de l'assurance maladie. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653162&fastReqId=1722276377&fastPos=1 Consulté le 26 mai 2014.

juin 2004, que pour sa mise en œuvre, des mesures appropriées[700] soient prises pour garantir la sécurité de la vie privée des individus et la confidentialité des données de santé constituant ce dossier. Le 13 Août 2004, la réforme de l'assurance maladie est validée par le Conseil Constitutionnel avec le projet de création du DMP. Il est de principe que tout traitement de données à caractère personnel contenues dans les dossiers médicaux électroniques doive respecter pleinement les règles de protection des données personnelles. La question qui se pose alors est de savoir: quelles sont les mesures techniques et juridiques prises par les responsables de la gestion du DMP pour assurer la protection attendue par la CNIL ? Ces dispositions ressortent dans la conception du DMP (paragraphe 1) prévu pour tenir sur un support électronique avec pour corollaire un cadre conventionnel (paragraphe 2) spécial imposé par l'intervention d'outils informatiques.

Paragraphe 1: La présentation du DMP

L'article 3 de la loi du 13 août 2004 relative à l'assurance maladie dispose : *« afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé, chaque bénéficiaire de l'assurance maladie dispose (...) d'un dossier médical personnel ... »*.
Le dossier médical personnel est créé soit à l'initiative du patient chez un professionnel de santé ou à l'accueil d'un établissement de soins (par le personnel d'accueil), soit à l'initiative d'un professionnel de santé avec le consentement du patient. Conformément à l'article L. 162-5-3, alinéa 3 du code de la sécurité sociale, le médecin traitant *« le médecin traitant participe à la mise en place et à la gestion du dossier médical personnel »* [701]. Dans tous les cas, lors de

[700] « *S'agissant des garanties appropriées qu'il incombe au législateur de prévoir, elle considère que les dispositions de l'article 2 doivent être complétées par une mention particulière indiquant que les données susceptibles d'être portées dans le dossier médical personnel sont couvertes par le secret professionnel tel que celui-ci est défini par le code pénal et que quiconque aura obtenu ou tenté d'en obtenir la communication en violation des dispositions du présent article s'exposera à des sanctions pénales, de même que quiconque aura modifié ou tenté de modifier les informations portées sur ce même dossier. »* Cnil. Délibération n°2004-054 du 10 juin 2004 portant avis sur le projet de loi relatif à la réforme de l'assurance maladie. http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653162. Consulté le 28 mai 2014.

[701]http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006073189&idArticle=LEGIARTI000006740743&dateTexte=&categorieLien=cid. Consulté le 28 mai 2014.

la création, le patient se voit remettre les éléments nécessaires à son accès au DMP via internet sans passer par les professionnels de santé. Le dossier médical personnel, récent en 2012 est encore beaucoup méconnu et la question se pose de savoir : qu'est-ce que le DMP et quelle est sa particularité par rapport aux dossiers voisins ?

A. Définition du DMP

Les dispositions législatives qui régissent actuellement le dossier médical personnel sont les articles L. 161-36-1 à L. 161-36-3-4 du code la sécurité sociale. Elles ont été transférées vers le code de la santé publique (articles L. 1111-14 à L. 1111-24 sous la section 3 intitulée dossier médical personnel et dossier pharmaceutique) par la loi n° 2009-879 du 21 juillet 2009 dite HPST. Ce transfert est un aspect de l'évolution que connaît ce dossier tant dans son concept que dans son contenu.

1. Le concept de dossier médical personnel : le résultat d'une évolution

Le DMP est l'aboutissement d'un long processus d'expérimentation de plusieurs types de dossiers médicaux sur support papier qui se sont révélés moins exploitables à long terme et moins pratiques. L'un des premiers dossiers médicaux français fut le carnet de santé destiné aux enfants. Il a été créé en 1945 et contenait uniquement des données biométriques de croissance, des renseignements sur les vaccinations effectuées et sur les affections aiguës de la première enfance. Pour les adultes, aucune loi n'obligeait les médecins à tenir un dossier médical jusqu'en 1970. La loi[702] n° 70 - 1318, suivi de son décret[703] d'application du 7 mars

« Les médecins traitants participent à la mise en place et à la gestion du DMP. Si l'assuré doit déclarer un médecin traitant à son organisme d'assurance maladie, plusieurs médecins peuvent jouer le rôle de médecins traitants dans le DMP. Un médecin traitant dans le DMP peut exercer des fonctions spécifiques : bloquer l'accès d'un professionnel de santé au DMP d'un de ses patients ; accéder aux documents masqués dans le DMP de ses patients, et le cas échéant, être en capacité de les assister en cas d'éventuelle volonté de démasquage d'un document masqué ; Consulté l'historique des actions menées dans le DMP de ses patients ». ASIP Santé, *Rapport d'activités 2010*. P. 26. http://esante.gouv.fr/sites/default/files/ASIP_RA2010.pdf. Consulté 13 février 2012

[702] Loi n° 70–1318 du 31 décembre 1970 portant réforme hospitalière publié au JORF du 3 janvier 1971. P. 00067.

1974 a rendu la tenue d'un dossier médical par les médecins, dans le cas de l'hospitalisation publique uniquement (ou pour les établissements privés participant au service public hospitalier), obligatoire[704] à compter du 31 décembre 1970.

La loi[705] du 30 juillet 1991 portant réforme hospitalière a mis à la charge des établissements de santé publique ou privée la tenue de dossiers médicaux. Son décret[706] d'application intervenu le 30 mars 1992 précisait qu'« un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé... ». Les médecins libéraux ont été associés aux obligations hospitalières de tenue de dossier de suivi médical par arrêté[707] du 25 novembre 1993 de la convention nationale des médecins suivi de la loi numéro 94-43 du 18 janvier 1994 relatif à la santé publique et à la protection sociale par ses articles L. 145–6 à L. 145 - 11. Ses conditions d'utilisation ont été précisées par le décret[708] du 1er mars 1995. Prévue pour être menée jusqu'au 31 juillet 1997, cette expérience a été interrompue en

---

http://www.legifrance.com/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19710103&numTexte=&pageDebut=00067&pageFin= Cette loi a été abrogée le 4 janvier 1992. Consulté 13 février 2012

[703] Décret n°74-230 du 7 mars 1974 relatif à la communication du dossier des malades hospitalisés ou consultants des établissements hospitaliers publics publié au JORF du 12 mars 1974. P. 02832. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=149ACEA76D57E03C011E0CD492060203.tpdjo02v_3?cidTexte=LEGITEXT000006062172&dateTexte=19920331 Ce décret a été abrogé le 1er Avril 1992. Consulté 13 février 2012

[704] D'ailleurs, une décision de la Chambre disciplinaire du Conseil national de l'ordre des médecins français datant du 22 septembre 1993 a blâmé un médecin pour défaut de tenue d'un dossier médical. En effet, *« considérant (...) que le Dr X (...) ne tenait pas pour ses malades de dossier médical sur lequel les observations auraient été portées au jour le jour,(...) qu'il peut donc être reproché au Dr X, à ce titre une insuffisance de surveillance technique, constitutive d'une violation de l'article 34 du code de la déontologie médicale ; qu'une telle faute... est contraire à l'honneur et par suite exclue du champ d'application de l'article(...) portant amnistie(...) Il sera fait une juste appréciation de la gravité des faits(...) en lui infligeant la peine du blâme »*. Docteur PRADEAU, F. *Le dossier du patient dans les établissements de santé : tenue, contenu, archivage et communication.* P.1. http://membres.multimania.fr/pradeau/exposes/DosMed/dossier_medical_synthese_0110 15.pdf. Consulté le 2 janvier 2012.
Cette décision a été confirmée en 1995 par le Conseil d'État. CE. 154253 du 28 juin 1995 inédit au recueil Lebon. http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CÉTATEXT000007881812&fastReqId=755892474&fastPos=2. Consulté le 2 janvier 2012.

[705] Article L. 710–2 de la loi n° 91- 48 du 31 juillet 1991 portant réforme hospitalière (1) publiée au JORF n°179 du 2 août 1991 p. 10255. NOR: SPSX9000155L.

[706] Article R. 710-2-1 du décret n° 92-329 du 30 mars 1992. publié au JORF n°78 du 1 avril 1992 p. 4607. NOR: SANH9200522D.

[707] Ministère des affaires sociales de la santé et de la ville. Arrêté du 25 novembre 1993 portant approbation de la convention des médecins (article 21) publié au JORF du 26 novembre 1993. p. 16297.

[708] Décret n° 95-234 du 1er mars 1995 relatif au dossier de suivi médical et au carnet médical institué par l'article 77 de la loi numéro 94 - 43 du 18 janvier 1994 relatif à la santé publique et à la protection sociale publié au JORF n° 54 du 4 mars 1995. p. 03448. NOR: SPSS9500441D.

1996 à la faveur d'une autre portant sur le carnet de santé[709]. L'article[710] L. 162-1-1 du code de la sécurité sociale précisait que le carnet de santé doit être délivré à chaque patient de plus de 16 ans[711] qui devrait obligatoirement le présenter lors des consultations. Mais le support papier constitue une des faiblesses[712] de ce carnet[713] à l'ère du développement des technologies de l'information et de la communication. Ainsi, sans abroger le contenu de l'article 162-1-1, les pouvoirs publics ont opté pour une informatisation des données médicales car « *un dossier médical informatisé est à la fois plus lisible et plus précis qu'un dossier manuel*[714] ». L'informatisation des dossiers médicaux permet un meilleur suivi de l'état de santé des patients et donc d'assurer une meilleure qualité de soins.

[709] Décret n° 96-925 du 18 octobre 1996 relatif au carnet de santé institué par l'article L. 162-1-1 du code de la sécurité sociale et modifiant ce code (deuxième partie: Décrets en Conseil d'État) publié au JORF n°246 du 20 octobre 1996. P. 15429. NOR: TASS9623355D.

[710] Actuel article R. 162-1-1 du code de la sécurité sociale.

[711] « *Art. R. 162-1-1. - En application de l'article L. 162-1-1, un carnet de santé est délivré à l'assuré social et à chacun de ses ayants droit âgés de plus de seize ans par l'organisme d'assurance maladie dont il relève pour le service des prestations ; il est renouvelé en tant que de besoin. «Le carnet comporte les éléments nécessaires à l'identification de l'assuré ou de son ayant droit, à l'exclusion de son nom patronymique. «Art. R. 162-1-2. - Tout médecin appelé à donner des soins à un patient auquel a été attribué le carnet de santé institué par l'article L. 161-1-1 doit porter sur ce carnet, dans le respect des règles déontologiques qui lui sont applicables, la date des soins, son cachet et sa signature et, sauf opposition du patient, les constatations pertinentes pour le suivi médical de ce patient, notamment la mention des actes effectués ainsi que celle des examens et traitements prévus à l'article L. 324-1.* » http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000746502&fastPos=1&fastReqId=711824834&categorieLien=id&oldAction=rechTexte. Consulté le 2 janvier 2012.

[712] Le support papier pose un double problème : il favorise le maintien d'une prise en charge cloisonnée des patients. Le transfert du malade d'une structure à une autre ne permet pas la transmission du dossier médical original qui le concerne. L'établissement qui produit une information de santé relative à un patient hospitalisé doit conserver l'original du document sur lequel figure cette information (circulaire n° 394 du 11 août 1978 relatif à la communication des dossiers médicaux des malades à leur médecin traitant ou à un autre établissement hospitalier). Les services ministériels énoncent qu'« qu'il est fréquent que des médecins traitants successifs ou divers spécialistes soient appelés à avoir le même malade, l'hôpital doit donc être à même d'adresser à tout moment à ces médecins des copies de la totalité ou d'une partie des pièces ». DUPUY, Olivier. *Le dossier médical et dossier médical personnel, supports complémentaires ou concurrents ? in Xe séminaire d'actualité de droit médical*. P 53.

[713] Il faut noter que le carnet de santé délivré lors de la déclaration de naissance de tout enfant (article L. 2132 - 1 du code de la santé publique) est maintenu et l'article L. 1111 - 22 permet l'utilisation des informations contenues dans le dossier médical personnel pour l'alimentation de ce carnet.

[714] DEGOULET, Patrice et FIESCHI, Marius. *Traitement de l'information médicale. Méthodes et applications hospitalières.* Paris, Masson, 1991. Chapitre 10 : informatisation des dossiers médicaux. 27 mars 2010 par USMCS. http://www.lescentresdesante.com/article115.html Consulté le 17 janvier 2012.

Partant du principe de l'adjonction d'un volet médical à la carte vitale prévue par l'ordonnance[715] n° 96-345 du 24 avril 1996, la première solution a été d'envisager d'intégrer le dossier médical de chaque patient à sa carte vitale. Mais, face à certaines incertitudes[716] d'ordre technique et sécuritaire ce projet a également été abandonné. Mme Jeannette GROS[717] répondait par la négative à la question de savoir si l'on ferait figurer le dossier médical sur la carte vitale 2 en précisant que même : « *les soins d'urgence ne seraient finalement plus sur la carte vitale elle-même (...) Celles-ci seraient stockées soit sur d'énormes serveurs (...) soit à travers des données dispatchées en ligne*[718] ».

Selon l'Agence nationale d'accréditation et d'évaluation en santé (ANAES[719]), le dossier médical peut se définir comme « *une mémoire écrite des informations cliniques, biologiques, diagnostiques et thérapeutiques d'un malade, à la fois individuelle et collective, constamment mise à jour*[720] ». Mais, selon le rapport[721] de la mission pour la relance du projet

---

[715] Article L. 161–31. II. de l'ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins. NOR:TASX9600042R publiée au JORF n° 98 du 25 avril 1996 p. 6311. «*Cette carte comporte un volet médical destiné à recevoir les informations pertinentes nécessaires à la continuité et à la coordination des soins mentionnées à l'article L. 162-1-4.*»

[716] « Les pouvoirs publics ont souhaité faire évoluer le contenu de la part d'assurance-maladie. Plusieurs solutions ont été envisagées. Dans son rapport du 20 mars 2002, le Conseil économique et social regroupe celles-ci en trois axes: la solution la plus large consisterait à porter l'intégralité du dossier médical de la personne sur la carte vitale 2, la solution la plus étroite consistait à intégrer sur la carte vitale 2 le même contenu que sur la carte vitale 1, à savoir : les informations sur les droits de la personne au regard de l'assurance maladie. S'agissant de l'hypothèse qui consiste à insérer l'intégralité du dossier médical sur la carte vitale, le Conseil économique et social constate que cela est difficilement envisageable. Les obstacles sont d'ordre technique : il apparaît que la carte ne peut contenir qu'un nombre limité de données (...) Se pose également la question de la sauvegarde du dossier. (...) S'agissant de la solution médiane, le Conseil économique et social remarque que continuera à se poser le problème du coût élevé de la carte et de la transmission de ces informations lors de son renouvellement en cas de perte. En fait, un certain nombre de difficultés techniques n'ont pas trouvé de réponse : les modalités de mise à jour des données déjà contenues sur la carte». DUPUY, Olivier. *Le dossier médical et dossier médical personnel, supports complémentaires ou concurrents ? in Xème séminaire d'actualité de droit médical*. P 49-50.

[717] Jeannette GROS, membre du Conseil économique et social et administratrice de la Mutualité sociale agricole (MSA) en tant qu'agricultrice, a réalisé le rapport sur les nouvelles technologies et la santé le 20 mars 2002, à la demande du premier ministre. Elle a présenté ce rapport les 9 et 10 avril 2002 devant le Conseil économique et social.

[718] BLIN, Marc. *Où mènent les nouvelles technologies.* Professions santé infirmier infirmière n° 37 de mai 2002. P. 6.

[719] Aujourd'hui HAS (Haute autorité de santé)

[720] Agence nationale d'accréditation et d'évaluation en santé (ANAES). *Le dossier du patient en ergothérapie.* Mai 2001. P.16. http://www.hassante.fr/portail/upload/docs/application/pdf/ergoth_rap.pdf . Consulté le 10 août 2012.

[721] GAGNEUX, Michel. Rapport de la mission de relance du projet de dossier médical personnel. *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé*. 23 Avril 2008. P. 25. www.sante.gouv.fr/IMG/pdf/Rapport_DMP_mission_Gagneux.pdf. Consulté le 10 août 2012.

du dossier médical personnel, le concept actuel de dossier médical personnel est une vision évoluée de la fonction de dossier médical. Il est passé de la phase de simple dossier mémoire à une phase de dossier personnel en passant par une étape plus dynamique de dossier partagé. A l'origine, il avait été conçu pour servir d'aide-mémoire au professionnel de santé quant aux antécédents de son patient, qu'il soit sur support papier ou un film ou même électronique (sur le disque dur de l'ordinateur du professionnel de santé). Un seul patient a ainsi, plusieurs dossiers médicaux. Pourtant, le développement de la société a contribué à pencher, désormais, pour un dossier médical partagé tant entre professionnels qu'entre professionnels et patients. Cette fonction est plus efficacement remplie par la numérisation des données médicales du patient et leur partage. Dans un premier temps, le dossier électronique fut nommé «dossier médical partagé». «*La logique d'un dossier électronique partagé réside dans la capacité donnée à chaque professionnel ou entité de santé, sous réserve du consentement du patient : d'accéder à des informations produites et détenues par d'autres, et éventuellement stockées ailleurs ; de pouvoir les consulter et les exploiter selon une présentation et une ergonomie adaptées à sa pratique ; d'alimenter le dossier partagé en données utiles à la coordination des soins, sous sa responsabilité et à partir de son poste de travail.*[722]»

Mais, tel qu'envisagé, le dossier médical doit être avant tout la propriété du patient même s'il est « *configuré par et pour les professionnels de santé*[723] ». Il est créé avec son consentement[724] et dans le respect de ses droits. En principe, aucun mouvement ne peut y être effectué sans l'accord de ce dernier. C'est pourquoi, le dossier médical partagé a, finalement, été dénommé « dossier médical personnel ». La mission de relance du DMP définit alors le dossier médical personnel comme « *une présentation particulière, accessible aux patients*

[722] Ibidem. P. 27.

[723] Ibidem. P. 30.

[724] Article L 1111-14 CSP: «*Ce dossier médical personnel est créé auprès d'un hébergeur de données de santé à caractère personnel agréé dans les conditions prévues à l'article L. 1111-8» : « Les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée. »* http://www.legifrance.gouv.fr/affichCode.do;jsessionid=3D4751935737C1CCE076B4DBA9189639.tpdjo10v_1?idSectionTA=LEGISCTA000020890569&cidTexte=LEGITEXT000006072665&dateTexte=20120106. Consulté le 10 août 2012.

sans intermédiaire médicale, du dossier patient partagé institué aux fins d'amélioration de la qualité, de la coordination et de la continuité des soins[725]*. »*

La définition du dossier médical personnel a jusque-là été laissée à l'appréciation des professionnels ou de l'équipe soignante, selon la pratique, la représentation ou les conditions d'exercice du professionnel de santé. Il peut, alors, être compris de plusieurs manières. Le rapport[726] GAGNEUX en énumère quelques unes : un dossier de suivi médical[727], un dossier médical[728], une fiche d'observation[729], un dossier patient[730], un dossier commun minimum, un dossier de spécialité, un dossier médical de synthèse, un dossier de réseau[731], etc... Mais, le DMP est différent de tous ces dossiers. Il ne se substitue pas aux dossiers médicaux des professionnels même s'il contribue à les faire évoluer. *« Le DMP n'a pas vocation à se substituer aux dossiers papier ou informatisés établis dans les cabinets des médecins libéraux et dans les établissements de santé, mais à s'y ajouter*[732]*. »* Il servira d'espace d'intégration

[725] GAGNEUX, Michel. Rapport de la mission de relance du projet de dossier médical personnel. *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé*. 23 Avril 2008. P. 35. www.sante.gouv.fr/IMG/pdf/Rapport_DMP_mission_Gagneux.pdf. Consulté le 10 août 2012.

[726] GAGNEUX, Michel. *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*. 23 avril 2008. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//084000279/0000.pdf . Consulté le 10 août 2012.

[727] Loi du 18 janvier 1994, dossier supprimé par les ordonnances de 1996 (Rapport GAGNEUX p. 25 précité).

[728] Le dossier cité par les article R. 1112-2 et suivants du CSP modifiés par le décret 2006-119 du 6 février 2006 relatif aux directives anticipées prévues par la loi n° 2005-370 du 22 avril 2005 relative aux droits des malades et à la fin de vie et modifiant le code de la santé publique (dispositions réglementaires). JORF n° 32 du 7 février 2006. p. 1973. Texte n° 32. NOR: SANP0620219D.

[729] L'article R. 4127-45, alinéa 1er CSP (Article 45 du code de déontologie médicale) dispose que *« le médecin doit tenir pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte tous les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques* ».

[730] Le dossier auquel fait référence l'ANAES dans le cadre de son référentiel d'accréditation est le « dossier patient ». *« Le dossier du patient, document récapitulatif et de synthèse, permet l'évaluation de la qualité des pratiques professionnelles médicales et soignantes, partie intégrante de l'activité des professionnels de santé. »* Service d'évaluation des pratiques de l'ANAES. *Evaluation des pratiques professionnelles dans les établissements de santé. Dossier patient : Amélioration de la qualité, de la tenue et du contenu*. Juin 2003. P. 3. http://www.hassante.fr/portail/upload/docs/application/pdf/200908/dossier_du_patient_amelioration_de_la_qualite_de_la_tenue_et_du_contenu_-_reglementation_et_recommandations_-_2003.pdf. Consulté le 10 août 2012.

[731] GAGNEUX, Michel. *Les concepts: dossier patient partagé, dossier du professionnel et dossier médical personnel* in Bulletin juridique du praticien hospitalier. Septembre 2008. N° 110. P. 15.

[732] CNIL. *La CNIL autorise le déploiement du dossier médical personnel sur l'ensemble du territoire*. 14 décembre 2010. Disponible sur: http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-autorise-le-deploiement-du-dos sier-medical-personnel-sur-lensemble-du-territoire/. Consulté le 3 mars 2011.

permettant au praticien de passer aisément, sans duplication des saisies de son dossier « métier » au « dossier partagé[733] ».

Les finalités du dossier médical personnel ont été déterminées dès le départ et le Conseil Constitutionnel a indiqué en 2004[734] qu'il servira, d'une part, à améliorer la qualité des soins, et, d'autre part, à réduire le déséquilibre financier de l'assurance maladie mais sa définition n'a pas fait l'objet d'une telle précision. Le DMP n'a pas de définition légale. Il est juste présenté à travers son objectif et son fonctionnement par les organismes intervenant dans son pilotage. Ainsi, est-il défini par la CNIL comme un « *dossier informatisé créé pour chaque bénéficiaire de l'assurance maladie qui le souhaite. Il permet le regroupement et le partage entre les professionnels et établissements de santé des informations jugées utiles à la coordination des soins »*[735]. Quant à l'ASIP[736] santé, elle le présente comme «*un dossier qui rassemble les informations médicales d'un patient nécessaires à la coordination des soins, utilisé sous la forme d'un service électronique accessible grâce aux technologies informatiques. C'est un service public, proposé gratuitement à tous les bénéficiaires de l'assurance maladie[737]».* Quatre systèmes d'information se complètent pour permettre au DMP de proposer plusieurs services aux utilisateurs (patients et professionnels de santé). Il s'agit de:

- « Système d'information DMP : au cœur du dispositif, il permet de créer, d'alimenter et de consulter des DMP. Ce système interagit avec les logiciels de professionnels de santé DMP-compatibles et propose un accès Web aux professionnels de santé comme aux

[733] GAGNEUX, Michel. 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. 23 avril 2008. p. 27 http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/ /084000 279/0000.pdf. Consulté le 3 mars 2011.

[734] Conseil constitutionnel. Décision n° 2004-504 DC du 12 août 2004. Considérant n° 6. JORF du 17 août 2004, p. 14657. Recueil, p. 153. *« 6. Considérant, en premier lieu, qu'aux termes du nouvel article L. 161-36-1 du code de la sécurité sociale, le dossier médical personnel est institué « afin de favoriser la coordination, la qualité et la continuité des soins, gages d'un bon niveau de santé »* http://www.Conseil-constitutionnel.fr/Conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/2004/2004-504-dc/decision-n-2004-504-dc-du-12-aout-2004.909.html. Consulté le 10 décembre 2011.

[735] CNIL. La CNIL autorise le déploiement du dossier médical personnel sur l'ensemble du territoire. 14 décembre 2010. http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-autorise-le-deploiement-du-dossier-medical-personnel-sur-lensemble-du-territoire/ Consulté le 10 décembre 2011.

[736] L'ASIP santé étant l'organisme en charge du pilotage du projet DMP, la plupart des informations d'ordre technique ou pratique données dans le cadre de cette étude seront tirées de ses publications.

[737] ASIP Santé, Rapport d'activités 2010. PP 26 et 28. http://esante.gouv.fr/sites/default/files/ASIP_RA2010.pdf Consulté le 10 décembre 2011.

patients[738]. Conçu sur la base d'exigences fortes d'ergonomie, de fonctionnalité et de confidentialité des données, il est surveillé 24 heures sur 24 et soumis quotidiennement à des tests de sécurité et de performance.

- Système d'information Portail de communication dédié au DMP : Il présente l'ensemble du système DMP, sous un angle informatique et pédagogique, propose des informations pratiques destinées aux internautes, patients ou professionnels de santé qui cherchent à mieux comprendre ce service. C'est aussi la porte d'entrée de l'accès Web au système d'information DMP, pour le patient comme pour le professionnel de santé.
- Système d'information Support : Il est destiné à être utilisé par le service d'assistance aux utilisateurs, DMP Info Service, un centre de relations avec les usagers qui répond à leurs interrogations, formulées par téléphone ou sur le site Internet.
- Système d'information Pilotage : Il permet d'agréger les différentes informations statistiques remontées par les trois SI précédents, afin de disposer d'une vision complète du fonctionnement du dispositif.[739] »

Cette absence de définition légale du dossier médical personnel crée une imprécision qui constitue « *un frein au développement du projet et à l'adhésion des différents acteurs*[740] ». Présenté comme un dossier médical électronique a vocation à être à la fois personnel[741] et partagé, il crée des inquiétudes sur la manière de l'aborder. Son objectif est de renforcer le rôle du patient comme acteur de sa santé, en facilitant l'accès de celui-ci à ses données de santé et d'améliorer la coordination et la qualité des soins prodigués, en favorisant la communication de données entre professionnels de santé. Les députés estiment que ce double rôle personnel et partagé gagnerait à être clarifié « *pour délimiter les champs de compétences*

[738] L'accès web au système DMP a été ouvert dès le 5 janvier 2011 tandis que l'accès web des patients l'est depuis Avril 2011.

[739] ASIP Santé, Rapport d'activités 2010. PP 26 et 28. http://esante.gouv.fr/sites/default/files/ASIP_RA2010.pdf Consulté le 10 décembre 2011.

[740] LASBORDES, Pierre. Rapport n° 1847 (Assemblée nationale), n° 567 (Sénat) sur le dossier médical personnel (DMP) : quel bilan d'étape pour quelles perspectives ? (Compte rendu de l'audition publique du 30 avril 2009) P. 8.

[741] *« Le patient garde à tout moment la possibilité de le fermer, de supprimer tout ou partie des documents qu'il contient, ou de masquer certaines données de santé. De ce point de vue, le DMP, qui est à la fois personnel et partagé, est conforme aux droits des patients qui posent comme principes l'information, le consentement et la confidentialité. »* Site officiel du DMP. *Qu'est-ce que le DMP ?* www.dmp.gouv.fr. Consulté le 09 janvier 2012.

respectifs et les usages qui seront assignés au dossier médical même si ces derniers sont conçus comme évolutifs[742]*» ;* évolutions qui touchent également le contenu même du DMP.

2. Le contenu évolutif du dossier médical personnel

Le contenu du dossier médical a retenu l'attention du législateur au cours de ces quatre dernières décennies mais sa composition et son organisation ont souvent été modifiées en fonction du type de dossier médical. Avant 2002, le contenu d'un dossier de patient dépendait à la fois des circonstances de la prise en charge de ce dernier et des règles d'organisation adoptées par l'établissement ou le professionnel. Ainsi, le contenu du dossier médical constitué en établissement de santé était plus explicite que celui du médecin de ville. La circulaire[743] du 11 Août 1978 annexé au décret[744] du 14 janvier 1974 relatif au fonctionnement des centres hospitaliers précisait à l'article 23-17[745] la composition détaillée

[742] Idem

[743] Circulaire n°394 du 11 Août 1978. Bulletin officiel 78/41. p. 15546.

[744] Décret n°74-27 du 14 janvier 1974 relatif aux règles de fonctionnement des centres hospitaliers et des hôpitaux locaux JORF du 16 janvier 1974 p. 603.

[745] Article 23-17 de la circulaire n° 394 du 11 août 1978
« *Avec l'accord du malade, un dossier médical doit être adressé au médecin de ville ou au médecin d'un établissement public ou privé, qui en fait la demande.*
Ce dossier est constitué par un membre de l'équipe médicale hospitalière, à partir du dossier médical complet conservé par l'établissement. Il doit comporter la reproduction des pièces suivantes :
- la fiche d'identification du malade ;
- la fiche indiquant les motifs de l'hospitalisation ;
- les conclusions de l'examen initial ;
- le compte rendu de l'hospitalisation ;
- la fiche de sortie ;
- l'ordonnance à la sortie du malade.
Seront jointes à ces six documents, si le malade au cours de son hospitalisation a fait l'objet des soins ou examens ci-dessous énumérés, les copies des :
- comptes rendus radiologiques ;
- comptes rendus opératoires ;
- résultats des électrogrammes ;
- et s'ils ne figurent pas, de façon détaillée, dans le compte rendu d'hospitalisation, des résultats cumulatifs des examens biologiques (anatomie et cytologie pathologiques, biochimie, hématologie, microbiologie, antibiogrammes, etc.).
Seuls sont à retenir par le médecin hospitalier pour entrer dans le dossier destiné au médecin désigné par le malade des comptes rendus et résultats d'examens ayant eu valeur probante dans le diagnostic et la thérapeutique. »
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=10906F3B7D0823EBCBAB5324ACE11A9D.tpdjo12v_1?cidTexte=LEGITEXT000006062174&dateTexte=20030526. Consulté le 10 décembre 2011.

du dossier médical d'un centre hospitalier. Ce fut le premier texte dans le processus d'uniformisation du contenu des dossiers médicaux. Ce décret a été abrogé[746] le 21 mai 2003. Le décret[747] de 1992 qui va suivre ne concernera pas uniquement les dossiers des personnes hospitalisées dans les centres hospitaliers mais tous les établissements publics ou privés de santé. Il sera également détaillé. Mais, pour tenir compte de toutes les informations relatives au patient même en dehors des cas d'hospitalisation, un dossier de suivi médical est mis en place par la loi[748] du 18 janvier 1994 relative à la santé publique et à la protection sociale.

Le contenu de ce dossier de suivi médical est donné à l'article L. 145-8: *« Dans le respect des règles déontologiques applicables, les chirurgiens-dentistes, les sages-femmes, les médecins et les établissements de santé publics et privés communiquent au médecin mentionné à l'article L. 145-7 une copie ou une synthèse des informations médicales qu'ils détiennent concernant le patient et qu'ils estiment utile d'insérer dans le dossier de suivi médical.[749] ».* Mais le décret[750] du 29 avril 2002 ne détaillera que les dossiers des patients hospitalisés. En effet, ce règlement indiquait qu' *« un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé. Ce dossier contient au moins les éléments suivants, ainsi classés :*
1° les informations formalisées recueillies lors de consultations externes dispensées dans l'établissement, lors de l'accueil au service des urgences ou au moment de l'admission et au cours du séjour hospitalier, et notamment :

---

[746] Décret 2003-462 du 21 mai 2005 (article 5) relatif aux dispositions réglementaires des parties I, II et III du code de la santé publique publié au JORF n° 122 du 27 mai 2003. p. 37006. Texte n° 3. NOR: SANP0321523D.

[747] Article 9, R.710-2-2 du décret n° 92-329 du 30 mars 1992 relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santé publics et privés et modifiant le code de la santé publique (deuxième partie: Décrets en Conseil d'État) JORF n°78 du 1 avril 1992 p. 4607. NOR: SANH9200522D.

[748] Loi n° 94-43 du 18 janvier 1994 relative à la santé publique et à la protection sociale (1) publiée au JORF n°15 du 19 janvier 1994 p. 960. NOR: SPSX9300136L.

[749] Article L. 145-8 de la loi n° 94-43 du 18 janvier 1994 relative à la santé publique et à la protection sociale (1). NOR: SPSX9300136L publiée au JORF n° 15 du 19 janvier 1994 p. 960.

[750] Décret n° 2002-637 du 29 avril 2002 relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 1111-7 et L. 1112-1 du code de la santé publique. NOR: MESP0221143D. JORF n° 101 du 30 avril 2002 p.7790. Texte n° 8.
Ce texte a été abrogé le 21 mai 2003. Mais, il est repris par l'article R. 1112-2 du code de la santé publique tel que modifié par le décret 2006-119 du 6 février 2006 relatif aux directives anticipées prévues par la loi n° 2005-370 du 22 avril 2005 relative aux droits des malades et à la fin de vie et modifiant le code de la santé publique (dispositions réglementaires). JORF n° 32 du 7 février 2006. P. 1973. Texte n° 32. NOR: SANP0620219D.
La modification ajoute un point q) aux dispositions antérieures du 1°: *« q) Les directives anticipées mentionnées à l'article L. 1111-11 ou, le cas échéant, la mention de leur existence ainsi que les coordonnées de la personne qui en est détentrice ».*

a) la lettre du médecin qui est à l'origine de la consultation ou de l'admission ;

b) les motifs d'hospitalisation ;

c) la recherche d'antécédents et de facteurs de risques ;

d) les conclusions de l'évaluation clinique initiale ;

e) le type de prise en charge prévue et les prescriptions effectuées à l'entrée ;

f) la nature des soins dispensés et les prescriptions établies lors de la consultation externe ou de passage aux urgences ;

g) les informations relatives à la prise en charge en cours d'hospitalisation : état clinique, soins reçus, examens para-cliniques, notamment d'imagerie ;

h) les informations sur la démarche médicale, adoptée dans les conditions prévues à l'article L. 1111 - 4 ;

i) les dossiers d'anesthésie ;

j) le compte rendu opératoire ou d'accouchement ;

k) le consentement écrit du patient pour les situations où ce consentement est requis sous cette forme par voie légale ou réglementaire ;

l) la mention des actes transfusionnels pratiqués sur le patient et, le cas échéant, copie de la fiche d'incident transfusionnel mentionné au deuxième alinéa de l'article R. 666 - 12 - 24 ;

m) les éléments relatifs à la prescription médicale, à son exécution et aux examens complémentaires ;

n) le dossier de soins infirmiers ou, à défaut, les informations relatives aux soins infirmiers ;

o) les informations relatives aux soins dispensés par les réseaux professionnels de santé ;

p) la correspondance échangée entre professionnels de santé.

2° les informations formalisées établies à la fin du séjour : elle comporte :

a) le compte rendu d'hospitalisation et la lettre rédigée à l'occasion de la sortie ;

b) la prescription de sortie et les doubles d'ordonnance de sortie ;

c) les modalités de sortie (domicile, autres structures) ;

d) la fiche de liaison infirmière.

3° Informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant de tels tiers.

Sont seules communicables les informations énumérées au 1° et 2° »

Ce décret a été abrogé le 21 mai 2003. Les dispositions[751] législatives en vigueur restent encore avares en précisions s'agissant des informations devant constituer un dossier patient en dehors des hospitalisations et chez les médecins de ville. Il me paraît donc nécessaire que l'on interroge d'autres sources pour en savoir davantage.

Pour répondre au recours exercé par les députés portant sur leurs craintes d'atteinte à la vie privée du fait du fonctionnement du dossier médical personnel, le Conseil Constitutionnel a rappelé *« qu'il comportera notamment « des informations qui permettent le suivi des actes et prestations de soins » ainsi qu'un « volet spécialement destiné à la prévention » ; que, pour atteindre cet objectif, le nouvel article L. 161-36-2 prévoit que chaque professionnel de santé inscrira au dossier « les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge*[752] *»*. L'article L. 161-36-2 du code de la sécurité sociale dispose : « *(…) 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, notamment des informations qui permettent le suivi des actes et prestations de soins. Le dossier médical personnel comporte également un volet spécialement destiné à la prévention »*. Le dossier médical personnel contient donc «*les données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins*[753] ». Quelles sont ces données ?

La liste établie par l'article L. 161-36-2 est précédée de «*notamment*», un adverbe introduisant un ou des exemple(s). La liste n'est donc pas exhaustive. Le reste du contenu pourra alors être recherché dans des publications administratives dont les informations délivrées par le «*service unique d'accueil dématérialisé dénommé « portail du dossier médical personnel», destiné aux bénéficiaires de l'assurance maladie et aux professionnels de santé*[754] ». Le dépliant[755] d'information des professionnels proposé par le portail du dossier

---

[751]Article L. 1111.15 du code de la santé publique : *«(…) à l'occasion du séjour d'un patient, les professionnels de santé habilités des établissements de santé reportent sur le dossier médical personnel les principaux éléments résumés relatifs à ce séjour ».*

[752] Conseil constitutionnel. Décision n° 2004-504 DC du 12 août 2004. Considérant n° 6. JORF du 17 août 2004, p. 14657. Recueil, p. 153. http://www.Conseil-constitutionnel.fr/Conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/2004/2004-504-dc/decision-n-2004-504-dc-du-12-aout-2004.909.html. Consulté le 7 janvier 2012.

[753] Article L. 1111-8, alinéa 1. CSP

[754] Article L. 1111-19, alinéa 1 CSP. Ce portail permet *« un accès unique non seulement au DMP, mais à un ensemble de dossiers qui ont vocation à intégrer le DMP ou à être consultables simultanément, comme le*

médical personnel indique que le DMP ne remplace pas les dossiers professionnels et n'a pas vocation à être exhaustif. Il contient les documents que les professionnels jugeront utiles à la coordination des soins de leurs patients[756]. Ce sont *des informations personnelles nécessaires au suivi du patient: traitements, antécédents médicaux et chirurgicaux, compte rendus hospitaliers et de radiologie, analyses de laboratoire*. Si ces indications apportent un peu plus de clarté que les termes de l'article L. 161-36-2 du code de la sécurité sociale précité, elles demeurent un peu vagues. Elles sont moins précises sur la forme et la structure du dossier. Les professionnels pourront, ainsi être libres du choix de leur contenu comme ils en ont eu l'habitude. Mais, face à l'objectif de coordination des soins que vise le DMP, il faut craindre que cette grande ouverture ne soit à l'origine d'un désordre quant à son contenu. Chaque professionnel serait tenté d'y mettre ce qu'il voudra et les éléments de contenu risquent d'être différents d'un patient et/ou, surtout, d'un professionnel de la même spécialité à l'autre. Certains seront probablement moins professionnels que d'autres et cela pourrait avoir pour conséquence d'être un frein à la coordination des soins recherchée.

La rubrique[757] consacrée au contenu d'un dossier médical sur le portail du service public (selon sa mise à jour datant du 31 juillet 2009), propose un contenu variable fortement inspiré du décret de 2002 précité en distinguant les informations communicables des informations non communicables avant et après 2002. « *Depuis 2002, le dossier doit être structuré en trois parties :*

---

dossier communicant de cancérologie, le dossier pharmaceutique et les dossiers de réseaux de santé ». DOOR, Jean-Pierre. *Rapport sur le dossier médical personnel*. 29 janvier 2008. p. 68.

[755] GIP ASIP Santé. *L'essentiel sur le DMP au service de votre pratique professionnelle*. www.dmp.gouv.fr

[756] le DMP est un dossier médical destiné à la coordination des soins. Tout au long du parcours de soins du patient, les professionnels de santé qu'il consultera en ville et à l'hôpital déposeront dans le DMP avec l'accord du patient, les comptes-rendus de ses consultations et séjours et les résultats d'examens. L'ensemble de ces informations constituera progressivement l'histoire médicale du patient. Chacun des professionnels de santé doit tenir à jour un dossier médical concernant son patient et doit compléter ce dossier à chacune des rencontres avec lui. Il existe, ainsi, un dossier médical du médecin généraliste, un dossier médical du spécialiste, du biologiste, de l'hôpital ou de la clinique que le patient a consulté. Chacun de ces dossiers médicaux professionnels est détenu et mis à jour par le professionnel ou l'établissement de santé. Dans chacun de ces dossiers, certaines informations sont utiles à la coordination des soins et ce sont celles-ci que les professionnels déposeront dans le DMP. Le DMP est donc différent de tous ces dossiers médicaux détenus par les professionnels ; lui seul regroupe l'ensemble des informations utiles à la coordination du parcours de soins présentes dans les différents dossiers professionnels. www.dmp.gouv.fr

[757] Service public. Contenu du dossier médical. http://m.vosdroits.service-public.fr/particuliers/F1220.xhtml Consulté le 13 février 2012

- *la première partie doit contenir les informations formalisées recueillies lors des consultations externes dispensées dans l'établissement, au service des urgences ou au moment de l'admission et au cours du séjour hospitalier ;*
- *la deuxième partie doit contenir les informations formalisées établies à la fin du séjour;*
- *la troisième partie doit contenir le cas échéant, les informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou qu'elles concernent de tels tiers.*

Les informations contenues dans cette troisième partie du dossier ne sont pas communicables[758].»

L'ASIP santé propose une représentation synthétique et technique du contenu DMP dans son rapport[759] d'activités de 2010. *«Le DMP est structuré en huit espaces : espace de synthèse et de données médicales générales, traitement et soins, compte rendu, imagerie médicale, analyses de laboratoire, prévention, certificats et déclarations, espace d'expression personnelle du patient ».* Cette présentation donne une idée plus élaborée, mieux organisée du contenu[760] du DMP tel qu'envisagé dès la loi de 2004[761], que nous espérons voir s'améliorer avec le décret DMP, prévu pour la fin de la première phase de généralisation du DMP en 2013. Il est attendu du décret DMP qu'il fournisse une liste exhaustive des informations que le dossier sera susceptible de recevoir et des précisions sur l'organisation de l'information du point de vue de l'usage. *Les professionnels de santé ont besoin d'une information aussi exhaustive que possible, mais suffisamment hiérarchisée pour éviter l'accumulation des*

[758] Idem

[759] ASIP Santé, *Rapport d'activités 2010*. p. 26. http://esante.gouv.fr/sites/default/files/ASIP_RA2010.pdf Consulté le 13 février 2012.

[760] « *Le DMP informatisé est appelé à recevoir outre leurs données d'identification, l'ensemble des informations « concourant à la coordination, la qualité, la continuité des soins et la prévention ». Concrètement, ceci recouvre :*
- les données médicales générales (antécédents, allergies et intolérances reconnues, vaccinations, historique de consultation, synthèse, etc.) ;
- Les données de soins (résultats d'examens, comptes rendus d'actes diagnostiques et thérapeutiques, bilans, traitements prescrits et administrés, protocoles de soins, etc.) ;
- les données de prévention (facteurs de risques individuels, compte rendu, traitement préventif, etc.) ;
- des documents d'imagerie médicale ;
- un espace d'expression du titulaire. »
Mission interministérielle de revue de projet sur le dossier médical personnel (DMP). *Rapport sur le dossier médical personnalisé (DMP)*. 8 Novembre 2007. p.1. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//074000713/0000.pdf. Consulté le 13 février 2012.

[761] Le DMP tel que prévu en 2004 est appelé à évoluer et être destiné, à terme, à unifier toutes les données de santé relatives à une même personne dans un seul document.

données inutiles[762] (à un certain moment). En fonction de leur spécialité, certains attendent de retrouver dans le DMP des informations bien spécifiques et dans un souci d'homogénéité, il serait important de former les futurs professionnels à des méthodologies de rédaction de contenu de DMP[763]. Ces formations se révèlent d'autant plus importantes que ce dossier paraît être un modèle particulier distinct des autres dossiers de santé.

B. Le DMP et les autres dossiers électroniques

Le DMP est aussi différent des autres dossiers médicaux français que des dossiers médicaux ayant été expérimentés à l'étranger.

1. Le dossier médical personnel et les autres dossiers médicaux français

Le dossier médical personnel n'est pas le seul dossier électronique qui ait été mis en place par la politique de santé publique et de sécurité sociale en France. Non seulement, il est l'aboutissement d'une succession de dossiers médicaux, comme nous l'avons déjà indiqué, mais il est également proche d'autres dossiers partagés qui ont eux, pu avancer un peu plus rapidement dans leur mise en place. D'initiative moins générale ou plus privée, il existe bien des dossiers informatisés proches du dossier médical personnel notamment le dossier communicant de cancérologie[764] (seulement pour les patients atteints de cancer) ou le dossier

---

[762] Mission interministérielle de revue de projet sur le dossier médical personnel (DMP). *Rapport sur le dossier médical personnalisé (DMP)*. 8 Novembre 2007. p.26. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//074000713/0000.pdf. Consulté le 12 décembre 2013

[763] « *Le Professeur Albert-Claude BENHAMOU, estime, en tant que chirurgien, que sa priorité est de retrouver aisément, dans le DMP de son patient, les informations ayant une incidence vitale pour sa prise en charge(…) ainsi que tous les antécédents dont la méconnaissance peut avoir des conséquences iatrogènes catastrophiques. Pour atteindre cet objectif, il lui paraît fondamental de former les étudiants en médecine et en pharmacie aux usages de l'informatique de santé et surtout à la rédaction de notes de synthèse conçues dans cet esprit.* » LASBORDES, Pierre. *Rapport sur le dossier médical personnel(DMP) : quel bilan d'étape pour quelles perspectives ? (compte rendu de l'audition publique du 30 Avril 2009).* 20 juillet 2009. n° 1847 Assemblée Nationale. N°567 Sénat. http://www.ladocumentationfrancaise.fr/rapports-publics/094000364/index.shtml. Consulté le 27 mai 2014

[764] *« Issu du premier Plan Cancer (2003-2007), le dossier communicant de cancérologie (DCC) est désormais conçu comme un service spécialisé du DMP, au service de la coordination des soins pour les patients atteints de cancer. En facilitant l'échange d'informations, il établit un lien privilégié entre chaque professionnel de santé, qu'il relève de la médecine de ville comme de l'hôpital, afin d'accompagner la prise en charge du patient*

hôpital patient[765] (de l'AP - HP, Assistance Publique hôpitaux de Paris) ou encore le dossier socio-médical partagé[766] expérimenté dans les Yvelines. Mais, nous nous intéresserons à ceux qui sont d'envergure nationale et générale et qui ont été mis en route en même temps que le

---

pendant et après la phase aiguë de son traitement. Son usage permettra notamment de faciliter les réUnions de concertations pluridisciplinaires (RCP) et d'intégrer le programme personnalisé de soins (PPS), grâce aux fonctions de partage du DMP accessible à l'ensemble des professionnels de santé. Les comptes rendus d'anatomie et cytologie pathologiques, les compte rendus opératoires, indispensables au suivi d'un patient, mais également l'ensemble des documents structurés utiles à la coordination des soins, font partie également des éléments intégrés au DMP et sur lesquels le service DCC pourra s'appuyer. » ASIP santé. Communiqué de presse. *Cancérologie et coordination de soins : Déploiement du DCC : l'ASIP santé et l'INCA retiennent les 7 régions pilotes*. Paris, 11 janvier 2011. http://esante.gouv.fr/sites/default/files/Communique_de_presse_11_01_11_regions_phase_pilote_DCC_DMP.pdf. Consulté le 27 mai 2014

Le cadre national de ce dossier qui en définit les conditions de mise en œuvre a été publié en Octobre 2010.

« *Le DCC est un service permettant à l'ensemble des professionnels de santé impliqués dans la prise en charge d'un patient atteint d'un cancer de partager entre eux et avec le patient l'ensemble des documents médicaux de cette prise en charge. Le DCC n'est donc pas une application.*

Sur un plan technique, le service DCC ainsi défini met en œuvre : des fonctions de communication (importation et exportation) des données et documents au sein des applications habituellement utilisées par les professionnels de santé (logiciels de cabinet, SIH, plateaux techniques…) ; des infrastructures d'hébergement et des fonctions de sécurité communes avec le DMP, intégrées aux applications utilisées par les professionnels; un ensemble de documents plus ou moins structurés et plus ou moins spécifiques à la cancérologie, tous référencés dans une classification, elle-même intégrée à un cadre national d'interopérabilité. »

http://esante.gouv.fr/sites/default/files/INCa_ASIPSante_Cadre_National_DCC_DMP.pdf

Pour plus d'informations sur le DCC, voir sur le site internet de l'Institut national du cancer, *Dossier communicant de cancérologie.* 11 janvier 2011. http://www.e-cancer.fr/soins/parcours-de-soins/dossier-communicant-de-cancerologie

L'Asip santé et l'INCA ont publié en Septembre 2013 un document de référence qui permettra le déploiement du DCC par chaque agence régionale de santé dans le DMP. *Mise en œuvre du service DCC et DMP cible 2013-2015*. http://esante.gouv.fr/sites/default/files/ServiceDCCduDMP_Cible2013_2015_Septembre2013.pdf. Consulté le 27 mai 2014.

[765] C'est un Dossier Hospitalier Patient unique AP-HP, permanent et partagé quel que soit le point d'entrée du malade et sa circulation ultérieure dans les hôpitaux de l'AP-HP. Fondé sur des nomenclatures internationales standardisées, ce dossier Patient répondra aux règles d'interopérabilité nécessaires à l'échange d'informations dans le cadre d'un dossier médical partagé. Le dossier sera aussi communiquant avec les professionnels de santé de ville et le patient, dans un cadre répondant aux impératifs de sécurité, de confidentialité et d'éthique exigibles. L'avantage de ce dossier est d'améliorer la prescription des examens et des médicaments ainsi que la gestion des rendez-vous et des ressources soignantes, éviter également la perte de temps et la redondance d'examens, partager une information fiable et sécurisée avec les professionnels de ville et fluidifier le parcours du patient. http://www.reseau-chu.org/les-articles/article/article/le-dossier-hospitalier-patient-tient-ses-promesses/ Consulté le 27 mai 2014.

[766] C'est un service numérique permettant aux professionnels médico-sociaux de partager les informations nécessaires au suivi à domicile des personnes âgées en perte d'autonomie. Un microprocesseur mobile sécurisé au format d'une clé USB échange les données sanitaires et sociales avec l'ensemble des systèmes d'information des intervenants. *Colloque Industries du numérique et santé* des 28 et 29 février 2012. Paris Bercy. http://www.numerique-sante.fr/ateliers-pratiques. Consulté le 27 mai 2014.

Par délibération en date du 24 septembre 2009, la CNIL a autorisé le Conseil général des Yvelines à expérimenter ce dossier. *Délibération n°2009-522 du 24 septembre 2009 portant autorisation de la mise en œuvre à titre expérimental par le Conseil général des Yvelines d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'une plateforme de dossier médico-social partagé (DMSP) dans la région des Yvelines (autorisation n°1372117)*. http://legimobile.fr/fr/cnil/del/aut/2009/2009-522/ . Consulté le 27 mai 2014.

DMP mais ont connu, plus rapidement, du succès : le Web médecin et le dossier pharmaceutique.

a. Le « web médecin » ou historique des remboursements

Même s'ils ont tous été initiés par la loi du 13 Août 2004, et dans le même contexte, le web médecin, le DMP et le DP diffèrent en plusieurs points : leur objectif de création, leur contenu, les garanties de protection des droits des titulaires des dossiers qu'ils offrent.

i. L'objectif de la création du web médecin

Le Web médecin, ou historique des remboursements, est un relevé des données de remboursement des 12 derniers mois de chaque bénéficiaire de l'assurance maladie, détenu par son organisme gestionnaire de sécurité sociale et mis à la disposition des médecins conventionnés[767]. Dans le but de lutter contre les actes redondants et le nomadisme médical, ce relevé de données a été créé par la loi relative à l'assurance maladie du 13 août 2004 et, mis en application par le décret du 9 février 2006.

Le Web médecin permet aux médecins qui délivrent les soins aux patients, quel que soit leur lieu d'exercice (cabinet libéral, établissements de santé, centre de santé, les dessins salariés des régimes spéciaux), de connaître l'historique des actes et prestations délivrés. Mais l'acceptation ou le refus de ce traitement n'a aucun impact sur le niveau de prise en charge du bénéficiaire de l'assurance maladie. Avant la loi du 21 juillet 2009 dite HPST, l'accès au DMP

[767] C'est un service proposé par l'assurance maladie issu de l'article R. 162-1-10 du code de la sécurité sociale : « *pour l'application de l'article L. 162-4-3, les organismes gestionnaires des régimes de base d'assurance maladie assurent, à l'usage des médecins conventionnés ou exerçant leur activité dans un établissement ou un centre de santé, à l'occasion de soins qu'ils délivrent, la mise en œuvre d'un service de consultation par voie électronique des informations afférentes aux prestations délivrées à leur bénéficiaire* ».

A ce jour, seuls les médecins « *conventionnés ou exerçant leur activité dans un établissement ou un centre de santé* » ont accès à cet historique. Le rapport de la Cour des comptes sur le financement de la sécurité sociale 2008 relevait la prévision d'une extension de cet accès aux médecins urgentistes pour 2009, mais, en 2012, ce n'est pas encore le cas.

Il résulte des termes de l'article L. 162 - 4 - 3 du code de la sécurité sociale prévoyant que les médecins peuvent utiliser le service du Web médecin à l'occasion « des soins qu'ils délivrent » que sont exclus de ce service les médecins ne réalisant pas des prestations remboursables, notamment, les médecins de travail, les médecins experts et les médecins des compagnies d'assurances.

conditionnait cette prise en charge[768]. Il faut croire que les dénonciations[769] de la CNIL ont porté leur fruit avec la réforme de 2009. L'article L. 1111-15 du code de la santé publique créé par l'article 50 de la loi du 21 juillet 2009 reprend l'ancien article L. 161-36-2 du code de la sécurité sociale sans le deuxième alinéa qui prévoyait la condition d'accès au DMP à laquelle était subordonnée la prise en charge.

L'objectif de la création du Web médecin est différent de celui du DMP et du dossier pharmaceutique (DP) qui a pour mission de permettre la coordination des soins. Pourtant, initialement, l'historique des remboursements avait été créé en prélude à l'usage du DMP. En 2004, l'objectif affiché était celui d'une meilleure coordination des soins, dans l'attente du DMP alors annoncé pour 2007. Il était prévu que, de manière complémentaire au DMP, les données de remboursement détenues par l'assurance maladie puissent être mises à disposition des médecins, dès que le patient donne son consentement. Mais, le DMP, mettant du temps à se déployer, l'historique a été présenté non plus comme une mesure transitoire, dans l'attente du DMP, mais comme une disposition conjuguée à la mise en place de ce dernier pour « responsabiliser l'ensemble des acteurs »[770]. La maîtrise des dépenses de santé a été mise en avant, déterminant ainsi, les développements postérieurs qui privilégient l'intérêt économique.

La gestion du système du Web médecin est confiée à la caisse nationale de l'assurance-maladie des travailleurs salariés (CNAMTS), qui, responsable des traitements mis en œuvre à cet effet, est ténue d'obtenir une autorisation préalable de la CNIL[771] sur présentation de

---

[768] Article L. 161-36-2 du code de la sécurité sociale sous la loi du 13 août 2004 : « *le niveau de prise en charge d'exactes et prestations de soins par l'assurance-maladie prévue à l'article L. 322-2 est subordonné à l'autorisation que donne le patient, à chaque consultation ou hospitalisation, aux professionnels de santé auxquels il a recours, d'accéder à son dossier médical personnel et de le compléter. Le professionnel de santé est tenu d'indiquer, lors de l'établissement des documents nécessaires au remboursement et à la prise en charge, s'il a été en mesure d'accéder au dossier.* »

[769] *« La Commission observe que, conformément aux exigences rappelées ci-dessus, le texte qui lui est présenté, par la référence qu'il convient aux dispositions de l'article L. 1111-8 du code de la santé publique, implique que la création du dossier médical personnel repose sur le consentement exprès de la personne concernée. Néanmoins, dans la mesure où le niveau de prise en charge des actes et prestations est subordonné à l'accès du professionnel de santé au dossier, il apparaît que ce consentement n'est pas totalement libre. »* Cnil. Délibération n°2004-054 du 10 juin 2004 portant avis sur le projet de loi relatif à la réforme de l'assurance maladie. http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653162. Consulté le 28 mai 2014.

[770] Cour des comptes. *Rapport sur le financement de la sécurité sociale 2008*. p. 236. Disponible sur: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000597/0000.pdf. Consulté le 28 mai 2014.

[771] Article R. 162 - 1 - 10 alinéa 3, a) à c) du décret du 9 février 2006.

documents justifiant essentiellement des mesures prises pour assurer la sécurité des données contenues dans ce dossier.

ii. Le contenu du web médecin

Le décret[772] relatif aux modalités d'accès des médecins aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie donne une liste très détaillée du contenu de l'historique des remboursements. Mais le site internet de l'assurance maladie en propose une version très synthétique et simplifiée pour ses bénéficiaires. Il indique, en effet, que par son accès à l'historique des remboursements, le médecin peut consulter les informations suivantes :

- « *les consultations chez un médecin (généraliste ou spécialiste) ou chez un chirurgien-dentiste ;*
- *les médicaments remboursés (nom et posologie) ;*
- *les actes de radiologie (nature de l'examen et date) ;*
- *les actes de biologie (nature de l'examen et date) ;*
- *les arrêts de travail indemnisés (date et durée) ;*
- *les hospitalisations dans les établissements privés et publics (durée et nature du séjour, date d'admission) ;*
- *les transports (date et mode de transport).*[773] »

Cette présentation a le mérite de la simplicité mais, elle omet une partie des informations qui ne semblent pas être les moins importantes : « *les données relatives au bénéficiaire de l'assurance maladie*[774] ». Du fait de leur caractère nominatif, elles sont les plus déterminantes et peuvent fortement contribuer à démasquer les usurpateurs d'identité car une personne peut, parfaitement, se présenter dans un centre de soins avec une carte vitale qui n'est pas la sienne. Une autre possibilité serait qu'une personne figurant sur la liste des noms

[772] Article R. 162-1-11, 1°

[773] AMELI. *A quel type d'informations le médecin peut-il accéder ?* http://www.ameli.fr/assures/soins-et-remboursements/l-historique-des-remboursements/qu-est-ce-que-l-historique-des-remboursements.php. Consulté le 12 mars 2012.

[774] « *a) Numéro d'identification au répertoire national d'identification des personnes physiques ;*
b) Nom et prénom d'usage ;
c) Date de naissance. »

que contient la carte fasse ouvrir le dossier d'une autre ou que le médecin consulte le dossier d'un autre individu que le patient qu'il a en face de lui.

L'assurance maladie considère que le web médecin n'est pas un outil de partage de l'information médicale, au sens strict du terme, mais simplement la mise à disposition des médecins de données administratives relatives aux actes de soins. Cela justifie que les médecins ne soient pas aptes à l'alimenter ; c'est l'apanage de l'assurance maladie. Les médecins ne peuvent pas accéder aux comptes rendus des consultations, ni d'opération, ni à aucun résultat d'examen. Toutefois, la référence aux médicaments remboursés, aux actes de radiologie et de biologie suffit à considérer ce contenu comme renfermant des données suffisamment médicales pour se faire une idée de l'état de santé d'une personne. Certes, sans les résultats de ces examens on ne peut établir l'état pathologique d'un individu, mais cela suffit à émettre des suspicions préjudiciables à ce dernier. Il importe donc de réserver à ces informations les mêmes dispositions sécuritaires prévues pour les données sensibles dans leur ensemble. L'ordre des médecins, réclamant plus de garanties pour le traitement des données contenues dans l'historique des remboursements avait tenu à préciser que les données contenues dans cette base sont « *clairement des données médicales et la prise en charge financière par l'assurance-maladie ne change pas leur statut*. » Ceci est valable tant « *pour le protocole d'examen spécial propre aux personnes atteintes d'affection de longue durée exonérées du ticket modérateur que pour le codage de la totalité des actes effectués et des prescriptions délivrées. Ces informations médicales permettent d'identifier une pathologie précise même si celle-ci n'est pas clairement notifiée*[775] ».

Le contenu du web médecin constitue, dans l'ensemble, la réunion de celui du DP (sans les médicaments non remboursés) et celui du DMP, ce dernier ayant, en plus, deux espaces : les comptes rendus et l'espace d'expression personnelle du patient. C'est donc un dossier qui était bien élaboré pour « *favoriser progressivement l'émergence de nouvelles pratiques et permettre ensuite une acceptation plus rapide du DMP*[776] ». Mais la Cour des comptes déplore qu'aucune réflexion approfondie n'ait été menée dans ce sens par la

[775] Conseil national de l'ordre des médecins. *Historique des remboursements de l'assurance maladie : l'ordre des médecins demande des garanties*. 4 septembre 2007. http://www.Conseil-national.medecin.fr/article/historique-des-remboursements-de-l-assurance-maladie-l-ordre-des-medecins-demande-des-garanties-62. Consulté le 12 mars 2012.

[776] Cour des comptes. *Rapport sur le financement de la sécurité sociale 2008*. P. 236.

CNAMTS. Par ailleurs, vue l'étendue du contenu du web médecin, reprenant une bonne partie de celui réservé au DMP, on craint un risque de redondance des données lorsque le DMP sera prêt à l'intégrer.

La CNIL a également noté, dans sa délibération du 10 juillet 2007 autorisant la généralisation de l'historique des remboursements, « *qu'aucune alimentation du DMP par les services du Web médecin ni accès aux services du Web médecin à travers la consultation du dossier médical ne sont actuellement prévues*[777] », et considéré « *qu'une telle alimentation se heurterait à une différence de régime juridique, de finalité et de destinataires*[778] ». La Commission, tout comme la Cour des comptes, n'a pas non plus manqué d'émettre quelques réserves quant aux mesures prises pour la protection des droits des assurés.

iii. La protection des droits des assurés

La consultation de l'historique des remboursements par un médecin est soumise à l'accord préalable du patient[779] tout comme l'exige l'accès au DMP. Cette consultation n'est pas une obligation pour le médecin, et le patient a la possibilité d'y opposer un refus. Le consentement du patient est réputé obtenu par la simple remise de sa carte vitale. L'accès au web médecin se fait à partir de l'authentification et de l'identification du médecin au moyen de sa carte CPS ou un dispositif d'authentification individuel similaire et agréé par le groupement d'intérêt CPS[780] et de l'assuré à partir de sa carte vitale.

L'utilisation de la carte vitale comme preuve de consentement paraît moins convaincante en ce sens que plusieurs hypothèses peuvent justifier une utilisation sans consentement réel. L'influence morale consciente ou non du médecin sur son patient peut amener ce dernier à remettre la carte vitale par simple courtoisie. Une autre hypothèse serait que la carte soit utilisée à l'insu du patient à la suite d'un vol, d'une perte au par un usage fait par le médecin sans requérir au préalable le consentement du bénéficiaire (au détour d'une

[777]Délibération n° 2007-194 du 10 juillet 2007 autorisant la mise en place généralisée par la Caisse nationale d'assurance maladie des travailleurs salariés d'un traitement permettant aux médecins d'accéder aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie. Historique des remboursements ou web médecin.
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017651846&fastReqId=1903689407&fastPos=15. Consulté le 28 mai 2014.

[778] Idem.

[779] Article R. 162 - 1 - 12 alinéa 2 du code de la sécurité sociale.

[780] Article R. 162 - 1 - 13 du code de la sécurité sociale.

utilisation visant à permettre la transmission de l'accueil de soins). Dans ces conditions, comme preuve d'expression de son accord, la remise d'une attestation de consentement à l'assuré, comme dans le cas du dossier pharmaceutique, paraît être une solution. L'acceptation de ce document constituerait alors une preuve de son consentement ou, en tout au moins, de la remise de la carte vitale en toute connaissance de cause. Une autre solution serait de munir le titulaire de la carte vitale d'un « *code porteur*[781] » qui serait indispensable pour tout usage de cette carte.

La carte vitale elle-même, comme outil d'accès au web médecin, pose un problème de sécurité qui, à ce jour n'est pas résolue car les cartes vitales 1 continuent d'être utilisées par une bonne partie des assurés. L'assurance maladie avait prévu remplacer ces cartes par des cartes vitales 2[782] censées être plus sécurisées. La Cour des comptes relevait qu'avec le mécanisme de cartes de la première génération, « *l'assuré ne peut savoir si un professionnel a accédé à son historique des remboursements. Quant au médecin, il ne sera pas en mesure d'historiciser l'acceptation ou le refus de consultation de façon à se protéger d'un recours d'un patient qui contesterait avoir autorisé l'accès (même si le système conserve un journal des accès)*[783] ». Les assurés dépositaires des cartes vitales 1 demeurent donc encore plus exposés que ceux qui détiennent les cartes vitales 2.

L'assuré dispose d'un droit d'accès aux données à caractère personnel le concernant et, selon le cas, d'un droit de rectification de ces données auprès de la Caisse d'assurance maladie dont il relève ou du contrôle médical pour les informations relevant du protocole de soins. Le droit d'accès n'est donc pas direct, ni le droit de rectification, non plus comme cela est permis au titulaire du DMP. En outre, contrairement au DMP le bénéficiaire n'a pas le droit au masquage de ses données dans le cadre du web médecin ; celui-ci étant un « dossier

[781] Ce code serait l'équivalent du code PIN des cartes bancaires. ZORN, Caroline. *Données de santé et secret partagé*. P. 426

[782] La carte vitale 2 est la deuxième génération de carte vitale mise en circulation à partir de 2007. Arrêté du 14 mars 2007 relatif aux spécifications physiques et logiques de la carte d'assurance maladie et aux données contenues dans cette carte publié au JORF n° 65 du 17 mars 2007. p. 4983. Texte n° 30. NOR: SANS0721152A. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000461627&dateTexte=&categorieLien=id. En application du décret n° 2007-199 du 14 février 2007 relatif à la carte d'assurance maladie et modifiant le code de la sécurité sociale (deuxième partie : Décrets en Conseil d'État)**.** NOR: SANS0720208D publié au JORF n°39 du 15 février 2007 p. 2799. Texte n° 26.
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=27AE5B892F720CE705E9243C025EB68F.tpdjo03v_1?cidTexte=JORFTEXT000000275461&categorieLien=id. Consulté le 28 mai 2014.

[783] Cour des comptes. *Rapport sur le financement de la sécurité sociale 2008*. p. 238

métier » contrairement au DMP qui est, avant tout, personnel. Les articles R. 162-1-12 à R. 162-1-15 qui mettent en place ce dispositif sont muets sur le cas des mineurs[784] contrairement aux législations sur le DMP et le DP.

S'agissant de la traçabilité des accès, la CNAMTS est chargée de gérer une infrastructure d'accueil (portail) assurant le contrôle d'accès du dispositif puis le routage des requêtes vers les serveurs des organismes gestionnaires des différents régimes de base concernés. Les traces enregistrées seront consultables en ligne pendant une durée de trois mois. Cette phase de consultation étant achevée, la durée totale de conservation de ces traces sera de deux ans[785]. Ainsi, contrairement à la réglementation du DMP, celle du Web médecin ne permet pas à chaque bénéficiaire de l'assurance maladie de pouvoir consulter directement l'historique des accès. En 2006, un amendement[786] des parlementaires a été censuré par le Conseil Constitutionnel[787] au motif qu'elle était sans rapport avec l'équilibre financier de la sécurité sociale alors qu'il visait à permettre aux assurés sociaux d'accéder à leurs données ainsi qu'à l'historique permettant d'identifier les médecins qui ont consulté leur relevé.

Face aux intrusions dont le système informatique de l'assurance maladie a fait l'objet, l'ordre des médecins a critiqué cette situation qui empêche l'assuré de savoir qui a consulté

---

[784]« *La Commission constate que les textes concernant le système du "Web médecin" ne prévoient aucune disposition particulière concernant les personnes mineures. En revanche, des dispositions particulières du code de la santé publique reconnaissent aux mineurs la possibilité de recourir à des actes de soins sans que leurs parents en soient informés par dérogation au principe de l'autorité parentale (L. 1111-5 du code de la santé publique), sur une interruption volontaire de grossesse (L. 2212-10 du CSP), un mode de contraception (L. 5134-1 du CSP) ou la prévention, le dépistage, le diagnostic et le traitement ambulatoire des infections sexuellement transmissibles (L. 3121-2-1 du CSP).*
Dans les cas précités, la CNAMTS a indiqué que les professionnels de santé sont directement remboursés et que ces activités sont rattachées, dans les systèmes d'information de l'assurance maladie à un numéro d'identification non signifiant. Ces soins n'apparaîtront donc pas dans les relevés de remboursement et ne pourront donc pas être consultés dans le système du "Web médecin". La Commission estime qu'il serait souhaitable que soit rappelé dans les plaquettes d'information, tant aux médecins qu'aux patients, le fait que le service du "Web médecin" ne peut être consulté, en règle générale, qu'à l'occasion de la délivrance des soins et en présence des patients concernés, quel que soit leur âge. »
Délibération de la CNIL n° 2007-194 du 10 juillet 2007 autorisant la mise en place généralisée par la Caisse nationale d'assurance maladie des travailleurs salariés d'un traitement permettant aux médecins d'accéder aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie. Historique des remboursements ou web médecin. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017651846&fastReqId=1903689407&fastPos=15. Consulté le 28 mai 2014.

[785] Idem

[786] SENAT. Amendement 205. *Discussion des articles additionnels du financement de la sécurité sociale pour 2007*. Vendredi 17 novembre 2006. http://www.senat.fr/cra/s20061117/s20061117H1.html#toc2. Consulté le 26 mai 2014.

[787] Conseil constitutionnel. Décision n° 2006-544 DC du 14 décembre 2006. http://www.Conseil-constitutionnel.fr/Conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2006/2006-544-dc/decision-n-2006-544-dc-du-14-decembre-2006.1016.html. Consulté le 26 mai 2014.

son historique et à quel moment. L'ordre considère que « *seule cette faculté garantirait à chaque patient le respect effectif de la confidentialité des données figurant sur la base de données, le respect des procédures mises en place, comme le respect de l'interdiction faite par la loi aux médecins qui ne délivrent pas de soins (médecin de compagnies d'assurances en particulier) d'accéder à ces données*[788]. » Cependant, il faut reconnaître que cette limitation de droit d'accès n'est pas préjudiciable à l'assuré sur tous les plans. Le web médecin étant plus un « dossier métier » qu'un dossier personnel, il a été conçu pour servir davantage les intérêts de l'assurance maladie que ceux de l'assuré puisqu'il lui sert d'outil de travail à but économique. Dès lors le droit au masquage a ici moins d'importance que dans le cadre du DMP. De plus, pour protéger la confidentialité des données, moins il y a de possibilités d'accès, moins il y a de risques d'atteinte compte tenu de la probabilité d'usurpation d'identité numérique dont pourrait être victime l'assuré.

Par ailleurs, le danger pourrait venir de la négligence des médecins dans la prise de dispositions pour sécuriser leur système d'information. La CNIL, dans sa délibération du 10 juillet 2007, fait remarquer que les données risquent de se trouver « *en clair* » sur les postes du praticien si celui-ci n'installe pas au minimum un antivirus ou un pare-feu régulièrement mis à jour sur son ordinateur. Les échanges sont sécurisés par des connexions chiffrées si Internet et le poste de travail ne sont pas censés conserver les données consultées. Mais le risque demeure qu'un médecin consulte l'historique des remboursements après le départ de son patient sans son accord et en son absence. Pour remédier à cette faille, une version HR5 de la carte vitale a été prévue pour interrompre la connexion aussitôt que la carte vitale est retirée du lecteur. Mais le test[789] qui aurait eu lieu le 17 septembre 2008 n'aurait pas été concluant. On se demande alors pourquoi l'assurance maladie n'a pas adopté le même dispositif que celui utilisé pour le dossier pharmaceutique qui permet la fermeture automatiquement du dossier dès le retrait de la carte vitale. Devrions-nous y voir un manque

[788] Conseil national de l'ordre des médecins. *Historique des remboursements de l'assurance maladie : l'ordre des médecins demande des garanties*. 4 septembre 2007. http://www.Conseil-national.medecin.fr/article/historique-des-remboursements-de-l-assurance-maladie-l-ordre-des-medecins-demande-des-garanties-62. Consulté le 28 mai 2014.

[789]FRASLIN, Jean-Jacques. *11 millions d'euros pour le « web zinzin* ». 16 septembre 2008. http://www.i-med.fr/spip.php?article221. Consulté le 21 mai 2013.
« Jean-Jacques FRASLIN est médecin généraliste à Bouguenais, dans la grande banlieue de Nantes. Il est un des fondateurs et des principaux animateurs du site Fulmedico, de la « Fédération des utilisateurs de logiciels médicaux et communicants » (association 1901). Ses qualités d'expertise largement reconnues font que son avis est très souvent demandé par les institutions, organismes ou entreprises s'occupant d'informatique médicale. » http://www.carnetsdesante.fr/Fraslin-Jean-Jacques. Consulté le 21 mai 2013.

de volonté politique ou un manque de moyens financiers à injecter dans un projet qui a déjà coûté au moins 11 millions d'euros[790] ?

Le rapport de la Cour des comptes sur le financement de la sécurité sociale et les exigences de garanties de l'ordre des médecins montrent que la mise en œuvre du web médecin comporte encore d'énormes failles quant à la protection des droits des assurés. Mais, le plus surprenant, c'est que la CNIL, même après avoir relevé des défaillances dans sa délibération du 10 juillet 2007 aie autorisé sa mise en place généralisée. Le dossier pharmaceutique a fait l'objet de moins de critique.

b. Le dossier pharmaceutique

Le dossier médical personnel et le dossier pharmaceutique sont régis par la même section du code de la santé publique (1ère partie, 1er titre, 1er chapitre, section 3), article L. 1111-14 à L. 1111-24. Mais seul l'article L. 1111-23 traite du dossier pharmaceutique sans en donner les détails. Le code de la sécurité sociale, partie réglementaire (titre 6, chapitre 1er, section 5) complète cette disposition en ses articles R.161-58-1 à R. 161-58-11.

Le dossier pharmaceutique (DP) est la liste de tous les médicaments qui ont été délivrés à une personne dans l'ensemble des pharmacies équipées pour ce nouveau service. Il collecte, pour chaque patient, l'ensemble de ses traitements médicaux (prescrits ou conseillés par les pharmaciens d'officine), sur une période de quatre mois. Le DP est différent de l'historique[791] que l'on retrouve habituellement dans les pharmacies en ce sens que cet historique est créé sans recourir à un consentement quelconque. Il centralise les traitements au niveau national chez un hébergeur de données de santé, pour permettre à toute officine dans laquelle se rend le patient de les consulter et de les compléter.

[790] Cour des comptes. *Rapport sur le financement de la sécurité sociale 2008*. P. 236

[791] Son contenu n'est consultable que dans la pharmacie qui a dispensé la liste de médicaments concernée et il ne permet qu'une analyse sur l'historique des médicaments dispensés par l'officine alors que le dossier pharmaceutique permet une analyse étendue à la consommation globale du patient. Cette liste n'est pas partagée alors que le DP est partagé et consultable de n'importe quelle pharmacie. Toutefois, dès la connexion de la carte vitale à l'ordinateur d'une officine équipée pour la gestion d'un DP, il apparaît à l'écran la possibilité de se connecter au DP de l'assuré ou de le Consulté si ce dernier en dispose déjà. Dans ce cas, sur l'écran apparaît en haut, à droite, un logo avec la mention « DP créé ». Dans le cas échéant, le logo comporte la mention « DP non créé » et la possibilité de le créer. Concernant le DMP, un autocollant DMP disponible dans la brochure d'information est apposé sur la carte vitale pour indiquer que le titulaire en dispose.

Le DP contient[792], en plus de l'identité du titulaire, les noms, les quantités, les dates d'achat des médicaments et rien de plus ; même pas les noms des pharmacies ayant délivrées les médicaments (mais ceux des pharmaciens ayant effectué une intervention quelconque sur le dossier[793]), ni aucun autre renseignement sur la santé du concerné. Le DP réunit aussi bien les médicaments prescrits sur une ordonnance que ceux conseillés par le pharmacien, les médicaments remboursés tout comme les non remboursés.

A la suite d'une expérimentation concluante dans un certain nombre de départements[794], la CNIL va autoriser[795], en décembre 2008 une généralisation du dossier pharmaceutique sur tout le territoire français dans les officines de ville. Cette autorisation a également été donnée pour une expérimentation dans les pharmacies hospitalières en mai

[792] Article R. 161-58-2 du code de la sécurité sociale par modification du décret dossier pharmaceutique
I. « *Le dossier pharmaceutique comporte les informations relatives :*
« 1° Au bénéficiaire de l'assurance maladie :
« a) Nom de famille ou nom d'usage, prénom usuel, date de naissance ;
« b) Sexe et, en cas de naissance multiple, rang de naissance.
« 2° A la dispensation des médicaments :
« a) Identification et quantité des médicaments, produits et objets définis à l'article L. 4211-1 du code de la santé publique dispensés pour l'usage du bénéficiaire, avec ou sans prescription médicale ;
« b) Dates de dispensation. »
Article R. 161-58-11 du code de la sécurité sociale (idem)
« Les données du dossier pharmaceutique sont conservées et accessibles dans les conditions suivantes :
« 1° Les données mentionnées au 1° du I de l'article R. 161-58-2 sont conservées par l'hébergeur et accessibles par le pharmacien d'officine pendant toute la durée du dossier ;
« 2° Les données mentionnées au 2° de l'article R. 161-58-2 sont, à compter de la date à laquelle elles ont été saisies, accessibles par le pharmacien d'officine pendant quatre mois, puis archivées par l'hébergeur pendant une durée complémentaire de trente-deux mois afin de permettre, en cas d'alerte sanitaire relative à un médicament, d'en informer les patients auxquels ce médicament a été dispensé. Au terme de la durée totale de trois ans, l'hébergeur détruit les données, ainsi que les traces d'interventions mentionnées au II de l'article R. 161-58-2. »
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000019938177&dateTexte=&oldAction=rechJO&categorieLien=id. Consulté le 21 mai 2013.

[793] Article R. 161-58-2 du code de la sécurité sociale par modification du décret dossier pharmaceutique
II. Chaque intervention sur le dossier pharmaceutique aux fins de création, de consultation, d'alimentation de clôture ou, à la demande du bénéficiaire ou de son représentant légal, de rectification des informations ou édition d'une copie, est datée et comporte l'identification du pharmacien d'officine qui a effectué cette intervention.
http://www.legifrance.gouv.fr/affichCode.do;jsessionid=CE2EDBC8E42A6DF46477AA75D40BD436.tpdjo15v_2?cidTexte=LEGITEXT000006073189&idSectionTA=LEGISCTA000019941682&dateTexte=20120412&categorieLien=id#LEGISCTA000019941682. Consulté le 21 mai 2013.

[794] Doubs, Meurthe-et-Moselle, Nièvre, Pas-de-Calais, Rhône, Seine-Maritime, Yvelines et Hauts-de-Seine

[795] CNIL, délibération n° 2008 - 487 portant autorisation de traitement de données personnelles permettant la mise en œuvre généralisée du dossier pharmaceutique. 2 décembre 2008. http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000020022185

2010[796]. Des mesures techniques et juridiques ont été prises pour assurer la protection des bénéficiaires depuis la création jusqu'à la destruction du dossier pharmaceutique.

i. La création du dossier pharmaceutique

Désormais effectif, le DP est créé par un pharmacien[797] d'officine pour chaque bénéficiaire de l'assurance maladie avec l'accord exprès[798] de ce dernier après avoir pris connaissance des informations relatives à sa création, son utilisation et sa clôture[799]. Le consentement[800] est matérialisé par la remise de la carte vitale. Il peut être délivré un DP pour les enfants mineurs tout comme le DMP est proposé aux assurés même mineurs dès lors qu'ils disposent d'un numéro de sécurité sociale qui leur est propre sur une carte vitale[801].

[796] Délibération n°2010-116 du 6 mai 2010 autorisant à titre expérimental des pharmacies hospitalières à mettre en œuvre des traitements de données personnelles nécessaires au dossier pharmaceutique. http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000022379205. Consulté le 21 mai 2013.

[797] Article L161-36-4-2, alinéa 2 du code de la sécurité sociale: *« 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. 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. 161-36-2.* » http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006073189&idArticle=LEGIARTI000017842048&dateTexte= Consulté le 21 mai 2013.

[798] L'acceptation informatique est automatiquement transmise au serveur de l'hébergeur DP dès que le formulaire de création est imprimé et remis pour signature matérielle de l'assuré. Le refus de la création est, certes, automatiquement transféré au serveur de l'hébergeur mais ne génère pas de formulaire de refus.

[799] « *Après avoir pris connaissance des informations relatives à la création, l'utilisation et la clôture du dossier pharmaceutique ainsi qu'à son droit à la rectification des données le concernant, communiquées par le pharmacien d'officine, le bénéficiaire de l'assurance maladie ou son représentant légal autorise expressément sa création…* » Article R. 161-58-3 CSS.
Et la charte du DP d'ajouter : « *lorsque le patient souhaite créer un dossier pharmaceutique, il donne son consentement auprès d'un pharmacien d'officine, après avoir pris connaissance des informations figurant sur le dépliant d'informations du dossier pharmaceutique dont le modèle est fixé par l'Ordre des pharmaciens* » CNOP. *Charte du dossier pharmaceutique*. Direction de la communication du Conseil national de l'ordre des pharmaciens. 2009. P.7.

[800] « *Il importe donc de rappeler aux pharmaciens d'officine qu'en cas d'indices pouvant faire douter de l'identité du porteur de la carte, il est de leur responsabilité de procéder aux vérifications indispensables. Il est rappelé à cet égard que, conformément aux dispositions de l'article 93 du décret n°2005-1309 du 20 octobre 2005, il appartient aux intéressés de justifier par tout moyen de leur identité*. » CNIL. Délibération n° 2008 - 487 portant autorisation de traitement de données personnelles permettant la mise en œuvre généralisée du dossier pharmaceutique. 2 décembre 2008. http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000020022185. Consulté le 21 mai 2013.

[801] Aujourd'hui, il n'est pas possible de créer un DMP à une personne mineure relevant du régime général de sécurité sociale ou des régimes associés, puisque n'ayant pas de NIR propre sur une carte vitale, ils ne peuvent disposer d'INS.

De même que le dossier médical personnel, le DP est créé « *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 du code de la santé publique*[802] ». A l'usage des pharmaciens d'officine, son ouverture et sa gestion se font par voie électronique à l'aide de l'identifiant national[803]. C'est le Conseil national de l'ordre des pharmaciens qui en organise la mise en œuvre[804]. Celle-ci réunit un Comité constitué des mêmes acteurs que ceux du dossier médical personnel : les organisations professionnelles concernées (syndicats représentatifs de l'officine, ordres des professionnels de santé prescripteurs, représentants des facultés de pharmacie, étudiants...), des partenaires publics (ministère de la santé, HAS, AFSSAPS[805], CNAM, CNIL, ASIP Santé...) et des associations de patients.

A la fin de la création du DP, le pharmacien remet un document au client attestant qu'il lui a été créé ce dossier. Comme pour le DMP[806], le patient a le choix de le créer ou non, de le fermer et même de ne pas y inscrire certains médicaments. Mais, le médecin a plus de prérogatives au niveau du DMP que le pharmacien pour le DP. Autant, après une première autorisation, le médecin peut se permettre d'ajouter des éléments sensibles au DMP sans en avertir le patient, autant aucune action ne peut se faire dans le DP par le pharmacien sans la présence et l'accord du titulaire qui donne accès à son dossier uniquement par sa carte vitale. Le pharmacien les mentionne dans le dossier[807]. Cela n'a pas de répercutions sur les droits au

[802] Article L. 161-36-4-2 du code de la sécurité sociale.

[803] Article R. 161-58-1 du code de la santé publique.

[804] Article L. 161-36-4-2 du code de la sécurité sociale et l'article L. 4231-2 du code de la sécurité publique relatif aux missions de l'ordre des médecins.

[805] Cette agence est devenue ANSM: (Agence nationale de sécurité du médicament et des produits de santé) depuis le 1er mai 2012.

[806] « *A l'occasion de mes rendez-vous avec mes médecins ou les professionnels de santé qui me suivent, je leur donne l'autorisation d'ajouter dans mon DMP les documents qu'ils jugent utiles à mon parcours de soins et nécessaires à la coordination (diagnostic d'une nouvelle pathologie, traitement d'une pathologie chronique, examen lié à des soins préventifs, prescription médicamenteuse, etc.). Dès lors que j'ai donné mon autorisation, ils peuvent aussi déposer des documents utiles en mon absence. Dans certains cas, les professionnels de santé peuvent ajouter des documents dits « sensibles » dans mon DMP sans que j'en sois averti. Je pourrai les Consulté une fois que j'aurai été informé de leur contenu lors d'un entretien avec le professionnel de santé qui me suit. De mon côté, dans le cadre d'un dialogue avec mon professionnel de santé, je peux demander que certains documents ne soient pas ajoutés dans mon DMP ou soient supprimés. Je peux également demander le « masquage » d'un document ; ce document ne sera alors plus visible que par son auteur, mon médecin traitant et moi-même.* » DMP.gouv.fr. Espace patient. *Mon médecin ajoute des documents dans mon DMP*. http://dmp.gouv.fr/web/dmp/patient/mon-medecin-ajoute-des-documents-dans-mon-dmp.

[807] Article R. 161-58-6. Code de la sécurité sociale (par modification du décret dossier pharmaceutique, article 1): « *Le bénéficiaire du dossier pharmaceutique ou son représentant légal peut s'opposer à ce que le pharmacien*

remboursement ou sur la procédure du tiers payant. Le titulaire du DMP peut ajouter au DMP toute information qu'il juge nécessaire de porter à la connaissance des professionnels de santé qui le suivent. Dans les deux cas, les titulaires conservent, en somme, leur droit de rectification, de suppression et d'opposition conformément à la loi informatique et libertés. Mais, les dispositions qui régissent le DP ne prévoient ni droit d'accès direct par le patient, ni droit de masquage ; ce qui limite les droits des bénéficiaires des DP contrairement à ceux des DMP. C'est l'occasion de se demander comment va se gérer ce genre de situation si le DP finit, un jour, par être intégré au DMP. Le bénéficiaire pourra-t-il jouir de ces droits sur tout le DMP sauf la partie DP ou des modifications législatives interviendront avant pour ouvrir ces droits aussi au contenu du DP ?

Le DP est aussi gratuit que le DMP. Grâce au DP, le pharmacien a la possibilité de vérifier les risques[808] de double emploi, de contre-indications ou d'interactions dangereuses car il a une vision globale des traitements ; ce qui procure une sécurité supplémentaire et des conseils personnalisés. Le pharmacien pourra adapter ses conseils en fonction des médicaments précédemment délivrés au patient dans son officine ou non. Il est le premier engagé dans la lutte contre les risques iatrogènes[809] médicamenteux. La loi du 4 mars 2002 relatif aux droits des malades et à la qualité des soins a insisté sur la nécessité d'une meilleure gestion des risques iatrogènes. Et la loi du 9 Août 2004 relative à la politique de santé publique a fixé comme objectif de parvenir en cinq ans à réduire la fréquence des événements iatrogènes d'origine médicamenteuse[810] (fautive et évitable) entraînant une hospitalisation.

---

consulte son dossier ou à ce que certaines informations mentionnées au 2° de l'article R. 161-58-2 y soient enregistrées. Dans ce cas, le pharmacien mentionne l'existence d'un refus. »

[808] Article R. 161-58-5.-I. code de la sécurité sociale : *« II. — Au moment de la dispensation, et sauf opposition du bénéficiaire ou de son représentant légal, le pharmacien, dans le respect des règles déontologiques et professionnelles qui lui sont applicables : « 1° Consulte le dossier pharmaceutique, afin de déceler et de signaler au bénéficiaire ou à son représentant légal les éventuels risques de redondances de traitements ou d'interactions médicamenteuses pouvant entraîner des effets iatrogènes connus et, le cas échéant, de refuser la dispensation ou de délivrer un médicament ou produit autre que celui qui a été prescrit, dans les conditions respectivement des articles R. 4235-61 et L. 5125-23 du code de la santé publique. »* Décret dossier pharmaceutique précité. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000019938177&dateTexte=&oldAction=rechJO&categorieLien=id. Consulté le 23 mai 2013

[809] Iatrogène vient du grec « iatros » : médecin, et « genein » : engendrer.
Un événement iatrogène est un événement non désiré pour le patient, résultant des soins médicaux. Le pharmacien étant le spécialiste du médicament, il est directement concerné par l'iatrogénie médicamenteuse. Mais qui dit iatrogénie ne veut pas dire pour autant faute ou erreur.

[810] Certes, les pharmaciens disposent déjà, dans la quasi-totalité des cas, d'un historique local des ordonnances dispensées aux patients qui fréquentent régulièrement leur officine. Le pharmacien peut donc, d'ores et déjà, agir contre l'iatrogénie médicamenteuse en se référant à cet historique et en tenant compte des informations dont il

ii. Le DP, une partie du DMP

Le DP a été initialement conçu pour être le volet « médicament » du dossier médical personnel par la loi du 30 janvier 2007[811]. Mais, la loi[812] de financement de la sécurité sociale du 19 décembre 2007 va destiner les données constituant le DP à être reportées dans le dossier médical personnel sous l'étiquette « volet médicaments ». Après l'autorisation de sa généralisation, le décret[813] relatif au dossier pharmaceutique est publié le 15 décembre 2008. En 2009, la loi HPST va insérer les dispositions relatives au dossier pharmaceutique dans le code de la santé publique par son article L. 1111-23. Ces actes ont ainsi rendu le dossier pharmaceutique indépendant vis-à-vis du dossier médical personnel qui prenait du retard à se déployer. Malgré sa relative indépendance, le DP est destiné à compléter le DMP, c'est pourquoi l'une des conditions du contrat passé par l'Ordre des pharmaciens avec l'hébergeur, porte sur la garantie de l'interopérabilité du DP avec le DMP[814].

Même si le dossier pharmaceutique est surtout "partagé" alors que le dossier médical personnel est surtout "personnel", l'exercice officinal, naguère centré sur le seul médicament, évolue aujourd'hui, vers une pratique davantage orientée vers le patient. Le dossier pharmaceutique favorise un approfondissement de la relation pharmacien - patient et un véritable suivi thérapeutique à l'officine. Il permet d'accompagner le patient dans la compréhension de son traitement, de vérifier qu'il y adhère, qu'il l'observe, qu'il en tire pour

---

dispose sur son patient. Mais, les historiques actuellement utilisés sont attachés au remboursement et sont donc loin d'être complets. Ils ne contiennent pas systématiquement les médicaments de médication officinale dispensés, ni les médicaments dispensés par d'autres officines au même patient.

[811] Article 25 - I -2° de la 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. JORF du 1er février 2007. Cette disposition a donné naissance à l'article L. 161 - 36 - 4 - 2 du code de la sécurité sociale.

[812] Loi n° 2007- 1786 du 19 décembre 2007 de financement de la sécurité sociale pour 2008. JORF n° 296 du 21 décembre 2007. p. 20603. Texte n° 1, articles 56 : « l'article. 161 - 36 -4 -2 du code de la sécurité sociale est ainsi modifiée : 1° après le mot « pharmaceutique », la fin du premier alinéa est supprimée ».

[813] Décret n° 2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique. JORF n°0293 du 17 décembre 2008. p.19237. Texte n° 26.

[814] Article R. 161-58-10. Code de la sécurité sociale (par modification du décret dossier pharmaceutique, article 1): *« Les dossiers pharmaceutiques sont hébergés chez un hébergeur unique de données de santé à caractère personnel, agréé en application des articles R. 1111-9 à R. 1111-16 du code de la santé publique. Cet hébergeur est sélectionné par le Conseil national de l'ordre des pharmaciens qui passe avec lui un contrat. Ce contrat précise notamment les conditions techniques nécessaires pour assurer la qualité et la continuité du service rendu, la conservation, la sécurité, la confidentialité et l'intégrité des données, ainsi que leur interopérabilité avec le dossier médical personnel »*

lui, le meilleur bénéfice et qu'il n'est pas gêné par les effets indésirables. Dans ces conditions, l'humanisation de la relation que favorise le DP entre en porte-à-faux avec la vision totalement alarmiste de M. Pierre LECOZ quant à l'informatisation des dossiers médicaux. Il existe un risque que la prise en charge du patient soit parfois plus tributaire des informations virtuelles mises à la disposition de l'équipe soignante que de leur échange de visu, incarné et intersubjectif. M. LECOZ craint que la *« technologisation »* de la relation soignant-soigné ne finisse insidieusement par effacer les visages et les émotions qu'ils font naître[815].

Mais, il faut surtout tenir compte de ce que le dossier pharmaceutique et le dossier médical personnel sont les outils qui ouvrent la voie au développement d'un meilleur partage des compétences entre professionnels de santé. Un dossier pharmaceutique, qui fonctionne en articulation avec le dossier médical personnel, devrait favoriser une culture du partage des informations, entre professionnels de santé, seule à même de permettre un suivi du patient et de tous les soins qu'il reçoit. Le rôle du pharmacien dans le circuit de pathologie chronique pourra, par exemple, être davantage développé comme le prévoit la loi[816] HPST du 21 juillet 2009 (article 38, 7°). Celle-ci autorise en effet, le pharmacien à renouveler, pour des situations de dépannage et de manière exceptionnelle, une prescription pour un patient chronique. À l'avenir et à la demande des prescripteurs initiaux, le pharmacien pourrait, également, lors d'un véritable entretien pharmaceutique, s'assurer que le patient a bien compris la prescription.

---

[815] LECOZ. Pierre. *Avis du CCNE à propos des questions soulevées par l'informatisation des données de santé*. Revue générale de droit médical n° 37, décembre 2010. p. 203.

[816] Article L 5125-1-1 A du code de la santé publique (article 38 de la loi du 21 juillet 2009) :
« Dans les conditions définies par le présent code, les pharmaciens d'officine :
1° Contribuent aux soins de premier recours définis à l'article L. 1411-11 ;
2° Participent à la coopération entre professionnels de santé ;
3° Participent à la mission de service public de la permanence des soins ;
4° Concourent aux actions de veille et de protection sanitaire organisées par les autorités de santé ;
5° Peuvent participer à l'éducation thérapeutique et aux actions d'accompagnement de patients définies aux articles L. 1161-1 à L. 1161-5
6° Peuvent assurer la fonction de pharmacien référent pour un établissement mentionné au 6° du I de l'article L. 312-1 du code de l'action sociale et des familles ayant souscrit la convention pluriannuelle visée au I de l'article L. 313-12 du même code qui ne dispose pas de pharmacie à usage intérieur ou qui n'est pas membre d'un groupement de coopération sanitaire gérant une pharmacie à usage intérieur ;
7° Peuvent, dans le cadre des coopérations prévues par l'article L. 4011-1 du présent code, être désignés comme correspondants au sein de l'équipe de soins par le patient. A ce titre, ils peuvent, à la demande du médecin ou avec son accord, renouveler périodiquement des traitements chroniques, ajuster, au besoin, leur posologie et effectuer des bilans de médications destinés à en optimiser les effets ;
8° Peuvent proposer des Conseils et prestations destinés à favoriser l'amélioration ou le maintien de l'état de santé des personnes.
Un décret en Conseil d'État fixe les conditions d'application des 7° et 8°. »
http://www.legifrance.gouv.fr/affichCode.do;jsessionid=1EEBD506AC448270B79EC93415E96E35.tpdjo14v_3?idSectionTA=LEGISCTA000020890194&cidTexte=LEGITEXT000006072665&dateTexte=20120413.
Consulté le 21 mai 2013.

Il vérifierait que la posologie est correcte et l'adapterait dans le cas contraire. Il contrôlerait que l'observance est optimale. Via le dossier médical personnel, le dossier pharmaceutique apporterait aux autres professionnels de santé une connaissance exhaustive des médicaments dispensés en ville et ou à l'hôpital.

iii. La sécurisation des données du dossier pharmaceutique

Seuls les pharmaciens et leurs collaborateurs[817] autorisés par la loi à délivrer les médicaments peuvent consulter un dossier pharmaceutique. Ils sont tenus au secret professionnel et ne peuvent accéder au DP qu'avec la carte vitale comme c'est le cas pour l'accès au DMP. Ni la sécurité sociale, ni la mutuelle, ni même le médecin n'ont accès au DP. Pour le dernier, le patient a la possibilité de demander une copie[818] papier de son DP dans une officine équipée de ce service en cas de besoin d'information quant au traitement que suit régulièrement le patient.

Le DP est enregistré sous un numéro exclusif[819], qui n'est destiné à aucun autre usage. Toutes les informations contenues et échangées sont chiffrées. Elles ne sont conservées ni sur la carte vitale, ni dans aucune pharmacie : elles sont stockées chez un « hébergeur de données de santé », avec qui le Conseil de l'ordre des pharmaciens a passé un contrat. Quand le

[817] Préparateurs, étudiants à partir de l'inscription en troisième année, etc… Ces intervenants, authentifiés par leur carte CPS ou CPE, communiquent avec l'hébergeur de données de santé via les liens sécurisés (HTTPS/SSLv3.0). L'hébergeur reçoit quotidiennement la liste des certificats d'authentification grillée ou annulée par le GIP–CPS. Les données de santé consultées par l'officine ne peuvent subsister dans son système informatique une fois la connexion achevée : elles sont automatiquement effacées par le LGO (logiciel de gestion d'officine).

[818] Article R. 161-58-9. Code de la sécurité sociale (par modification du décret dossier pharmaceutique, article 1)

[819] CNOP. Dépliant-patient. P. 3. Rubrique : *quels sont les droits des patients* ? du site du Conseil de l'Ordre des pharmaciens : http://www.ordre.pharmacien.fr/Le-Dossier-Pharmaceutique/Quels-sont-les-droits-des-patients.
Ce numéro est distinct de l'identifiant national prévu par l'article L1111-8-1 créé par la loi n°2007-127 du 30 janvier 2007, article 25 (V) publié au JORF du 1er février 2007 qui dispose: « *Un identifiant de santé des personnes prises 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.* »
http://www.legifrance.org/affichCodeArticle.do;jsessionid=571A31875C188A4CB6150C5FA59CD552.tpdjo10v_3?idArticle=LEGIARTI000006685788&cidTexte=LEGITEXT000006072665&dateTexte=20071221.
Consulté le 20 septembre 2011.

pharmacien consulte le DP, cet hébergeur lui envoie les données par un réseau informatique professionnel sécurisé. Dès que le pharmacien rend la carte vitale d'un individu, les données sur ses médicaments qui viennent d'une autre pharmacie disparaissent de son ordinateur. *« Le dossier pharmaceutique est automatiquement clos par l'hébergeur mentionné à l'article R. 161-58-10, s'il n'a fait l'objet d'aucun accès pendant une durée de trois ans. Lorsque le dossier pharmaceutique est clos, son contenu est détruit dans sa totalité par l'hébergeur*[820]*. »* Ce temps de conservation relativement court diminue considérablement les risques de détournement de finalité de ces traitements tout en ayant permis de réagir positivement en cas d'alerte sanitaire.

L'hébergeur du dossier pharmaceutique (GIE SANTEOS) a été choisi par le Conseil de l'ordre des pharmaciens sur de très nombreux critères (entre autres, la performance, l'ergonomie, la fiabilité, la confidentialité, l'interopérabilité avec le dossier médical personnel et, bien entendu, le coût). Il a reçu un agrément du ministère de la santé en application de l'article L. 1111 - 8 du code de la santé publique, obligation entrée en vigueur depuis 2009.

Pour garantir en toutes circonstances la sécurité et la continuité du service, toutes les données sont dédoublées par l'hébergeur et stockées sur deux sites géographiquement séparés. La signature numérique est réalisée à partir des certificats des pharmaciens. L'utilisateur possède un certificat sur sa carte CPS ou CPE[821]. Son poste de travail ou le serveur d'officine (suivant la localisation du composant du LGO[822] réalisant la signature) dispose de fonctionnalités permettant d'accéder au contenu de la carte à puce. Ces composants sont fournis par le GIP CPS. La traçabilité des échanges entre l'officine et l'hébergeur constitue un élément de preuve en cas de contentieux juridique car cela permettra si besoin est, de prouver qu'un pharmacien a consulté ou non un dossier pharmaceutique. L'hébergeur conserve l'ensemble des actions (consultations, alimentation...) effectuées sur son serveur dossier

[820] Article R. 161-58-4. Code de la sécurité sociale (par modification du décret dossier pharmaceutique, article 1)

[821] La CPE (carte professionnelle d'établissement) comme clé d'accès au DP par les préparateurs en pharmacie est perçue comme une faille du système car n'offrant pas toutes les garanties de chiffrement requises par l'article R. 1110-3 CPS du décret « confidentialité » du 15 mai 2007 publié au JORF du 16 mai 2007. La loi autorise uniquement le pharmacien à accéder au DP par sa CPS alors que le décret sur le DP étend l'accès aux préparateurs par leur CPE. ZORN, Caroline. *Données de santé et secret partagé*. P. 386 - 387.

[822] Logiciel de gestion d'officine.

pharmaceutique. L'ensemble des données qui circulent entre l'hébergeur et les officines est chiffré (crypté)[823].

Finalement, il faut croire que le succès du web médecin et du DP par rapport au DMP est lié au fait qu'ils sont plus "partagés" (« *des traitements de données métiers*[824] ») que "personnels", destinés à l'usage exclusif de professionnels spécifiques : le DP pour les pharmaciens et le web médecin pour les médecins conventionnés[825]. Le DMP est le seul dossier qui a vocation à suivre le patient durant toute sa vie. Il est conçu pour permettre, grâce à une centralisation des informations, le partage des données utiles à la coordination des soins entre les professionnels et établissements appelés à le prendre en charge sur l'ensemble du territoire. C'est un nouveau mode de partage de données de santé qui est ainsi mis en œuvre. C'est le « dossier du patient » qui en maîtrise le contenu et les accès. Le patient a la possibilité d'accéder directement, depuis son ordinateur, à son dossier médical. Il peut désigner chacun des professionnels de santé à qui il souhaite ouvrir des droits d'accès et la possibilité de masquer des données qui y figurent[826].

En attendant qu'il soit véritablement généralisé et populaire, le terrain devrait lui être préparé par le web médecin et la DP s'ils jouent le rôle qui leur a été assigné dans le plus grand respect des droits des assurés. Mais, la Cour des comptes craint que les divergences entre les enjeux qui justifient leur mise en œuvre respective ne constituent un frein à une véritable éclosion des projets. Pour elle, en effet, une coordination accrue des objectifs poursuivis par les dossiers médicaux français s'avère nécessaire[827]. Les difficultés que connaît le déploiement du DMP sont communes à d'autres dossiers médicaux étrangers, pourtant, ils en sont différents.

---

[823] Un système de cryptage et de décryptage des données est implanté dans le LGO, permettant la lecture et l'écriture des informations. Ces opérations sont transparentes pour les pharmaciens. Les données sont donc ininterprétables directement. Il a été prévu chez l'hébergeur deux bases de données distinctes :
- la première contient des informations sur l'identité des patients,
- la seconde sur dispensation ayant alimenté le dossier pharmaceutique.
Le lien entre ces deux bases est assuré chez l'hébergeur par un système de cryptage permettant d'accéder aux informations de dispensation uniquement à partir de l'identité du patient et jamais l'inverse.

[824] ZORN, Caroline. *Données de santé et secret partagé*. P. 381.

[825] Idem

[826] CNIL. *La Cnil autorise le déploiement du dossier médical personnel sur l'ensemble du territoire*. 14 décembre 2010. http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-autorise-le-deploiement-du-dossier-medical-personnel-sur-lensemble-du-territoire/. Consulté le 3 mars 2011.

[827] Cour des comptes. *Rapport sur le financement de la sécurité sociale 2008*. P. 233.

2. Le dossier médical personnel et les dossiers médicaux électroniques étrangers

« Le DMP dans son concept « dossier médical personnel » n'a pas d'équivalent actuel dans les autres États. Il y existe bien des dossiers médicaux partagés qui ne sont pas destinés aux patients[828]» : affirmait le député Dominique GERBOD. Certes, certains s'en rapprochent mais ni leur cadre juridique, ni leur mise en œuvre ne sont identiques à celui du DMP. La plupart des États européens dont la Belgique, les Pays-Bas, le Royaume-Uni, la Suède se sont engagés dans la mise au point d'un dossier médical semblable. Ailleurs, les États Unis[829], le Canada[830], l'Australie et le Brésil ont fait de grandes avancées dans des projets d'envergure régionale non sans difficulté[831]. Les pays d'Asie ne semblent pas vraiment s'intéresser à cette forme de partage de données et l'Afrique n'en a pas encore les moyens même si des États comme le Mali[832] montrent un grand intérêt pour la télésanté. Nous nous intéresserons aux dossiers médicaux électroniques du Québec (au Canada) du fait du lien historique de la francophonie et de la collaboration entre les acteurs des systèmes d'information de santé de la France et du Québec, de la Suède pour leur état d'avancement relativement « exemplaire » et le dossier électronique de l'Espagne, pour son système juridique complexe.

---

[828] GERBOD, Dominique. Audition dans le *rapport n° 1847 (Assemblée nationale) ou n° 567 (Sénat) sur le dossier médical personnel (DMP) : quel bilan d'étape pour quelles perspectives ? (Compte rendu de l'audition publique du 30 avril 2009).* p. 101.

[829] Ministère des Affaires étrangères. *Les dossiers médicaux électroniques: plus de la moitié des médecins américains sont "high-tech".* Bulletins-electroniques.com. 31 mai 2013. http://www.bulletins-electroniques.com/actualites/73132.htm. Consulté le 21 avril 2014.

[830] SALEM, Géraldine. *La qualité de vie des patients atteints de maladies chroniques : Aspects comparés des systèmes français, suédois, canadien et américain*. Rapport 2010. *« En raison d'un territoire immense (9 984 670 km2), le Canada constitue un exemple particulièrement pertinent en matière de coordination de soins. Au Canada, le secteur de la santé est fortement axé sur l'information, depuis la loi du 1er avril 1984. Le gouvernement fédéral considère que en effet que grâce à une « bonne information », le médecin peut ordonner le bon traitement, prescrire le médicament approprié ou recommander la meilleure approche préventive possible. Toute personne qui possède les renseignements dont elle a besoin est plus en mesure de prendre les bonnes décisions en matière de santé et de style de vie. Le Canada a donc beaucoup misé sur un investissement dans les technologies de l'information et des communications notamment sur un système de « Dossier de Santé Electronique » (DSE), très proche du dossier médical personnel français, qui permet de recueillir des renseignements plus pertinents, plus opportuns et plus rapidement. »* www.fondationroche.org. Consulté le 04 juin 2012.

[831] Rapport d'information enregistré à la présidence de l'Assemblée nationale le 29 janvier 2008, déposé en application de l'article 145 du règlement par la Commission des affaires culturelles, familiales et sociales sur *le dossier médical personnel* et présenté par M. Jean-Pierre DOOR, député. I, A. http://www.assemblee-nationale.fr/13/rap-info/i0659.asp#p34_266743. Consulté le 04 juin 2012.

[832] Asip santé. *Le Mali, pionnier de la e-santé en Afrique.* Le MAG n° 11. 19 février 2014. http://esante.gouv.fr/en/node/4321. Consulté le 21 avril 2014.

a. Le dossier santé du Québec (DSQ)

De prime abord, relevons la différence entre le dossier médical électronique (DME) et le dossier santé électronique (DSE). L'Association canadienne pour la protection médicale (ACPM) précise que le DME fait habituellement référence à une version électronique du dossier papier utilisé depuis longtemps par les médecins pour consigner les informations sur leurs patients. Le DME peut être un système simple mis en place dans un cabinet ou un système plus complexe en réseau. En revanche, un DSE est, en général une compilation des renseignements importants provenant de multiples sources et peut être composé à partir de divers dossiers électroniques fournis par différents fournisseurs de différentes provinces ou différents territoires. Le DME contient tous les renseignements médicaux consignés dans le cadre des soins prodigués à un patient par un médecin et par conséquent, est complet dans un domaine donné. Toutefois bien que le DME ait de la profondeur, il manque de globalité puisqu'il ne contient généralement pas les interactions avec les autres professionnels de la santé. A l'inverse, le DSE offre de la globalité, mais n'a pas le degré de détail que l'on s'attend à trouver dans un dossier médical. Autrement dit, le DSE ne renferme pas nécessairement toute l'information contenue dans le DME[833]. Dans le cadre de cette étude, nous analyserons le DSE du Québec.

Le dossier santé du Québec se développe dans un cadre général de promotion[834] de dossiers de santé électroniques pancanadienne par l'intermédiaire d'Inforoute[835] santé du Canada. Le dossier de santé électronique est défini comme étant un dossier à vie, sécurisé et privé, sur les antécédents médicaux d'une personne, accessible de façon électronique par les

[833] ACPM. *Les dossiers de santé électroniques: perspectives de la responsabilité médicale*. Août 2008. p. 5. http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/pdf/com_electronic_health_records-f.pdf . ou sur www.cmpa-acpm.ca. Consulté le 18 septembre 2013.

[834] Ce vaste projet d'informatisation du réseau de santé du Canada est évalué à 500 millions de dollars canadiens (380 millions d'euros) et doit se poursuivre jusque fin 2015. ASIP santé. *Lancement du dossier santé Québec dans la région de Montréal*. 21 février 2012. Http://esante.gouv.fr/actus/politique-publique/lancement-du-dossier-sante-quebec-dans-la-region-de-montreal. Consulté le 18 septembre 2013.

[835] *« Financé par le gouvernement du Canada,* Inforoute *collabore avec les dix provinces et les trois territoires pour mettre en œuvre des systèmes de DSE privés et sécurisés, dont les meilleures pratiques et les projets réussis dans une région peuvent être partagés ou reproduits dans d'autres régions.* Inforoute *agit en tant qu'investisseur stratégique des fonds octroyés par le gouvernement fédéral, en collaboration avec les provinces et les territoires. »* https://www.infoway-inforoute.ca/index.php/fr/a-propos-dinforoute/ce-que-nous-faisons. Consulté le 07 juin 2012.

prestataires de soins de santé autorisés[836]. Le DSQ collecte seulement les renseignements de santé jugés essentiels[837] aux services de première ligne. Il s'agit des médicaments prescrits et obtenus en pharmacie au Québec, des résultats des analyses de laboratoire effectués au Québec, des résultats des examens d'imagerie médicale (radiographies, tomodensitométrie [scanner], imagerie par résonance magnétique [IRM], etc.) effectués au Québec, les vaccins reçus au Québec, le sommaire rédigé par le médecin traitant après une hospitalisation au Québec et les allergies et intolérances. Les renseignements sur les médicaments seront, généralement, les premiers disponibles. Les résultats des analyses de laboratoire et des examens d'imagerie médicale effectués dans le réseau public viendront ensuite. Les autres renseignements seront disponibles plus tard. Ces renseignements seront accessibles de façon graduelle, au fur et à mesure que les pharmacies, les cliniques et les établissements de santé du Québec seront branchés au DSQ.

Prévu pour être implanté progressivement partout au Québec à compter de l'été 2013[838], le gouvernement a mis en place un système d'information de la population pour les sensibiliser à l'adhésion massive au projet. Le portail[839] créé à l'intention des professionnels et des patients et de toute personne intéressée offre une panoplie d'informations techniques et juridiques relatives à l'encadrement du DSQ.

---

[836] ACPM. *Les dossiers de santé électronique : perspectives de la responsabilité médicale*. http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_electronic_health_records-f.cfm. Consulté le 18 septembre 2013.

[837] Le dossier santé du Québec ne collecte donc pas l'histoire personnelle et familiale; les rapports d'intervenants sociaux; les chirurgies, interventions ou traitements reçus dans le passé ; les notes d'évolution des médecins, des infirmières et des autres professionnelles de santé ; les électrocardiogrammes ; les chirurgies mineures effectuées en clinique ; les interventions effectuées en clinique externe. *Bonne nouvelle ! Le dossier santé Québec bientôt partout au Québec !* Dépliant d'informations sur le dossier santé Québec. Mai 2013. Ministère de la santé et des services sociaux. P.2 ou site Internet: http://www.dossierdesante.gouv.qc.ca. Consulté le 18 septembre 2013.

[838] La région de Montréal, quatrième concernée par le déploiement du projet d'informatisation du réseau de santé du Canada a été couverte en 2013. En effet, à partir du 30 mars 2013 un dossier informatique sera automatiquement constitué pour toutes les personnes inscrites au régime d'assurance maladie du Québec dont la résidence principale est à Montréal, à moins d'un refus express de l'usager. A l'issue de cette première phase de déploiement, 325 cliniques, 43 établissements de santé (hôpitaux, centres de réadaptation, etc.), ainsi que 428 pharmacies de Montréal seront reliés par le DSQ. Le système prévoit l'échange d'ordonnances entre médecins et pharmaciens, avec le consentement du patient. À la fin de cette phase, le nombre de dossiers médicaux électroniques passera à plus de 3 400 000 au Québec.
ASIP santé. *Lancement du dossier santé Québec dans la région de Montréal*. 21 février 2012. Http://esante.gouv.fr/actus/politique-publique/lancement-du-dossier-sante-quebec-dans-la-region-de-montreal. Consulté le 18 septembre 2013.

[839] http://www.dossierdesante.gouv.qc.ca/

Après quelques difficultés lors de sa mise en place, le dossier santé du Québec (DSQ), le DMP à la québécoise a pris son envol en 2010. Ce projet de dossier électronique ne partage pas que ces péripéties[840] du début avec le DMP mais, il n'y est pas non plus identique. Des différences sont notables tant au niveau du cadre de leur fonctionnement que des droits des titulaires des dossiers.

i. Le fonctionnement du DSQ

Le DSQ est mis en œuvre par le ministère de la santé et des services sociaux, la Régie de l'assurance maladie du Québec (RAMQ), avec une forte implication des régions. Dossier médical à l'intention de tout assuré à partir de 14 ans, il a été conçu pour soutenir la prestation des soins et des services de santé tout comme le DMP a été créé pour assurer la coordination des soins. Le projet québécois prévoit, pour cela, non seulement l'échange entre les médecins mais également, l'échange d'ordonnance électronique entre médecins et pharmacies, avec le consentement du patient. Inclus dans le cadre général du projet du Canada de création des dossiers de santé électroniques en vue de faire des économies de l'ordre de plusieurs dollars par an[841], les objectifs[842] inavoués de la création du DSQ visent, à terme, la réduction des dépenses de santé comme le DMP.

---

[840] FRASLIN, Jean-Jacques. *Pas d'année zéro pour le DMP québécois ! Le dossier de santé du Québec (DSQ) patine dans une pharmacie en attendant sa généralisation en 2011*. 29 mars 2010. http://www.i-med.fr/spip.php?article380. Consulté le 18 mai 2012.

[841] *« Les avantages du DSE seraient nombreux : il permettrait au système de santé canadien d'économiser 6 milliards de dollars chaque année, notamment en évitant 7,5 % des erreurs de médication lors d'une hospitalisation, 15 % de tests de laboratoire non nécessaires et 32 % des attentes indues à l'urgence dues à un manque d'information sur le patient. Comment ? Grâce au regroupement des renseignements dans le DSE et à leur circulation dans le réseau de la santé* ».
Union des consommateurs. *Le dossier de santé électronique : le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux*. 31 mars 2010. p. 10. http://Uniondesconsommateurs.ca/ docu/vieprivee/100331UC_CVPC_DSE.pdf Consulté le 26 mai 2012

[842] Article 10 des Conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec : « *Le dossier de santé a pour seuls objectifs :*
1° de fournir aux intervenants habilités de l'information pertinente, organisée, intégrée et à jour, afin de faciliter la prise de connaissance rapide des renseignements de santé d'une personne au moment de sa prise en charge ou lors de toute prestation de services de santé rendus par ces intervenants, en continuité et en complémentarité avec ceux dispensés par d'autres intervenants ;
2° d'assurer l'efficacité de la communication du Dossier de santé, aux seules fins de la prestation de services de santé à la personne concernée. »
http://www.dossierdesante.gouv.qc.ca/download.php?f=1c562fd76cee9365f461946bb4f2312d. Consulté le 26 mai 2012

Les deux dossiers partagent les mêmes principes directeurs : celui du respect de la vie privée des personnes et la protection des renseignements de santé[843]. Ces principes constituent le fil conducteur des décrets[844] pris par le gouvernement pour préciser les conditions de mise

[843] Au Québec, la protection des données de santé oblige au respect de la confidentialité des dossiers médicaux et des renseignements personnels régi par les articles 20 du code de déontologie des médecins, l'article 60.4 du code des professions et l'article 42 de la loi médicale.

[844] Plusieurs décrets se sont succédés dans la mise en place du cadre légal du dossier santé Québec.

Décret 404-2008 28 avril 2008 qui définissait les conditions de mise en œuvre du projet expérimental du dossier de santé du Québec. C'est dans ce cadre que le dossier a débuté en 2008 dans la région de la capitale-nationale. Décret 404-2008, 23 avril 2008. Gazette officielle du Québec, 7 mai 2008, 140e année, n° 19. P. 1979. http://www.dossierdesante.gouv.qc.ca/fichier/Decret-404-2008.pdf. Consulté le 28 mai 2012

- Décrets 757-2009 du 18 juin 2009, Gazette officielle du Québec, 8 juillet 2009, 141eme année, n° 27. p.3162 portant *conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec*. http://www.dossierdesante.gouv.qc.ca/fichier/Decret-757-2009.pdf.

et 566-2010 du 23 juin 2010 (Modification du décret du 18 juin 2009). Gazette officielle du Québec, 14 juillet 2010,142ème année, n° 28. P. 3111.

Http://www.dossierdesante.gouv.qc.ca/fichier/Decret-566-2010.pdf Consulté le 28 mai 2012

« *La mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé repose sur le respect des principes suivants :*

1° le respect du droit à la vie privée de la personne et au secret professionnel ;

2° la transparence, en ce que les personnes visées à l'article 6 doivent être préalablement informées des objectifs de la deuxième phase du projet expérimental ainsi que des finalités et des modalités de fonctionnement du Dossier de santé. À cet effet, un Document d'information concernant la deuxième phase du projet expérimental, publié notamment sur le site Internet du ministère de la Santé et des Services sociaux, est remis à la demande de personnes intéressées ;

3° la participation volontaire, en ce que la personne demeure libre en tout temps de refuser d'avoir un Dossier de santé ;

4° la non-discrimination, en ce que chaque personne doit demeurer entièrement libre de refuser, en tout temps, la constitution pour elle-même d'un Dossier de santé et que ce refus ne doit aucunement mettre en cause son droit d'avoir accès et de recevoir les services de santé que requiert son état ;

5° la limitation de l'utilisation et de la communication des renseignements, en ce que les renseignements contenus dans le Dossier de santé d'une personne ne doivent être utilisés que pour les fins prévues à l'article 10 et ne doivent être communiqués qu'à des intervenants habilités, lorsque leur communication est nécessaire à l'exercice de leurs fonctions ;

6° les droits d'accès et de rectification, en ce que la personne :

a) a un droit d'accès aux renseignements que détiennent les entités visées à l'article 1, aux nom et prénom des intervenants ou à l'identifiant du système informatique muni d'un certificat d'objet qui les ont transmis ainsi qu'à la date de transmission de ces renseignements ;

b) a un droit d'accès à son Dossier de santé, aux nom et prénom de l'intervenant qui l'a consulté ainsi qu'à la date de cette consultation ;

c) peut exiger que des renseignements inexacts, incomplets ou équivoques la concernant et détenus par les entités visées à l'article 1 ou que contient son Dossier de santé ou dont la collecte, la conservation ou la communication n'est pas autorisée soient rectifiés ;

7° les droits de recours, en ce que toute personne a le droit de porter plainte auprès :

a) d'une personne responsable de l'accès aux documents et de la protection des renseignements personnels au sein d'une entité visée à l'article 1 ;

b) du responsable de la coordination centrale des demandes d'accès et de rectification et des plaintes visé à l'article 110 ;

c) de la Commission d'accès à l'information ;

d) du Ministre ;

8° la responsabilité et l'obligation de rendre compte, en ce que les entités visées à l'article 1 de même que les établissements et les intervenants visés à l'article 4 doivent s'assurer du fonctionnement adéquat des mesures et mécanismes mis en place, sous leur responsabilité, pour assurer la sécurité des actifs informationnels concernés et la confidentialité des renseignements ;

en œuvre des phases du projet expérimental du dossier de santé du Québec. Les décrets ont fait suite à la loi[845] modifiant la loi sur les services de santé et les services sociaux et d'autres dispositions législatives dite *« projet de loi n° 83[846] »*. Adopté le 25 novembre 2005 et sanctionné le 30 novembre de la même année, ce texte a jeté les bases de la mise en œuvre du DSQ sans en donner les détails d'exécution. Cette loi consacrait déjà les principes[847] qui ont été réaffirmés par les décrets. En 2012, le projet de loi n° 59 modifiant, entre autres, la loi sur les services de santé et les services sociaux et d'autres dispositions législatives, a permis l'adoption de la loi concernant le partage de certains renseignements de santé[848]. « *Cette loi a pour objet la mise en place d'actifs informationnels permettant le partage de renseignements de santé jugés essentiels aux services de première ligne et au continuum de soins, afin d'améliorer la qualité et la sécurité des services de santé et des services sociaux ainsi que l'accès à ces services. La loi a également pour objet d'améliorer la qualité, l'efficience et la performance du système québécois de santé en permettant une gestion et une utilisation*

9° la sécurité des actifs informationnels, en ce que les entités visées à l'article 1 doivent mettre en place un ensemble de mesures et de mécanismes visant à assurer la disponibilité, l'intégrité et la confidentialité des renseignements qu'ils détiennent. »

[845] Paragraphe 7 des notes explicatives du « projet de loi n° 83»: « *Le projet de loi instaure aussi des mécanismes visant la mise en place de services régionaux de conservation de certains renseignements de santé concernant une personne qui y consent. La mise en place de ces services vise à fournir aux intervenants habilités de l'information pertinente et à jour afin de faciliter la prise de connaissance rapide des renseignements de santé d'une telle personne au moment de sa prise en charge ou lors de toute prestation de services de santé fournis par ces intervenants, en continuité et en complémentarité avec ceux dispensés par d'autres intervenants. La mise en place de ces services vise de plus à assurer l'efficacité de la communication ultérieure des renseignements conservés par une agence ou un établissement autorisé par le ministre à offrir ces services, aux seules fins de la prestation de services de santé. »*
http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2005C32F.PDF. Consulté le 28 mai 2014.

[846] *Loi modifiant la loi sur les services de santé et les services sociaux et de dispositions législatives*. Projet de loi numéro 83 (2005, chapitre 32). Assemblée nationale. Édition officielle du Québec 2005. http://www2. publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2005C32F.PDF. Consulté le 28 mai 2014.

[847] Paragraphe 9 des notes explicatives du « projet de loi n° 83 » : « *Le projet de loi énonce un certain nombre de principes qui reconnaissent les droits des personnes concernées à l'égard des renseignements conservés par une agence ou un établissement autorisé et suivant lesquels les dispositions législatives devront être appliquées. Des modifications sont aussi proposées à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels afin d'ajouter aux fonctions exercées par la Commission d'accès à l'information celle de veiller au respect de la protection des renseignements ainsi conservés »*
http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2005C32F.PDF. Consulté le 28 mai 2014.

[848] *Loi concernant le partage de certains renseignements de santé*. Projet de loi n° 59 (2012, chapitre 23). Assemblée nationale. Édition officielle du Québec 2012. Http://www.dossierdesante.gouv.qc.ca/fichier/Loi-concernant-le-partage-de-certains-renseignements-de-sante.pdf. Consulté le 10 Août 2012.

maîtrisée de la formation sociaux sanitaires[849] ». Sanctionnée le 18 juin 2012 les dispositions de ce texte entrent, graduellement en vigueur à la date ou aux dates déterminées par le gouvernement[850].

Pour accéder aux renseignements de santé de leur patient, les professionnels[851] de santé sont authentifiés et identifiés[852] par une clé publique accompagnée d'un mot de passe comme le permet la carte CPS pour le DMP. Cet accès les conduit aux bases de données des établissements de santé et des pharmacies participant au projet expérimental pour y consulter le dossier du concerné[853]. Tout comme le DMP *« permet le regroupement et le partage entre les professionnels et établissements de santé des informations jugées utiles à la coordination des soins*[854], le DSQ relie *« les établissements de santé, les pharmacies, les cliniques médicales et les cabinets privés, les groupes de médecins de famille, les laboratoires et les centres d'imagerie diagnostique. L'information essentielle sur le patient provenant de ces*

[849] *Loi concernant le partage de certains renseignements de santé*. Sanctionné le 18 juin 2012. PL: 59. Chapitre P-9.0001. Dispositions générales, Titre I, article 1. p.5. http://www.dossierdesante.gouv.qc.ca/fichier/Loi-concernant-le-partage-de-certains-renseignements-de-sante.pdf ou http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2012C23F.PDF. Consulté le 10 Août 2012.

[850] *Décret n° 323-2013, du 27 mars 2013* loi concernant le partage de certains renseignements de santé (2012, chapitre 23). Gazette officielle du Québec, 10 avril 2013,145e année, n° 15. p1415.

[851] Les articles 68 et 69 de la loi concernant le partage des certains renseignements de santé donne la liste des intervenants autorisés à Consulté les renseignements collectés par le dossier santé Québec. Ce sont les médecins, les infirmières, les pharmaciens, les sages-femmes, les archivistes médicales, les biochimistes, les infirmières auxiliaires, les microbiologistes, les résidents et stagiaires en médecine et en pharmacie ainsi que les personnes qui agissent en soutien technique auprès des médecins et des pharmaciens. Ces intervenants doivent obtenir des droits d'accès pour être autorisés à Consulté le dossier santé. . Ces droits d'accès sont accordés par règlement du ministère en fonction du rôle professionnel de chaque personne. Ils définissent les renseignements qui peuvent être consultés. Certains intervenants autorisés ont accès à une partie seulement des renseignements accessibles au dossier alors que d'autres sont autorisés à accéder à la totalité de ces renseignements (Voir tableau du site Internet: http://www.dossierdesante.gouv.qc.ca/population/Comment-fonctionne-leDSQ/index.php?Lacces_aux_renseignements.). Consulté le 10 Août 2012.

[852] L'identification unique des intervenants, comme celle des usagers, s'avère essentielle. L'Assemblée nationale a adopté, le 5 décembre 2007, le projet de loi n° 51 (2008, chapitre 31), qui instaure un « registre des intervenants du secteur de la santé et des services sociaux » qui permettra d'attribuer un numéro d'identification unique à de tels intervenants ainsi que de recueillir, maintenir à jour, normaliser et rendre accessibles, selon les besoins, les données les décrivant.
Ministère de la santé et des services sociaux du Québec. *Dossier santé du Québec, rapport d'étape Septembre 2008*. P. 27. http://collections.banq.qc.ca/ark:/52327/bs1811704. Consulté le 26 mai 2012.

[853] Article 19 des conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec. http://www.dossierdesante.gouv.qc.ca/download.php?f=1c562fd76cee9365f461946bb4f2312d. Consulté le 26 mai 2012.

[854] CNIL. *La CNIL autorise le déploiement du dossier médical personnel sur l'ensemble du territoire*. 14 décembre 2010. http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-autorise-le-deploiement-du-dossier-medical-personnel-sur-lensemble-du-territoire/. Consulté le 26 mai 2012.

différents points de services sera centralisée et archivée dans des entrepôts de conservation sécurisés[855]. » L'agence[856] responsable de ces entrepôts est désignée par le ministère de la santé et des services sociaux pour conserver non pas la totalité des informations contenues dans le DSQ, comme c'est le cas de l'hébergeur du DMP, mais une partie constituée des renseignements dont certains sont « *convenus entre l'intervenant habilité et la personne concernée*[857] ». Ce sont : le numéro d'identification unique de la personne concernée ; ses contacts professionnels ; ses allergies et intolérances pouvant avoir une incidence sur sa santé ou sa prise en charge ; ses données d'immunisation ; les données d'urgence et les renseignements complémentaires qui la concernent.

Pour donner un cadre juridique adéquat à ces actions la loi concernant le partage de certains renseignements de santé reprend la liste des droits des patients en son article 2[858].

ii. Les droits des assurés sur leur DSQ

L´article 2[859] précité dispose : *« les dispositions de la présente loi doivent être appliquées et interprétées de manière à respecter les principes suivants :*

1° le droit à la vie privée de la personne et au secret professionnel

---

[855] Union des consommateurs. *Le dossier de santé électronique : le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux*. 31 mars 2010. P. 10. http://Uniondesconsommateurs.ca/docu/vieprivee/100331UC_CVPC_DSE.pdf. Consulté le 26 mai 2012.

[856] Article 18, Décret 757-2009 du 18 juin 2009, Gazette officielle du Québec, 8 juillet 2009, 141eme année, n° 27. p.3162 portant *conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec*. http://www.dossierdesante.gouv.qc.ca/fichier/Decret-757-2009.pdf. Consulté le 26 mai 2012.

[857] Article 7, 1° et 4° du second alinéa: « *ses contacts professionnels et les données d'urgence et les renseignements complémentaires* » Décret 757-2009 du 18 juin 2009, Gazette officielle du Québec, 8 juillet 2009, 141eme année, n° 27. p.3162 portant *conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec*. http://www.dossierdesante.gouv.qc.ca/fichier/Decret-757-2009.pdf. Consulté le 26 mai 2012.

[858] L'article 2 de la loi concernant le partage de certains renseignements de santé qui rappelle les droits des patients quant à la gestion de leurs renseignements personnels dans le cadre du dossier de santé est entré en vigueur le 4 juillet 2012. Décret 788-2012, 4 juillet 2012. Gazette officielle du Québec, 18 juillet 2012, 144eme année, n° 29. P. 3669.

[859] L'article 2 rappelle d'autres droits relatifs au traitement de toutes les données à caractère médical et non pas seulement le dossier santé Québec : la protection des renseignements de santé, les droits d'accès et de rectification, les droits de recours auprès de la Commission d'accès à l'information et un droit de réparation en cas de responsabilité et d'imputabilité du Ministère et la Régie de l'assurance maladie du Québec pour des problèmes de fonctionnement adéquat des actifs informationnels.

2° la transparence, en ce que les personnes doivent être informées des finalités des actifs informationnels mis en place par la présente loi, particulièrement du dossier santé Québec, et de leurs règles de fonctionnement ;

3° le droit de toute personne de manifester en tout temps son refus à ce que les renseignements de santé la concernant soient communiqués au moyen du dossier santé Québec ;

4° la non-discrimination en ce que la décision d'une personne de refuser le partage des renseignements de santé la concernant ne doit aucunement mettre en cause son droit d'avoir accès et de recevoir les services de santé que requiert son état de santé ;».

Les droits des patients ainsi énumérés sont identiques à ceux défendus par le cadre juridique du dossier médical personnel français. Cependant, alors que le DMP est créé à l'initiative du patient ou sur proposition du professionnel de santé mais avec l'accord express du concerné, le DSQ est créé avec l'accord implicite[860] de son titulaire. Le DSQ est généré pour chaque assuré social résidant sur le territoire de la région participant à l'opération de déploiement sauf refus explicite préalable de ce dernier [861]; la possibilité lui étant donnée de revenir, plus tard, sur sa décision. Le dossier de santé québécois est, ainsi, automatiquement créé sans l'accord exprès de l'assuré. Néanmoins, il garde le droit de refuser[862] de se voir attribuer un DSQ, postérieurement à la création sans que cette décision ne le prive des services de santé et

---

[860] *« Dans le plan d'affaires 2007-2010 du DSQ, il est mentionné que le cadre juridique exige que la population donne par écrit son consentement au partage des informations et des données cliniques qui pourront être consultées par les intervenants habilités selon le profil d'accès attribué. Le nombre de consentements obtenus auprès de la population est donc un levier essentiel à l'adhésion des cliniciens. Par ailleurs, au moment de mettre en place les diverses stratégies d'obtention du consentement, les gestionnaires et les professionnels de la santé, incluant les médecins, ont exprimé leurs craintes quant à la lourdeur de la gestion de la collecte du consentement explicite pour l'ensemble de la population québécoise. La complexité des processus et la gestion en cause ont fait ressortir les coûts élevés des mesures qui devraient être déployées pour recueillir, conserver, renouveler, révoquer et gérer ce type de consentement.*
Devant ces constats, le ministre de la Santé et des Services sociaux, M. Philippe Couillard, déposait, le 18 décembre 2007, le projet de loi n° 70 à l'Assemblée nationale afin d'introduire une approche de consentement implicite avec droit de refus en remplacement d'une approche de consentement explicite. Les partis d'opposition ainsi que les fédérations médicales ont applaudi cette décision adoptée par l'Assemblée nationale du Québec le 27 mai 2008. »
Ministère de la santé et des services sociaux du Québec. *Dossier santé du Québec, rapport d'étape Septembre 2008.* P. 27. http://collections.banq.qc.ca/ark:/52327/bs1811704. Consulté le 26 mai 2012.

[861] Article 6 des conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec. http://www.dossierdesante.gouv.qc.ca/download.php?f=1c562fd76cee9365f461946bb4f2312d. Consulté le 26 mai 2012.

[862] Le refus peut se faire en ligne sur le site dédié au dossier de santé ou par courrier postal ou par téléphone muni de sa carte d'assurance maladie. Le refus d'un mineur de moins de 14 ans est exprimé par l'un de ses parents (ou son tuteur légal ou tout autre détenteur de l'autorité parentale. Quant au majeur incapable, il est représenté par son curateur ou son mandataire).

de soins que son état requiert[863]. En France, la loi[864] précise que le refus de création du DMP n'a pas de répercussion sur les remboursements de soins, mais la législation québécoise reste moins expressive. Affirmer que le refus n'empêche pas que l'on bénéficie des soins, ne veut pas clairement dire que la part qui incombe à la RAMQ sera remboursée à celui qui refuse qu'on lui crée un DSQ. Une précision dans ce sens nous semble nécessaire pour éviter toute ambiguïté d'autant plus que l'assuré pourrait souffrir de marginalisation en cas de refus. En outre, la relation patient-professionnel de santé qui met le premier dans un état de reconnaissance contraindra moralement, de nombreuses personnes à ne pas manifester de refus même si l'idée de partage de leurs données de santé ne les réjouit pas beaucoup. Dans ces cas, le consentement implicite ne refléterait pas la volonté de l'assuré ou, du moins, serait entaché de vice.

L'opposition à la gestion d'un DSQ pour le patient aura pour effet d'empêcher la consultation de son dossier par les professionnels qui auraient été habilités à y accéder[865]. Mais, les renseignements de santé recueillis avant l'expression du refus demeureront accessibles aux professionnels de la santé qui les avaient consultés avant[866]. Cette dernière possibilité nous semble de nature à annihiler ce droit de refus qui a été reconnu à l'assuré. En effet, dans l'hypothèse où celui-ci tenait à garder secrètes les informations qui ont justement déjà été consultées par les premiers professionnels, il ne peut plus jouir de son droit à l'oubli car il n'a plus aucun moyen d'empêcher leur accès. Pour éviter de se retrouver dans cette situation, l'assuré dispose de 21 jours après l'annonce par le ministre de la date à laquelle vont débuter les travaux d'implantation du projet[867]. Ce délai nous semble relativement court

[863] Le ministère de la santé et des services sociaux envoie un formulaire de refus à l'assuré en l'informant qu'aucune formalité n'est à remplir pour participer au DSQ et qu'il a le droit de refuser l'accès à ses renseignements de santé. Le renvoi de formulaire dûment rempli et signé indique la volonté du patient de refuser de participer au projet DSQ.

[864] L'article 50 de la loi du 21 juillet 2009 a supprimé l'alinéa deuxième de l'article L. 166-36-2 du code de la sécurité sociale qui disposait que « *le niveau de prise en charge des actes et prestations de soins par l'assurance maladie (...) est subordonné à l'autorisation que donne le patient, à chaque consultation ou hospitalisation, aux professionnels de santé auxquels il a recours, d'accéder à son dossier médical personnel et de le compléter. Le professionnel de santé est tenu d'indiquer, lors de l'établissement des documents nécessaires au remboursement ou à la prise en charge, s'il a été en mesure d'accéder au dossier*. »

[865] En cas d'essai d'intrusion dans le dossier, une application indiquera la mention du refus et aucune consultation ne sera possible.

[866] Dans ce cas, le nom du consultant, la date et la justification de cet accès sont tracés.

[867] Ministère de la santé et des services sociaux. *Document d'information concernant la mise en œuvre de la deuxième phase d'expérimentation du dossier de santé du Québec*. P. 4. Mise à jour le 10 juin 2010.

malgré la campagne qui est menée autour du projet de mise en place du DSQ. De plus, même si nul n'est censé ignorer la loi, plusieurs personnes, même désireuses de refuser le DSQ, ne pourront pas exercer leur droit dans le délai soit par ignorance, soit par négligence, soit par manque de temps ou de moyens (accès internet ou moyen financier pour le timbre). Finalement, le système adopté pour la création du DMP (informer le patient et recueillir son consentement à l'occasion d'une consultation par exemple ou attendre qu'il en manifeste le désir) nous paraît plus respectueuse de la liberté du patient. Mais, il ne faut pas perdre de vue le fait que peu importe la solution choisie, les informations portées à la connaissance du patient pour le guider dans son choix doivent être suffisamment claires sur les conséquences de leurs choix sur le sort de leurs données de santé qui figureront dans le dossier médical électronique.

C'est un outil mis à la disposition des professionnels de santé autorisés pour leur permettre d'accéder rapidement à des renseignements jugés essentiels pour la prise en charge efficiente de leur patient. C'est donc un dossier « métier » contrairement au DMP qui est surtout personnel. Dès lors, l'assuré n'y a pas d'accès direct[868], ni de droit de masquage mais il peut exercer un droit de rectification et, même, de porter plainte par l'intermédiaire d'un responsable de coordination centrale des demandes d'accès, des rectifications et des plaintes. L'assuré n'a pas, non plus, de droit d'opposition sur les renseignements les plus importants. En revanche, de concert avec son médecin, il peut occulter le nom et les coordonnées de certains professionnels de santé qui l'ont ausculté ainsi que certaines données d'urgence et des renseignements complémentaires. Une question préoccupe, cependant l'Association canadienne de protection médicale (ACPM) qui se pose la question de savoir qui est propriétaire du dossier de santé électronique au Canada. Lorsque le dossier médical était sur support papier il était clairement établi par les tribunaux[869] que le propriétaire est l'établissement de santé, la clinique ou le médecin qui le tient et en contrôle l'accès. Aujourd'hui, avec le dossier de santé électronique, ces personnes et ces entités sont dites

---

http://www.dossierdesante.gouv.qc.ca/download.php?f=df11f15de2c7fbb8788186012489e4c7. Consulté le 26 mai 2012.

[868] Pour connaître le contenu de son dossier de santé le patient doit faire une demande adressée au responsable de l'accès des documents et de la protection de renseignements personnels. Les responsables de l'accès disposent d'un délai maximal de 20 jours pour traiter la demande, par la possibilité d'une prolongation de 10 jours sur préavis. Les frais peuvent être appliqués à cette demande.

[869] « *Les dossiers médicaux du patient, en tant que supports, appartiennent au médecin* ». Cour suprême du Canada. 11 juin 1992. McInerney c. MacDonald, [1992] 2 R.C.S. 138. Dossier 21899. http://csc.lexum.org/fr/1992/1992rcs2-138/1992rcs2-138.html. Consulté le 5 novembre 2011.

« gestionnaires de données » car ils sont responsables de la gestion de l'information contenue dans le dossier de santé électronique. La possibilité que le patient soit le propriétaire de son dossier n'est pas envisagé dans le système canadien. La question de la propriété reste donc toujours sans réponse dans les textes qui encadrent les dossiers de santé électronique pancanadien. C'est pourquoi l'ACPM encourage tous les participants à un dossier de santé électronique, y compris les médecins, les autres professionnels de santé, les centres hospitaliers, les autorités sanitaires et les gouvernements à s'assurer que leur rôle concernant la propriété et la gestion de l'information dans un dossier de santé électronique soit clairement défini[870]. Une bonne définition des rôles permet de rassurer le patient quant à la personne responsable de la gestion de l'information sur sa santé et lui donne un meilleur contrôle sur son information dans un système de dossier de santé électronique.

L'accès au DSQ par les professionnels de santé n'a pas la même étendue pour tous. Si l'autorisation d'accès à un établissement de soins ouvre droit à tout professionnel faisant partie de l'équipe de soins à la consultation du DMP, les professionnels de santé n'accèdent qu'aux informations jugées nécessaires en fonction de la matrice d'habilitation[871]. Les personnes autorisées à consulter le DSQ sont également limitées dans leurs actes en fonction de leur rôle et de leur responsabilité[872] dans un souci de préservation de la confidentialité des renseignements contenus dans les dossiers médicaux et pharmaceutiques. Pour assurer davantage la protection des droits du titulaire, le système prévoit une traçabilité de toute intervention ou de tout accès au DSQ, tout comme le DMP, de manière à en garantir l'intégrité et les éléments de preuve pour d'éventuels recours en cas d'infraction. Ce qui fait moins la préoccupation des législateurs tant au Québec qu'en France, c'est la sécurité des données personnelles des professionnels de santé qui restent tracés dans les dossiers médicaux électroniques. L'ACPM attire l'attention des décideurs sur cet aspect[873].

---

[870] ACPM. *Les dossiers de santé électronique : perspectives de la responsabilité médicale*. http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_electronic_health_records-f.cfm. Consulté le 5 novembre 2011.

[871] La matrice est consultable sur le site dédié au DMP http://www.dmp.gouv.fr/web/dmp/matrice-d-habilitations-des-professionnels-de-sante. Consulté le 31 mai 2012.

[872] Section 1 du chapitre IX (articles 112 à 117) des conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec.
http://www.dossierdesante.gouv.qc.ca/download.php?f=1c562fd76cee9365f461946bb4f2312d. Consulté le 31 mai 2012.

[873] *« Les interventions posées par les professionnels de la santé et l'information connexe pourront être accessibles dans un système de dossiers électroniques (p. ex., le nombre de patients, les pratiques en matière*

Le Québec a mis en place un cadre juridique plus propice à la bonne marche de son projet DSQ par l'adoption des décrets établissant les conditions de sa mise en œuvre. A côté, certains organismes de réglementation de la médecine au Canada ont publié des cadres conceptuels de gestion de l'information, des lignes directrices ou des politiques sur la gestion des dossiers patients en format électronique pour aider les médecins à mieux comprendre comment gérer l'information des patients dans un environnement de DSE. Quant à l'ACPM, en collaboration avec l'association médicale canadienne (AMC) a publié un document intitulé *« Ententes sur le partage de données : Principes applicables aux dossiers médicaux électroniques/dossiers de santé électroniques*[874] » pour donner une orientation aux médecins et à tous les participants au projet. Tout cela contribue à faire prendre au DSQ une avance sur le DMP qui attend encore, aujourd'hui (18 septembre 2013), son décret d'application pour donner plus de précisions relatives à sa mise en œuvre. La création d'un dossier de santé électronique pancanadien est la prochaine étape de l'évolution des dossiers médicaux électroniques au Canada. Compte tenu de cet état d'avancement, une coopération entre la France et le Québec dans le domaine des dossiers médicaux électroniques est une initiative enrichissante. L'ASIP santé collaborant avec le ministère de la santé et des services sociaux québécois. Les échanges permettent de comparer les expériences et d'établir une coopération qui a conduit à une interopérabilité sémantique des systèmes d'information de santé. La

---

d'ordonnance, les taux d'infection). Bien que le rôle des professionnels de la santé dans la société puisse exiger l'accès à leurs « renseignements personnels », il importe de prendre en considération qui devrait avoir accès à cette information et comment elle peut être utilisée et divulguée. L'ensemble des provinces et des territoires au Canada ont des lois sur la protection des renseignements personnels. Il n'en demeure pas moins que dans certaines circonstances aucune loi ne pourrait s'appliquer aux renseignements personnels des professionnels de la santé. Peu importe si une telle loi existe ou non, les professionnels de la santé devraient être informés de quelle manière on compte accéder, utiliser ou divulguer leurs renseignements, et devraient avoir la possibilité de donner ou de refuser leur consentement. Il faudrait favoriser une approche pondérée pour l'utilisation et la divulgation des renseignements personnels des professionnels de la santé. (…) Tel que discuté précédemment, il est reconnu que les renseignements personnels des professionnels de la santé peuvent être tirés des DSE et servir à la planification des systèmes de santé. Dans la mesure où l'information sur les professionnels de la santé est utilisée à cet égard, l'ACPM est d'avis qu'il serait possible de protéger la confidentialité liée aux professionnels de la santé en tant qu'individu en utilisant ces renseignements en agrégat et sans identification. » ACPM. *Les dossiers de santé électronique : perspectives de la responsabilité médicale*. http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_electronic_health_records-f.cfm. Consulté le 31 mai 2012.

[874] ACPM. *Les dossiers de santé électroniques : perspectives de la responsabilité médicale*. http://www.cmpa-acpm.ca/cmpapd04/docs/submissions_papers/com_electronic_health_records-f.cfm. Consulté le 31 mai 2012.

production de référentiels communs à l'ensemble de la francophonie est la première étape de la recherche de possibilités de coopération industrielle entre la France et le Québec[875].

b. Le dossier patient national de la Suède (NPÖ)

Le dossier médical électronique suédois est le premier système gérant les données médicales dans leur globalité et c'est également l'un des premiers de ce type au niveau mondial. Pour la Suède, ce projet constitue le pilier de l'implémentation d'une stratégie nationale dans le secteur des soins de santé.

La mise en place du projet NPO (National Patient Overview) ou « Nationell patientöversikt » s'est faite dans la même période que le dossier médical français. Le NPÖ, littéralement, « Résumé Patient National » est, en Suède, la plate-forme nationale d'informations des patients sur la santé. Ayant pour objectif de faciliter les échanges de données entre les acteurs du secteur médical, il permet aux professionnels de santé d'accéder aux données de santé de leurs patients et d'avoir une meilleure vision d'ensemble de l'état de santé de ces derniers. Les diagnostics s'en trouvent alors, plus ajustés tout comme dans le cas du DMP français et cela facilite également le parcours des patients. Le NPO ne remplace pas les dossiers médicaux traditionnels mais il permet seulement de rendre plus accessibles certaines données à un plus grand nombre d'établissements de soins. Il s'agit des informations concernant les établissements où le patient a reçu des soins, les médicaments prescrits, les diagnostics. Le maître d'œuvre du projet NPÖ est le « Sjukvårdsrådginvningen », en abrégé, SVR AB, l'équivalent de l'ASIP santé de France. Le SVR AB a pour mission de développer les nouvelles technologies de l'information et de la communication en matière de santé dans le cadre de l'article 18[876] de la loi suédoise sur les données personnelles.

[875] ASIP santé. *Le Québec à l'honneur des huitièmes journées internationales des industriels*. 15 décembre 2011. Http://esante.gouv.fr/actus/services/le-quebec-a-l-honneur-des-8emes-journees-nationales-des-industriels. Consulté le 31 mai 2012.

[876] L'article 18 fixe les conditions dans lesquelles les données sensibles de santé peuvent être traitées: lorsque les données sont nécessaires à la médecine préventive, les soins de santé, les diagnostics médicaux, l'administration de soins ou la gestion des services de soins et des hôpitaux.

Une récente étude[877] réalisée auprès des professionnels de santé de la municipalité de Örebro a permis de mettre en exergue l'intérêt des patients pour ce service et son utilité pour les professionnels. 90% des derniers déclarent être satisfaits et 60% le reconnaissent utile pour leur travail.

Il n'existait pas de législation spécifique en la matière jusqu'en mai 2008. En effet, le Riksdag[878] a adopté une loi sur la protection et l'administration des données personnelles de santé qui est entrée en vigueur le 1er juillet 2008[879]. Ce texte, adapté à la législation sur le traitement des toutes les données personnelles existante[880], permet, non seulement, de clarifier les règles régissant les échanges électroniques de données personnelles de santé entre les prestataires de soins, mais également de préciser les droits des patients sur leurs données de santé recueillies et des conditions très strictes de contrôle de l'accès auxdites données.

[877] *ePractice Editorial Team. National patient summary users are satisfied, says survey. 23 mars 2012.* www.epractice.eu/en/news/5347051. Consulté le 31 mai 2012.

[878] Le Parlement suedois.

[879] « Patientdatalag (SFS 2008 : 355)». http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Patientdatalag-2008355_sfs-2008-355/?bet=2008:355. Consulté le 29 mai 2014.
La loi 2008: 355 a été complétée par l'ordonnance sur les données patient (SFS 2008: 360, patientdataförordningen) du 29 mai 2008 et mise à jour par l'ordonnance 2013:124 entrée en vigueur le 1er Avril 2013.

[880] Plusieurs sources servaient de base à la gestion informatisée des données de patients : La première loi règlementant le traitement des données personnelles était la loi informatique et libertés (SFS 1973: 289, datalag) modifiée après transposition de la Directive 95/46/CE et devenue la loi suédoise sur les données à caractère personnel (SFS 1998: 204, personuppgiftslag); la loi sur les dossiers patients (1985 : 562) dite patientjournallagen et la loi sur le registre des soins de santé (1998 : 543, lagen om hälsodataregister) du 11 juin 1998; la loi sur l'agence suédoise de données à caractère personnel (SFS 1998:204,personuppgifslag) du 29 Avril 1998; la loi sur les biobanques dans les soins de santé : medical care act, (SFS 2002 : 297) du 23 mai 2002; la loi sur la prévention médicale, la recherche et le traitement des madies et des blessures (SFS 1982 :763, halso-och sjukvårdslagen) du 30 juin 1982.

i. Les droits des patients

Le gouvernement suédois, dans, le but de répondre au droit à l'information du citoyen, a mis en place un site Internet[881] à l'intention des professionnels et des patients. Les documents publiés dans les centres de santé sont rédigés dans un suédois simple et clair accessible à tous les citoyens[882].

Le patient suédois, libre d'en décider la création, est propriétaire de son dossier médical électronique dont le droit d'accès est laissé à sa discrétion. Tout comme en France, le patient peut consulter directement son dossier en ligne et gérer son utilisation et sa mise à disposition. De ce fait, il est informé de l'utilisation qui est faite de ses données médicales. Les informations qui lui sont donc transmises sont celles portant sur : la personne en charge du contrôle des données et les destinataires du traitement, la finalité du traitement, les catégories de données en cours de traitement, les obligations d'information découlant de la loi ou du règlement, des mesures prises pour la confidentialité et la sécurité de ses données, son droit d'accès au dossier et les modalités pour y parvenir, son droit de rectification, son droit aux dommages et intérêts en cas de traitement de ses données outrepassant la finalité prédéfinie, les conditions de conservation et d'allégement du contenu et son droit d'exprimer sa volonté quant au traitement de ses données[883]. Le patient est également informé de son droit de faire retirer à tout moment certaines données de son dossier. Les noms des éventuels destinataires des traitements lui sont communiqués tout comme les sources de recueil de ses données (lui-même ou des informations provenant des proches ou d'autres centres de santé[884]). Son droit de restriction lui est aussi notifié[885]. En effet, le patient aura le droit de bloquer l'accès à son dossier pour certains professionnels de santé. Ainsi une partie de son dossier sera verrouillée et ne sera accessible qu'aux professionnels pour lesquels le patient donnera son autorisation. C'est le droit de masquage du patient suédois. Il est exercé dans des conditions similaires à celles du droit de masquage[886] du patient français sur son DMP. Pour

[881] www.nationellpatientöversikt.se

[882] chapitre 3 paragraphes 13. Patientdatalag (SFS 2008 : 355).

[883] Chapitre 8, paragraphe 6. Patientdatalag (SFS 2008 : 355).

[884] chapitre 7, paragraphe 3. Patientdatalag (SFS 2008 : 355).

[885] chapitre 6, paragraphe 2. Patientdatalag (SFS 2008 : 355).

[886] « Le masquage des données de santé consiste en la possibilité, pour le propriétaire d'un dossier de santé informatisé soit de refuser de donner les informations, soit d'en interdire l'accès ». CNIL. *Délibération n° 2010-*

le patient français, la possibilité d'accès en urgence (dit *mode « bris glace* ») permet aux professionnels de forcer l'accès aux informations masquées et de se justifier plus tard, l'intrusion du professionnel étant tracée dans le journal d'accès du patient. La délibération de la CNIL du 2 décembre 2010 recommande que le masquage des données ne soit pas signalé dans le dossier du patient français[887]. Dans le cas suédois, face à l'indication qu'une partie des informations a été verrouillée, le professionnel de santé qui estime qu'elles sont cruciales pour sauver la vie du patient peut requérir du confrère qui a œuvré au verrouillage, le déblocage du système [888] si le patient concerné n'est pas en mesure d'exprimer sa volonté. Finalement, le législateur suédois tout comme le législateur français confient le dossier médical électronique au patient qui en maîtrise les accès et en contrôle le contenu tant qu'il peut manifester sa volonté et que sa santé ou sa vie n'est pas menacée.

Un droit de refus de traitement de ses données médicales est accordé au patient. Si ce droit d'opposition est manifesté après le début d'un traitement, le processus est immédiatement interrompu et les données sont effacées du registre dès que possible[889].

ii. La sécurité des données des patients

Le dossier patient ne contient que les informations jugées nécessaires aux fins d'administration efficace de soins. Ainsi, y sont enregistrées les informations relatives à l'identité du patient, les informations de base indispensables aux professionnels de santé, les

---

449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel. www.cnil.fr Voir aussi LESSIS (Les entreprises des systèmes d'informations sanitaires et sociaux). *Données personnelles de santé, un masquage des données de santé au service de tous les acteurs*. [en ligne], LESSIS-janvier 2007. Disponible sur: www.lesiss.org. Consulté le 15 Août 2013.

[887] « *Le patient disposera également d'un « droit de masquage » qui lui permettra de rendre inaccessiblesà certains professionnels desanté des données présentes dans son DMP. L'existence de documents masqués ne sera pas signalée.*» CNIL. *Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel*. [en ligne], disponible sur: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516. Consulté le 2 juillet 2014.

[888] chapitre 6, paragraphe 4. Patientdatalag (SFS 2008 : 355).

[889] chapitre 7, paragraphe 2. Patientdatalag (SFS 2008 : 355).

antécédents médicaux pour les maladies les plus graves et les diagnostics, les traitements prescrits et l'identité des professionnels de santé ayant administré ces soins[890].

C'est le professionnel de santé qui détermine les conditions dans lesquelles une autorisation d'accès au dossier de son patient peut être accordée[891]. Le NPO n'est accessible qu'aux seuls personnels de soins qui prennent le patient en charge ou, qui, pour une quelconque raison en ont besoin dans le cadre de leur travail[892]. Le personnel de soins doit être habilité et détenir un certificat électronique pour avoir accès aux NPO[893]. Les accès au dossier médical suédois sont tracés de sorte à permettre d'identifier la personne qui a consulté le dossier du patient. Pour rendre ce contrôle effectif les établissements de soins adoptent des habitudes[894] de travail élaborées à cet effet[895] sous la vigilance du gouvernement ou de l'autorité désignée par celui-ci. Les autorités publiques mettent la documentation nécessaire à la disposition des professionnels de santé et prennent des mesures visant à les encourager à opter pour les dossiers médicaux entièrement ou partiellement automatisés[896].

Présenté comme le droit du patient sur son dossier automatisé, la possibilité de restriction d'accès peut être utilisée par ce dernier comme une barrière de protection de sa vie privée pendant un processus de soins. Lorsque la situation se présente, l'accès aux données automatisées est immédiatement interrompu et le dossier est gelé[897]. Toutefois, les parents ou tuteurs légaux de mineurs n'ont pas le droit de restreindre l'accès aux dossiers de ceux-ci. Cette limite imposée aux parents et tuteurs légaux de mineurs peut être interprétée comme une méconnaissance du droit à la vie privée de ces personnes de jeune âge. Si les représentants légaux sont appelés à protéger les droits des mineurs en attendant leur majorité, cette disposition vient en violation d'un principe fondamental : le droit à la protection de la vie privée d'une des couches sociales les plus vulnérables. C'est une différence majeure dans la

[890] chapitre 3, paragraphe 6. Patientdatalag (2008 : 355). http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Patientdatalag-2008355_sfs-2008-355/?bet=2008:355. Consulté le 30 juillet 2013.

[891] Chapitre 4 paragraphe 2. Patientdatalag (SFS 2008 : 355).

[892] Chapitre 4 paragraphe 1. Patientdatalag (SFS 2008 : 355).

[893] Chapitre 4, paragraphes 1 et 2. Patientdatalag (SFS 2008 : 355).

[894] Ils sont tenus de procéder au contrôle systématique des accès de façon régulière.

[895] chapitre 4, paragraphe 3. Patientdatalag (SFS 2008 : 355).

[896] chapitre 4, paragraphe 2. Patientdatalag (SFS 2008 : 355).

[897] chapitre 4, paragraphe 4. Patientdatalag (SFS 2008 : 355).

gestion du dossier médical électronique entre la France et la Suède en ce sens que le code de la sécurité sociale français permet au représentant légal de rendre inaccessibles certaines informations[898] du DMP de son protégé.

Dans un souci de protection de la vie privée du patient, les entreprises pharmaceutiques sont tenues de crypter les identités des patients avant de transmettre les informations relatives aux médicaments et autres produits pharmaceutiques aux Comités des médicaments[899] .

c. Les dossiers médicaux électroniques en Espagne

L'Espagne fait partie des pays pionniers en matière de programme pilote pour le partage des dossiers médicaux informatisés. Depuis 2009, date de leur initiation, les dossiers médicaux électroniques sont subventionnés et gérés par les régions. En Andalousie par exemple, le programme numérique DIRAYA[900] donne des résultats encourageants avec 95 % de la population couverte, 300 millions de rendez-vous pris par SMS, Internet ou téléphone et 8 millions d'e-prescriptions par mois[901]. Le gouvernement organise une meilleure coordination de ces initiatives régionales avec un projet d'interopérabilité nationale.

Selon une étude menée par Accenture[902], alors que la France connaît une légère baisse dans l'adoption des solutions informatiques de santé, les praticiens espagnols affichent l'un

[898]Article L-161-36-4 du code de la sécurité sociale : « *un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et des Conseils nationaux de l'ordre des professions de santé, fixe les conditions d'application […] les conditions d'accès aux différentes catégories d'informations qui figurent au dossier médical personnel, les conditions dans lesquelles certaines informations peuvent être rendues inaccessibles par le titulaire du dossier médical personnel ou son représentant légal ainsi que les modalités selon lesquelles le professionnel de santé accédant au dossier médical personnel a connaissance de l'inscription au dossier d'informations rendues inaccessibles par son titulaire ou son représentant légal*. » Loi n° 2007-1786 du 19 décembre 2007 dite loi de financement de la sécurité sociale pour 2008 (transféré par la loi n° 2009-879 du 28 juillet 2009-article 50). JORF n° 0296 du 21 décembre 2007 p.20603. Texte 1 sur 184. NOR BCFX0766311L.

[899] chapitre 4, paragraphe 6.

[900] http://www.juntadeandalucia.es/servicioandaluzdesalud/principal/documentosacc.asp?pagina=pr_diraya
Pour plus d'informations, visionner la vidéo en français sur le site suivant: http://www.juntadeandalucia.es/servicioandaluzdesalud/principal/documentosacc.asp?pagina=pr_diraya_present_fr. Consulté le 30 juillet 2013.

[901] Présentation vidéo du programme sur le site précité. http://www.juntadeandalucia.es/servicioandaluzdesalud/principal/documentosacc.asp?pagina=pr_diraya_present_fr. Consulté le 21 avril 2014.

[902] Accenture est une entreprise internationale de Conseil en management, technologies et externalisation. ww.accenture.com

des taux les plus élevés en la matière de 2011 à 2012[903]. Les patients espagnols ont connu une nette amélioration de la qualité de leurs soins pendant cette même période. Les médecins espagnols échangent davantage des informations de santé et sont parmi les plus nombreux à avoir adopté et utilisé des systèmes de dossiers médicaux électroniques[904]. Par le biais d'alerte ou d'e-mails, ils sont informés sur les compte rendus des rencontres de leurs patients avec d'autres praticiens ou établissements de soins.

Il ne fait aucun doute que l'Espagne porte un grand intérêt aux dossiers médicaux électroniques. Mais, quid de l'environnement juridique qui encadre la gestion de ces dossiers médicaux quand le régime juridique est marqué par la décentralisation des compétences ?

i. Un encadrement juridique complexe

L'Espagne fait partie des premiers États à avoir transposé la directive européenne sur la protection des données personnelles le 13 décembre 1999[905]. Cette loi organique autorise le traitement automatisé des données sensibles pour des raisons médicales[906] ; ce qui donne toute légitimité au traitement informatisé des données de santé.

Le domaine de la santé relève autant de la compétence du gouvernement que des communautés autonomes ; le ministère de la santé coordonnant le projet relatif aux dossiers médicaux électroniques entre les différentes communautés. Le système juridique espagnol de gestion des dossiers médicaux est complexe en ce sens qu'il n'existe pas de législation

[903] Accenture. *Étude Accenture menée auprès des médecins : changement de tendance en France en matière d'informatique médicale*. L'enquête en ligne a été menée auprès de 3700 médecins dans 8 pays dont l'Allemagne, l'Angleterre, l'Australie, le Canada, l'Espagne, les États-Unis, la France et Singapour. L'étude visait à évaluer l'attitude des praticiens vis-à-vis des solutions d'information et de communication médicale et la perception des avantages offerts par celles-ci. Les résultats ont révélé que chez les praticiens français l'adoption d'un système informatique de santé et des plates-formes d'échange d'informations de santé (EIS) a légèrement baissé. Disponible sur: Http://www.accenture.com/fr-fr/Pages/insight-acn-doctors-survey-profile-he. Voir également: Recueil Dalloz, 2009. Disponible sur: Élthcare-it.aspx. Consulté le 2 mai 2014.

[904] Accenture. *Doctors Survey: Us Country Profile*. [en ligne], disponible sur: http://www.accenture.com/ SiteCollectionDocuments/PDF/Accenture-Doctors-Survey-US-Country-Profile-Report.pdf. Voir le tableau p.10 et p.15. Consulté le 2 mai 2014.
Pour la version française, voir la même page sur le lien suivant: http://www.accenture.com/SiteCollection Documents/Local_France/PDF/Accenture-Doctors-Survey-France-Country-Profile.pdf. Consulté le 2 mai 2014.

[905] Loi organique 15/1999 du 13 décembre 1999 relative à la protection des données à caractère personnel. BOE n° 298 du 14 Décembre 1999. Disponible sur: http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750. Consulté le 2 mai 2014.

[906] Article 7, Loi organique 15/1999 du 13 décembre 1999 relative à la protection des données à caractère personnel.

spécifique nationale portant sur les dossiers médicaux électroniques. Certes, des lois et des décrets existent qui régissent, notamment, les droits et les obligations des patients et des professionnels de santé quant à la gestion des dossiers médicaux, le régime juridique du consentement donné pour la collecte et le traitement de ses données de santé, le contenu des dossiers médicaux électroniques, mais tous ces textes n'ont pas une portée nationale. La plupart d'entre eux s'adressent spécifiquement à des communautés bien déterminées. Néanmoins, les communautés autonomes doivent conformer leurs normes, en matière de dossier médical électronique à ces textes de portée nationale. La loi organique 15/1999 régissant la protection des données à caractère personnel et la loi 41/2002 relative à l'autonomie du patient constituent des fondements de cette législation.

Ainsi, l'article 15 de la loi[907] 41/2002 du 14 novembre 2002 portant sur les règles fondamentales relatives à l'autonomie du patient ainsi que ses droits et obligations en matière d'information et de documentation clinique a-t-elle fixé un contenu minimum de dossier médical (papier et électronique). Les communautés autonomes ont la liberté de modeler le type d'informations que doit contenir un dossier médical électronique selon les besoins et les spécificités de leur région[908]. Il y a donc presqu'autant de dossiers médicaux électroniques que de communautés autonomes engagées dans le processus. C'est pourquoi le gouvernement met tout en œuvre pour assurer l'interopérabilité des différents systèmes publics et privés afin de permettre une facilité d'accès électronique aux services publics des citoyens. Cela est régi par la loi 11/2007[909] du 22 juin relative à l'accès des citoyens aux services publics par voie électronique. Pour favoriser l'interopérabilité des systèmes d'information et faciliter cet accès électronique à tous les services y compris ceux de santé, le décret[910] n° 4/2010 du 8 janvier 2010 a été pris. L'administration électronique des services de santé est régie par la loi[911] n° 16/2003 du 28 mai portant sur la cohésion et la qualité du système national de santé. L'article

[907] Bulletin officiel de l'État "Boletín oficial del estado" n° 274 du 15 novembre 2002, pp. 40126 - 40132. http://www.boe.es/diario_boe/txt.php?id=BOE-A-2002-22188. Consulté le 2 mai 2014.

[908] C'est ce que rappellent les premières lignes du décret royal 1093/2010 du 3 septembre 2010.

[909] Article 21. Bulletin officiel de l'État " Boletín oficial del estado" n° 150, du 23 juin 2007, pp. 27150 - 27166 https://www.boe.es/buscar/doc.php?id=BOE-A-2007-12352. Consulté le 2 mai 2014.

[910] Real decreto 4/2010, de 8 enero, por el que se regula el Esquema National de Interoperabilidad en el ámbito de la Administración Electrónica. http://noticias.juridicas.com/base_datos/Admin/rd4-2010.html. Consulté le 10 février 2014.

[911] Ley 16/2003, de 28 de mayo, de cohesón y calidad del Sistema National de Salud. http://noticias.juridicas.com/base_datos/Admin/l16-2003.html. Consulté le 10 février 2014.

56 de cette loi établit la base du cadre juridique des dossiers médicaux électroniques en Espagne. Il précise, en effet qu'afin que les citoyens reçoivent les meilleurs soins de santé possible dans un établissement ou un service du système national de santé, le ministère de la santé coordonnera les mécanismes d'échanges électroniques de données personnelles de santé antérieurement confiées aux communautés autonomes. Cela permettra à la fois aux patients concernés et aux professionnels impliqués dans sa prise en charge d'accéder uniquement aux informations contenues dans les dossiers médicaux qui sont strictement nécessaires à l'assurance de la meilleure qualité de soins et la confidentialité et l'intégrité des données quel que soit l'administration prestataire. Ces dispositions sont complétées, par le décret[912] 183/2004 relatif à la carte individuelle de santé, notamment ses articles 3 et 4 et le décret royal n° 1093/2010 relatif au contenu du dossier médical.

Le décret royal 1093/2010[913] entérine la loi 41/2002 en tenant compte de la diversité des systèmes d'information et des types de dossiers médicaux élaborés par les différentes régions. L'idée est d'obtenir un consensus entre les professionnels de santé, d'harmoniser les pratiques et de permettre l'utilisation de tous les dossiers par toutes les écoles et les appareils fonctionnels qui composent le SNS[914]. L'article 3 du décret énonce la liste des documents devant obligatoirement figurer dans chaque dossier médical avec le pouvoir pour les communautés autonomes de créer des modèles intégrant d'autres éléments qu'ils jugent appropriés. Il est impératif que toutes les informations obligatoires car l'omission d'une de ces données empêche toute possibilité d'interopérabilité entre les systèmes. Il s'agit du rapport clinique initial, du rapport clinique de consultations externes, du rapport clinique des urgences, du rapport clinique des soins primaires, des résultats d'analyses de laboratoire, des résultats d'imagerie médicale, des rapports de soins infirmiers et des résumés des antécédents médicaux.

A l'instar de la diversité de contenus prévus pour les dossiers médicaux électroniques espagnols, les droits des patients font l'objet de législation différente d'une communauté autonome à l'autre. Mais, ces législations doivent, en principe, rester conformes aux normes

---

[912] Real decreto 183/2004, de 30 enero, por el que se regula la tarjeta sanitaria individual. http://noticias.juridicas.com/base_datos/Admin/rd183-2004.html. Consulté le 10 février 2014.

[913] Décret royal approuvant la liste minimale de données que doit contenir un dossier médical. Bulletin officiel de l'État " Boletín oficial del estado" n° 225 du 16 septembre 2010, pp. 78742 - 78 767. http://www.boe.es/buscar/doc.php?id=BOE-A-2010-14199. Consulté le 10 février 2014.

[914] Système national de santé.

établies par la loi 41/2002. Par exemple, pour la communauté de Catalogne la loi 16/2010 du 3 juin 2010[915] modifiant la loi 21/2000 du 29 décembre 2000 légifère sur le droit à l'information médicale et l'autonomie du patient ainsi que la documentation clinique. Quant à la Galice, elle a adopté la loi 3/2005 du 17 mars 2005[916] modifiant la loi 3/2001 du 28 mai 2001 régissant le recueil du consentement du patient dans le cadre de l'élaboration de son dossier médical. Le Pays basque a quant à lui, pris un décret 38/2012 le 13 mars 2012[917] portant sur le dossier médical et les droits et obligations des patients et des professionnels de santé en matière de documentation clinique.

Toutefois, force est de constater, que d'une part, aucune des législations nationales ou communautaires n'a été consacrée à des dispositions spécifiques à la sécurité de traitement des données médicales. Actuellement, la question de la protection des données médicales est régie par la loi organique sur la protection des données personnelles de 1999 et son règlement de 2007[918], notamment les dispositions relatives aux données sensibles[919]. Même si un arrêté[920] du 26 octobre 2011 sur les critères techniques et/ou scientifiques d'accès aux dossiers médicaux à des fins épidémiologiques ou de santé publique régit la communauté de Galice, nous estimons que ce texte n'est pas suffisant face à la multitude de dossiers médicaux en Espagne, à l'absence de réglementations similaires dans les autres communautés autonomes et à leur état d'avancement dans le processus. D'ailleurs, cet arrêté ne régit pas la gestion des dossiers médicaux dans le cadre de soins de santé hospitaliers ou de médecine de ville qui font l'objet de notre étude.

---

[915] Ley 16/2010, de 3 de junio, de modificación de la ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica. http://noticias.juridicas.com/base_datos/CCAA/ca-l16-2010.html. Consulté le 10 février 2014.

[916] Ley 3/2005, de 7 de marzo, de modificación de la ley 3/2001, de 28 de mayo, reguladora del consentimiento informado y de la historia clínica de los pacientes. http://noticias.juridicas.com/base_datos/CCAA/ga-l3-2005.html. Consulté le 10 février 2014.

[917] Decreto 38/2012, de 13 de marzo, sobre historia clínica y derchos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica. http://noticias.juridicas.com/base_datos/CCAA/pv-d38-2012.html. Consulté le 10 février 2014.

[918] Real decreto 1720/2007, de 21 diciembre, por el se aprueba el reglamento de desarrollo de la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.html. Consulté le 10 février 2014.

[919] Article 7 de la loi organique 15/1999. « *Datos especialmente protegidos* ». http://noticias.juridicas.com/base_datos/Admin/lo15-1999.t2.html#a7. Consulté le 10 février 2014.

[920] "Diario oficial de Galicia" (DOG) n° 219 du mercredi 16 novembre 2011. p. 33555.

D'autre part, aucune législation n'étant spécifiquement consacrée aux dossiers médicaux électroniques contrairement à la France, l'encadrement juridique est fondé sur des textes approximatifs portant sur la protection de toutes les données personnelles. Pourtant, tout le système de la e-santé semble bien organisé et se dérouler dans une certaine harmonie. La gestion des dossiers médicaux électroniques est liée à l'e-prescription. Le patient est identifié grâce à sa carte de santé[921], et le médecin est identifié et accrédité par voie électronique. Ensuite, automatiquement, la prescription est à la fois mémorisée dans une base de données des prescriptions et enregistrée dans le dossier médical électronique du patient.

Compte tenu de cette absence de législation particulière, les droits des patients espagnols dans le cadre de la gestion des dossiers médicaux électroniques sont analysés au regard des textes épars et approximatifs annoncés ci-dessus.

ii. La protection des droits des patients espagnols

Le décret royal 1720/2007 du 21 décembre 2007 portant approbation du règlement d'application de la loi organique 15/1999[922] et la directive européenne du 13 décembre 1999 sur la protection des données personnelles prévoient des dispositions relatives au consentement donné par le patient au traitement de ses données. L'article 12 du décret royal, développant en cela l'article 6 de la loi n° 15/999, impose le recueil du consentement du patient avant toute collecte et tout transfert de ses données personnelles. Cela, après lui avoir expliqué la finalité de ce traitement. Une demande d'autorisation est faite auprès de la personne concernée qui comporte les détails des données à traiter et la finalité de ces opérations. Le consentement peut être tacite ou express[923] de manière générale. Mais l'article 7.3 de la loi 15/1999 impose un consentement exprès pour le traitement des données de santé

[921] Le 20 septembre 2013 a été approuvé le projet de décret en Conseil des ministres qui modifiera le décret 183/2004 pour permettre que tous les citoyens espagnols bénéficiaires du système national de santé puissent disposer d'une carte individuelle de santé comportant un certain nombre de données de base et un code d'identification personnelle. Cette carte permettra l'interopérabilité des systèmes d'information de santé de toutes les communautés autonomes. MINISTERIO DE SANIDAD, SERVICIO SOCIALES E IGUALIDAD. *La tarjeta Sanitad Individual tendrá un formato único y será interoperable en todas las Comunidades Autónomas*. http://msc.es/gabinete/notasPrensa.do?id=2993. Consulté le 22 avril 2014.

[922] Pour rappel, il s'agit de la loi organique transposant la directive européenne 95/46/CE

[923] Article 14.1 du décret royal 1720/2007. Un consentement donné dans des conditions équivoques sur la finalité du traitement des données personnelles est considéré comme nul. La preuve du consentement peut être faite par tout moyen (article 12 du même décret royal).

tout comme en France, sauf dans les cas où la loi admet un traitement sans consentement[924]. De plus, le mineur espagnol de 14 ans peut lui-même exprimer son consentement au traitement de ses données personnelles sauf si la loi exige que l'on ait recours à l'assistance du titulaire de l'autorité parentale[925]. En France, la décision de création d'un dossier médical personnel revient au titulaire de l'autorité parentale parce que les informations relatives à l'état de santé du mineur sont, en principe, données à son représentant légal et accessoirement ou simultanément au concerné [926].

Le droit au refus de traitement de ses données est une prérogative laissée au patient espagnol tout comme le patient français, mais le premier est informé qu'il dispose de 30 jours pour exprimer son opposition (par l'envoi d'une lettre ou par appel à l'intention du responsable du traitement) sinon son consentement est réputé donné[927]. Un consentement donné initialement pour le traitement de ses données personnelles peut ultérieurement être révoqué. Dans ce cas, le responsable du traitement dispose de 10 jours à compter de la date de réception de la révocation pour mettre fin au traitement des données personnelles[928].

L'article 8 de la loi organique 15/1999 autorise les institutions, les centres et les professionnels de santé publique et privée à procéder au traitement de données personnelles relatives à la santé des personnes si les lois et règlements de l'État ou de la région l'autorisent sans recourir au consentement du concerné. Le décret royal 1720/2007 confirme cette règle en son article 10. Le consentement du titulaire des données n'est pas requis pour la divulgation

[924] Article 8 de la loi organique 15/1999.

[925] Article 13 du décret royal 1520/2007. L'article 9.3 de la loi 41/2002 permet au mineur, à partir de 16 ans, de manière générale, de consentir pour les traitements médicaux. Ainsi, à partir de 16 ans, en général, le mineur consent aux soins médicaux, au traitement de ses données et reçoit les informations relatives à son état de santé (dans les cas graves on peut également informer ses parents). Pour les mineurs de moins de 16 ans, la situation est moins claire. Selon l'article 9.3 précité tout dépendra de la capacité de discernement de ce mineur et en principe, c'est le médecin qui décide s'il a ou non la capacité pour consentir par lui-même à son traitement médical (tout dépendra du type de traitement, plus ou moins grave, du type d'affection).
Les dispositions de l'article 13 du décret 1520/2007 et celles de l'article 9.3 de la loi 41/2002 présentent différemment la situation du mineur dans la gestion de ses données personnelles de santé. Entre les mineurs de 14 ans selon le décret et ceux de 16 ans (âge auquel il est généralement reconnu que le mineur à la capacité de décider selon l'article 9.3 de la loi 41/2002), la situation n'est pas claire. Tout dépendrait du type de traitement médical. Dans les cas moins graves, le mineur peut consentir seul pour les traitements médicaux tout comme pour le traitement de ses données personnelles (par exemple c'est ce qui s'est passé au moment de donner la pilule abortive ou "la pilule du lendemain" au mineur de 15 ans, beaucoup de médecins considéraient que la mineur pouvait consentir seule sans nécessité d'informer ou de requérir l'avis des parents ou de recourir à leur consentement pour les traitements médicaux et le traitement de leurs données personnelles).

[926] Article L 1111-2 alinéa 5 du code de la santé publique.

[927] Article 14.1 du décret royal 1720/2007.

[928] Article 17 du décret royal 1520/2007.

de ses données personnelles médicales, y compris par voie électronique, par les centres de service inter-agences et le système national de santé, lorsque les traitements sont destinées à des soins de santé de la population et pour la cohésion et la qualité du système de santé national[929]. Ainsi présenté, le système espagnol paraît plus souple que le système français quant au droit du patient à exprimer sa volonté préalable au traitement de ses données de santé. L'équivalent de cette disposition en droit français est celui du traitement automatisé de données médicales sans le consentement du concerné pour des raisons de santé publique. Mais l'expression *« cohésion et qualité du système national »* paraît bien vaste et peut favoriser des abus de la part des professionnels de santé sous prétexte que cela contribue au bon fonctionnement du système national de santé espagnol.

Le patient a un droit d'accès et de rectification à son dossier médical. Mais il ne peut exercer ce droit au détriment du droit à la confidentialité des informations des autres. C'est pourquoi, en cas de risque d'atteinte à la vie privée des autres patients et professionnels impliqués dans le même groupe thérapeutique que le patient concerné, le professionnel de santé est habilité à lui refuser ce droit d'accès[930]. En outre, l'article 16 de la loi 41/2002 impose la préservation des données personnelles d'identification du patient (l'anonymisation complète) lorsqu'un centre de santé ou un professionnel accède au dossier médical à des fins judiciaires, épidémiologiques, de santé publique, de recherche ou d'enseignement. Exceptionnellement, les données d'identification ne seront pas séparées de données cliniques lorsque l'accès serait justifié par une enquête judiciaire où l'unification des données est essentielle pour les investigations des tribunaux, ou dans le cadre d'actions menées en vue de prévenir un risque grave ou un danger pour la santé publique. Dans ces conditions, il est de rigueur que l'accès soit fait par un praticien de la santé soumis au secret professionnel ou un autre professionnel soumis à une obligation de secret équivalente[931]. La cour européenne des droits de l'homme milite en faveur de la préservation de la vie privée des patients en ce domaine. Dans l'affaire[932] C. C. contre Espagne, le requérant alléguait, en invoquant l'article 8

[929] L'article 10. 5 du décret qui régit cette situation en précise bien le cadre en se référant au chapitre 5 de la loi 16/2003 relative à la cohésion et la qualité du système de santé qui traite du système d'information sanitaire (article 53).

[930] article 18. 1 et 3 de la loi 41/2002.

[931] Article 16. 3 de la loi 41/2002.

[932] Cour européenne des droits de l'homme. Arrêt, *C. C. contre Espagne*. Strasbourg, 6 octobre 2009. Requête n° 1425/06. Arrêt rendu définitif le 6 janvier 2010. in *Note d'information sur la jurisprudence de la Cour* n° 123,

de la Convention européenne des droits de l'homme, que son droit au respect de la vie privée avait été violé du fait de la divulgation de son identité, qui figurait en toutes lettres dans les décisions judiciaires rendues en Espagne et qui, notamment, était associée à son état de santé dans le jugement rendu en première instance. Même si pour le gouvernement espagnol l'état de santé du requérant était l'objet principal de la procédure initiale dirigée contre la compagnie d'assurance qui lui avait refusé une indemnité parce qu'elle estimait qu'il avait dissimulé son état de santé, la Cour européenne des droits de l'homme a jugé que la publication de ces éléments a porté atteinte au droit du requérant au respect de sa vie privée et familiale garantie par l'article 8 de la Convention[933]. En effet, « *eu égard aux circonstances particulières de la présente affaire, notamment au principe de la protection spéciale de la confidentialité des informations relatives à la séropositivité, la Cour estime que la publication en toutes lettres de l'identité du requérant, associé à son état de santé, dans le jugement rendu par le juge de première instance n'était justifiée par aucun motif impérieux*. »

Cette décision de la cour européenne des droits de l'homme permet de constater que les patients européens ont une garantie supplémentaire de protection de leurs informations personnelles si la législation interne ou les autorités internes ne l'assurent pas suffisamment. Mais il est bien plus rassurant d'avoir un cadre juridique bien organisé et précis qui régisse les dossiers médicaux électroniques, matrices de données aussi sensibles que sont les informations de santé.

Compte tenu de la différence d'organisation de cadre juridique entre le système de dossier médical personnel français et celui de dossiers médicaux électroniques espagnols la comparaison n'est pas aisée. La complexité du système juridique qui entoure la gestion des dossiers médicaux électroniques espagnols constitue un défi de taille pour plusieurs professionnels. Si pour les juristes cela rend plus difficile l'établissement d'un cadre juridique commun aux dossiers médicaux électroniques, les médecins et autres professionnels de santé auront plus de difficultés à trouver des précisions quant aux directions médico-légales à suivre.

Octobre 2009. p. 18. Lire l'intégralité de la décision sur le lien URL suivant : Http://hudoc.echr.coe.int/sites/eng/pages/search.aspx#{"dmdocnumber":["855403"],"itemid":["001-94632"]}. Consulté le 7 août 2012.

[933] La Convention européenne des droits de l'homme, dénomination usuelle de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales est un traité international signé par les États membres du Conseil de l'Europe le 4 novembre 1950 et entré en vigueur le 3 septembre 1953.

La situation espagnole rappelle également un obstacle auquel se heurte l'harmonisation de la législation relative à la gestion des données médicales dans l'espace européen. Pourtant, le développement des dossiers médicaux électroniques et partagés dans l'espace européen pourrait répondre à un besoin de coordination de soins de santé au sein de l'Union. Cela permettrait par exemple, à un patient français ou européen pris en charge dans un hôpital différent, hors de son État d'origine, de pouvoir bénéficier de soins de meilleure qualité, grâce aux informations fournies par son DMP ou son équivalent. Les standards HL7 (Health Level Seven)[934] auxquels ont adhéré plus de 55 pays dont la France offrent déjà un mécanisme homologué de normes permettant des échanges informatisés d'informations médicales, administratives et financières dans le secteur de la santé. Mais toutes ces initiatives ne sont véritablement profitables au titulaire du DMP que si l'on tient suffisamment compte du consentement de ce dernier.

Paragraphe 2 : Le consentement du titulaire dans le processus de création du DMP

Jusqu'au 13 août 2004[935], date de création du dossier médical personnel, les professionnels et établissements de santé se dotaient de dossiers médicaux informatisés en dehors de toute obligation légale ou réglementaire. Le traitement automatisé des données de leurs patients constituait une méthode pratique et beaucoup plus bénéfique pour l'archivage des informations médicales et l'échange avec d'autres professionnels ou établissements de santé. Ayant pris conscience des risques d'atteinte qu'encourent les données de santé des patients et en vue d'un partage plus accru de celles-ci, le législateur a instauré dès 2004 un cadre légal pour la création et la gestion des dossiers médicaux informatisés, notamment, le dossier médical personnel. Ce cadre privilégie le consentement du titulaire du dossier médical

[934] Site internet de référence: http://www.hl7.org/.

[935] Loi n° 2004-810 du 13 Août 2004 relative à l'assurance maladie. JORF du 17 Août 2004 mais rectifiée au JORF n° 276 du 27 novembre 2004. P 20151 et suivant. NOR: SANX0400122Z. http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20041127&numTexte=5&pageDebut=20151&pageFin=20151. Consulté le 7 août 2012.

qui n'est plus le médecin traitant mais celui dont les données médicales sont traitées : le patient.

Dans le processus de création du dossier médical personnel, le droit français requiert le consentement du patient d'abord pour la création de ce dossier médical informatisé et ensuite pour son hébergement.

A. Le consentement du titulaire pour la création de son DMP

De tout temps, le domaine de la santé a accordé une certaine importance au consentement du patient lorsqu'il s'est agi de traitement de son état de santé. Mais la création et la gestion d'un dossier médical le concernant sur le support papier ou électronique au sein de leur établissement se faisaient sans l'avis de celui-ci. C'était un dossier métier dont la connaissance n'était réservée aux professionnels de santé. Aujourd'hui, la particularité du dossier médical personnel oblige les professionnels de santé à tenir compte d'un cadre médico-légal très strict en vue de la préservation de la vie privée de leurs patients.

Le législateur a établi un cadre légal du dossier médical personnel, accordant une grande importance à la volonté du patient. Toutefois, beaucoup d'informations quant aux modalités d'expression de son consentement lors de la création de son DMP par le titulaire proviennent du "*portail du dossier médical personnel*[936]" ou des brochures élaborées pour l'information des patients et des professionnels de santé. L'origine légale de cette condition ne nous semble clairement établie, mais la règle a été légitimée par les organismes en charge de l'encadrement technique et juridique du déploiement du dossier médical personnel.

[936] Article L 1111-19 du code de la santé publique alinéa un : « *Il est institué un service unique d'accueil dématérialisé, dénommé « portail du dossier médical personnel », destiné aux bénéficiaires de l'assurance maladie et aux professionnels de santé. Ce portail assure des fonctions d'information générale et un service de gestion permettant aux bénéficiaires de l'assurance maladie de gérer leur dossier médical personnel et les droits d'accès des professionnels de santé. Il assure le contrôle et la traçabilité des accès aux dossiers médicaux personnels. Il produit les données de suivi d'activité nécessaires à l'évaluation de ce service.* »

1. Le recueil du consentement du patient à la création du DMP présenté de manière anodine par la loi

A la lecture de la loi sur le dossier médical personnel, nous remarquons qu'elle ne comporte pas de dispositions stipulant clairement que le DMP est ouvert soit à l'initiative du patient, soit à celui du médecin avec l'accord du patient comme on l'apprend sur le portail dédié au dossier médical personnel ou les publications de l'ASIP santé. Elle se borne à déclarer à : «… *Chaque bénéficiaire de l'assurance maladie dispose, dans les conditions et sous les garanties prévues à l'article 1111-8 et dans le respect du secret médical, d'un dossier médical personnel constitué de l'ensemble des données mentionnées à l'article L 1111-8, notamment des informations qui permettent le suivi des actes et prestations de soins … ».* C'est dire que l'article L 1111-14 informe uniquement le patient qu'en tant qu'assuré, il peut bénéficier d'un dossier médical personnel sans préciser que son consentement sera requis pour la création de ce dossier. Pourtant, la même loi prend le soin de préciser, s'agissant du dossier pharmaceutique que celui-ci est créé pour chacun des bénéficiaires de l'assurance maladie avec son consentement[937]. Le rédacteur de la loi considérait-il qu'il est évident de recourir au consentement de concerné avant l'ouverture de son DMP au point qu'il n'est pas nécessaire de le préciser ?

L'article L 1111-8 exige que l'on obtienne l'accord du patient avant de stocker ses données médicales auprès d'un hébergeur quelconque. Doit-on en déduire que cet article est la source légale qui justifie les informations que produisent le portail relatif au DMP et les brochures ? Nous estimons que si l'une des étapes les plus importantes de la création du dossier médical est son hébergement, et que donner son accord pour l'hébergement implique un consentement préalable pour la création, cette disposition ne permet pas d'affirmer avec autant de précision les informations que véhiculent le portail et les brochures.

On aurait pu se convaincre que la source légale de cette règle demeure dans l'article 8 de la loi informatique et libertés qui oblige le responsable du traitement automatisé à requérir le consentement de l'individu dont les données personnelles de santé seront traitées avant d'être autorisé à le faire. Mais, cette disposition est aussi valable pour le dossier pharmaceutique, la recherche biomédicale, alors que le code de la santé publique dispose explicitement et respectivement à ses articles L 1111-23 et L 1122-1-1 que le consentement du concerné est

[937] Article L 1111-21 alinéa 1 du code de la santé publique.

requis avant de les entreprendre. Pourquoi a-t-il fallu être aussi clair et précis dans une circonstance semblable et être resté vague dans une autre et laisser des sources non légales, ni réglementaires compléter les informations ? Le législateur comptait-il sur la prise immédiate du décret sur le DMP annoncé par l'article L 1111-21[938] du code de la santé publique, pour cela ?

Toutes les brochures d'informations indiquent que le patient reçoit d'abord une brochure explicative sur le DMP puis il donne son consentement pour qu'un dossier soit créé à son nom. Le portail dédié au DMP précise même que ce consentement est dématérialisé. Le professionnel de santé accompagnant le patient dans le processus de création de son DMP attestant son accord en cochant la case prévue à cet effet sur le formulaire numérique de demande de création de DMP. Si l'on admet que le portail dédié au dossier médical personnel a une source légale tout comme l'ASIP santé, organisme de l'État créé par arrêté, doit-on considérer que les initiatives prises par ceux-ci ont une valeur tout aussi légale ou réglementaire en dehors de tout décret d'application ?

2. Le consentement à la création du DMP, une règle précisée par l'usage

La délibération du 2 décembre 2010 de la CNIL indique que « *l'Asip santé a fait le choix du recueil du consentement à l'ouverture d'un DMP qui puisse intervenir dès que la l'information est délivrée* ». En tant que maître d'ouvrage, l'Asip santé prend des décisions ou émet des règles relatives aux détails de la mise en œuvre du déploiement du dossier médical personnel. L'arrêté du 28 novembre 2009 portant approbation de modification de la convention constitutive du groupement d'intérêt public dénommé « *agence des systèmes d'information partagés de santé* » dispose qu'afin de favoriser le développement de systèmes d'information partagés dans les domaines de la santé et du secteur médico-social, l'Asip santé assure notamment, « *la réalisation et le déploiement du dossier médical personnel (DMP) prévu par les articles L 1111-14 à L 1111-24 du code de la santé publique et en particulier la maîtrise d'ouvrage de l'hébergement du DMP* ».

[938] « U*n décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et des Conseils nationaux de l'ordre des professions de santé fixe les conditions d'application des articles L 1100 en ce-14 à L 1111-19 (...)* »

Cette délégation de pouvoir assuré par l'arrêté donne-t-elle légitimement la compétence à l'Asip santé de compléter une disposition législative ?

L'interprétation de ces dispositions ne nous permet pas d'affirmer que l'Asip santé a reçu le mandat d'émettre des règles en complément des articles L 1111-14 à L 1111-24 régissant le dossier médical personnel. En outre, se fondant sur la théorie de la hiérarchie des normes juridiques, la réponse à cette question semblerait négative. Une règle émise par une autorité administrative à la valeur de document administratif conformément à l'article premier[939] de la loi du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverse disposition d'ordre administratif, social et fiscal. Un tel texte n'est, en principe, destiné qu'à exposer l'état de droit résultant de la loi ou de règlement qui justifie son intervention en vue d'assurer sur l'ensemble du territoire une application aussi uniforme que possible du droit positif. Dans cette mesure, elle ne saurait ajouter à cet état de droit soit en édictant de nouvelles normes, soit en donnant une interprétation erronée. Le Conseil d'État distinguait traditionnellement les circulaires interprétatives qui se contentaient de rappeler ou de commenter le texte de loi ou de décret et ne constituaient pas une décision puisqu'elles ne créaient pas de règles nouvelles et les circulaires réglementaires qui ajoutaient des éléments aux textes qu'elles devraient seulement commenter est ainsi créaient des règles nouvelles. Mais depuis l'arrêt[940] de la section du Conseil d'État, Mme Duvignères du 18 décembre 2002, la distinction entre circulaires interprétatives et réglementaires est abandonnée. Le Conseil d'État a fixé, comme nouveau critère de recevabilité pour le recours contre les circulaires, le critère impératif de la circulaire. Les circulaires non impératives sont celles qui se bornent à donner une interprétation d'un texte de loi ou de règlement de l'échelon supérieur afin que ces textes soient appliqués de manière uniforme sur le territoire. Il s'agit de simples recommandations. Au contraire, les circulaires impératives introduisent de nouvelles règles de droit et elles seules sont susceptibles de faire grief et donc de faire l'objet de recours pour excès de pouvoir « *si ces dispositions fixent, dans le silence des textes, une nouvelle*

[939] « *Sont considérés comme documents administratifs, (...) quel que soit leur date, le lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de la mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et décisions.* » 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.

[940] Conseil d'État, section du contentieux, Mme Duvignères, 18 décembre 2002, décision n° 233618, publié au recueil Lebon. www.Conseil-État.fr

règle entachée d'incompétence ou s'il est soutenu à bon droit que l'interprétation qu'elle prescrive d'adopter ne connaît le sens et la portée des dispositions législatives qu'elles entendaient expliciter[941]».

Dans la situation présente, ce complément de la disposition législative qui est général et impersonnel, vise, en plus, à renforcer les droits de l'individu ; ce qui constitue le but principal de tout le cadre légal qui entoure le traitement automatisé de données personnelles. Dès lors, ce que nous estimons pouvoir être perçu comme un dépassement de pouvoir de l'agence est positivement perçu au point de n'éveiller aucune réticence de la part des autorités, et particulièrement la Commission nationale informatique et libertés. Cette situation rencontre plutôt une approbation de la CNIL qui veille néanmoins à obtenir plus de garantie quant à un consentement éclairé et exprès du patient. D'abord, la Commission a souhaité que la brochure d'information remise à l'assuré soit rédigée dans un langage clair, accessible à chacun et qui fasse mention de l'absence de conséquences[942] du refus de création ou d'utilisation du DMP sur les remboursements des prestations par l'assurance maladie ainsi que sur la mise en œuvre du tiers payant. Le document devra souligner l'interdiction pour les organismes d'assurance, les mutuelles, les banques, les médecins du travail et les employeurs d'avoir accès au DMP. Ensuite, la CNIL a déclaré qu'elle n'a pas admis que le recueil complètement dématérialisé du consentement du patient puisse valablement attester de l'expression de consentement explicite au partage de données de santé le concernant. Elle estime qu'il importe de veiller à ce que le recueil du consentement à la création d'un DMP soit réel et que le patient puisse clairement apprécier les conséquences de l'accord qu'il donne. La CNIL a alors rappelé dans la délibération précitée que la confiance des patients, inhérente à une bonne compréhension du

---

[941] Conseil d'État, M. et Mme Philippe A, 8ème et 3ème sous-sections réunies-13 janvier 2010, décision n° 321416. www. Conseil-lebon.fr.

[942] Cette information constitue une évolution en ce sens que la première version de la loi relative à la réforme de l'assurance maladie prévoyait que les remboursements de la prestation dont a bénéficié l'assuré étaient subordonnée à son acceptation ou non de l'ouverture et la tenue en son nom de son dossier médical personnel. Mais la CNIL a décrié cette situation dans son avis rendu le 10 juin 2004 en relevant que les assurés sociaux ne sont pas réellement libres de refuser l'accès à leur DMP et que cela constitue une méconnaissance de leur droit à l'autonomie de la volonté. « *La Commission observe que, conformément aux exigences rappelées ci-dessus, le texte qui lui est présenté, par la référence qu'il convient aux dispositions de l'article L 1111-8 du code de la santé publique, implique la création du dossier médical personnel repose sur le consentement exprès de la personne concernée. Néanmoins, dans la mesure où le niveau de prise en charge des actes et prestations est subordonné à l'accès du professionnel de santé au dossier, il apparaît que ce consentement n'est pas totalement libre.* » CNIL. Délibération n° 2004-054 du 10 juin 2004 *portant avis sur le projet de loi relative à la réforme de l'assurance maladie*. http: //.www.legifrance.gouv.fr

DMP est un gage de son succès. A cet égard, la remise au patient d'un document formalisant son accord apparaît de nature à solenniser l'ouverture d'un DMP. La Commission se voit rassurer à ce sujet par l'engagement pris par le directeur de l'Asip santé de systématiser la remise au patient, lors de la création d'un DMP d'un document qui attestera du recueil de son consentement exprès. Cependant, il faut se rappeler que le consentement du patient à l'ouverture d'un DMP à son nom est légalement requis non seulement en tant qu'il est un dossier médical partagé mais aussi en tant qu'il est un dossier médical hébergé.

B. Le consentement du titulaire à l'hébergement de son DMP

« *les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support, papier ou informatique*[943]*, ne peut avoir lieu qu'avec le consentement express de la personne concernée. (...) Lorsque cet hébergement est à l'initiative d'un professionnel de santé ou d'un établissement de santé, le contrat prévoit que l'hébergement des données, les modalités d'accès à celles-ci et leurs modalités de transmission sont subordonnées à l'accord de la personne concernée*[944]*.* »

L'article L 1111-8 du code de la santé publique privilégie le recours au consentement de l'individu concerné avant tout hébergement de ses données personnelles de santé quel que soit l'initiateur de cette entreprise, mais il prévoit également une dérogation à ce principe.

[943] L'ajout de cette précision par la loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires du 21 juillet 2009 vient affecter la cohérence du dispositif exposé par cette loi. En effet, si l'hébergement est défini par la loi pour la confiance dans l'économie numérique de 2004 comme étant une activité de commerce électronique, il apparaît illogique de l'associer à des données conservées sur un support papier. Pour plus de détails sur cette analyse lire : Caroline Zorn. *Données de santé et secret partagé*. p. 256 à 259.

[944] Article L 1111-8 du code de la santé publique.

1. Le principe du recours au consentement

L'environnement juridique du dossier médical personnel place le patient au centre du dispositif et subordonne à son consentement toutes les manipulations informatiques dont font l'objet ses données de santé. Ainsi, l'insistance du législateur sur ce principe à travers les deux alinéas du même article montre-t-elle l'importance qu'il accorde à l'autodétermination du titulaire de données de santé lorsque celles-ci doivent être confiées à un fournisseur d'accès informatique. Si la loi est formelle à ce sujet, dans la mise en œuvre de ces dispositions, il paraît moins évident que les professionnels de santé ou les établissements de santé prennent vraiment le temps de requérir le consentement du patient, une seconde fois avant de confier ses données à un hébergeur. Ce qui paraît plus probable c'est de voir que ces professionnels utilisent le consentement donné à la création du DMP comme celui comptant aussi pour l'hébergement des données.

Conformément à l'article 32 de la loi du 6 janvier 1978 modifié qui impose une obligation d'information aux responsables de traitement de données personnelles, la brochure d'informations comporte des indications relatives, respectivement, à l'identité du responsable du traitement et de l'hébergeur. Ces renseignements portent également sur la finalité poursuivie par l'ouverture d'un DMP, son contenu, les modalités de création, d'alimentation, d'utilisation et de conservation, ainsi que les conditions d'exercice des droits des patients. Ces informations seront complétées par celles diffusées par le site dédié au dossier médical personnel et par une campagne de sensibilisation. Cette proposition faite par l'Asip santé a obtenu l'approbation[945] de la CNIL qui n'a pas exigé du responsable du traitementqu'il obtienne le consentement éclairé du patient en deux temps. D'ailleurs, le dispositif permet-il d'accepter la création d'un DMP mais de refuser l'hébergeur proposé ?

La réponse qui semble juste serait affirmative mais, à la condition de donner un motif légitime et valable. Ce motif porterait probablement sur le niveau de sécurité qu'offre l'hébergeur. Mais ces raisons seront rapidement rejetées dans la mesure où l'Asip santé, en accordant un agrément à l'hébergeur s'est, en principe, assurée de toutes les garanties de confidentialité qu'offre ce dernier. Par conséquent, contrairement à l'idée initiale de laisser le

[945] CNIL. *Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel*. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516. Consulté le 7 août 2012.

patient exercer son droit à l'autodétermination en lui permettant de donner son accord pour l'hébergement de ses données de santé, celui-ci ne dispose, en réalité, pas de choix quant à l'acceptation de l'hébergeur qui lui est proposé par le responsable du traitement.

Le consentement donné par le patient est l'une des mentions obligatoires devant figurer dans le contrat d'hébergement tel que prescrit par l'alinéa 2 de l'article L 1111-8. « *La prestation d'hébergement, quel qu'en soit le support, fait l'objet d'un contrat.* » Cette convention, lorsqu'elle a été conclue entre l'hébergeur et un établissement de santé ou un médecin doit obligatoirement comporter entre autres mentions[946], « *les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et de transmission*[947] *»*.

Pour rester dans la même logique consistant à laisser libre cours à la volonté du patient, il était prévu qu'il ne lui soit pas imposé d'hébergeur pour son DMP. Certes, l'Asip santé a sélectionné un hébergeur agréé, mais en parallèle, des hébergeurs agréés répondant à des conditions fonctionnelles notamment en matière d'interopérabilité définies par l'agence seront autorisés à proposer un service d'hébergement concurrent et pourront être subventionnés dans la stricte limite du coût de l'hébergeur de référence. Le patient sera donc libre de faire un choix différent de celui fait par l'Asip santé mais ses relations avec son hébergeur s'entretiendront par le biais de l'unique portail Internet dédié au DMP. Mais, la mission

---

[946] Article R1111-13 du code de la santé publique créé par décret n° 2006-6 du 4 janvier 2006-article 1 JORF du 5 janvier 2006 *: « Les modèles de contrats devant être joints à la demande d'agrément, mentionnés au 5° de l'article R. 1111-12, contiennent obligatoirement au moins les clauses suivantes :*
1° La description des prestations réalisées : contenu des services et résultats attendus ;
2° Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels de santé et les établissements de santé les prenant en charge et désignés par eux peuvent être autorisés à accéder à ces données ou en demander la transmission et l'indication des conditions de mise à disposition de ces données ;
3° Lorsque le contrat est souscrit par un professionnel de santé ou un établissement de santé, la description des modalités selon lesquelles les données hébergées sont mises à leur disposition, ainsi que les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et de transmission ;
4° La description des moyens mis en œuvre par l'hébergeur pour la fourniture des services ;
5° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure ;
6° Les obligations de l'hébergeur à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ;
7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement ;
8° Une information sur les garanties permettant de couvrir toute défaillance éventuelle de l'hébergeur ;
9° Une présentation des prestations à la fin de l'hébergement.»

[947] Article L 1111-8, alinéa 2 du code de la santé publique

interministérielle IGF[948], IGAS[949] et CGTI[950] sur le DMP avait mis en doute ce libre choix de l'hébergeur, dans son rapport de novembre 2007, estimant que « *les titulaires du DMP ne disposeront d'aucun critère objectif de différenciation et de choix entre les différents hébergeurs*[951].» Cette remarque a été prise en compte dans la mesure où l'Asip santé a désigné un seul groupe comme hébergeur officiel du DMP en 2010[952] sans faire référence à une quelconque possibilité des patients de faire un choix différent. L'avis d'appel public à la concurrence était destiné à sélectionner un seul opérateur pour l'hébergement national des dossiers médicaux personnels[953].

La place accordée à l'autodétermination dans le choix de l'hébergeur de son dossier médical personnel n'empêche pas que le législateur prévoie des hypothèses où le consentement du patient n'est pas pris en compte pour héberger son dossier.

2. Les dérogations au principe du recours au consentement du patient concerné

Le cinquième alinéa de l'article L 1111-8 du code de la santé publique prévoit une dérogation à l'obligation de requérir le consentement du patient avant d'héberger ses données de santé. Cet alinéa dispose : « *les professionnels et établissements de santé peuvent, (…) utiliser leurs propres systèmes ou des systèmes appartenant à des hébergeurs agréés, sans le consentement exprès de la personne concernée dès lors que l'accès aux données détenues est limité aux professionnels de santé ou à l'établissement de santé qui les a déposées, ainsi qu'à la personne concernée dans les conditions prévues par l'article L 1111-7*. »

---

948 Inspection générale des finances

949 Inspection générale des affaires sociales

950 Conseil général des technologies de l'information

951 Mission interministérielle de revue de projet sur le DMP. *Rapport sur le dossier médical personnalisé*. n° 2007-M-068-01. 8 novembre 2007. p. 37. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000713/0000.pdf. Consulté le 12 décembre 2013.

952 Asip Santé. Communiqué de presse. *Une nouvelle étape dans la mise en œuvre du dossier médical personnel*. 18 février 2010. http://esante.gouv.fr/sites/default/files/CP_notification_hebergeur18022010.pdf. Consulté le 12 décembre 2013.

953 Asip Santé. *AAPC DMP1 et hébergement*. 11 février 2010. http://esante.gouv.fr/en/asip-sante/marches-publics/attributions-de-marche/aapc-dmp1-et-hebergement. Consulté le 12 décembre 2013.

Il ressort de cette disposition que la dérogation n'est valable que si la consultation de ces données est très restreinte. Seuls les professionnels ou les établissements de santé qui les ont stockés et les titulaires de ces informations sont habilités à y accéder. Cet alinéa laisse une marge de liberté aux professionnels de santé lorsqu'ils utilisent leurs propres systèmes d'information ou des systèmes appartenant à des hébergeurs agréés. Pourtant, les conditions de recours aux données médicales en question ne diffèrent pas beaucoup de conditions habituelles où l'on a recours au consentement exprès du concerné. En effet, dans ces cas-là les hébergeurs tiennent les données de santé qui leur ont été déposées à la disposition de seulement ceux qui les leur ont confiées et ne sont autorisés à les transmettre à d'autres personnes que celles désignées dans le contrat d'hébergement. De même, lorsque le système d'information est propre au professionnel ou à l'établissement de santé qui a déposé les données, les consultations sont limitées à un certain nombre de personnes. Pourtant, lorsqu'on parle de système, cela implique un partage d'informations, ne serait-ce qu'entre les professionnels d'une même équipe ou d'un établissement de santé ; ce qui constitue déjà un premier niveau de risque. En outre, si la dérogation intervient dans le cas où les données sont déposées chez un hébergeur agréé, le nombre de personnes ayant accès à ces informations augmente dans la mesure où il faut y inclure l'hébergeur ; sans oublier la possibilité qu'un ou plusieurs des collaborateurs de ce professionnel prennent connaissance du contenu du dossier. Si tant est que le recours à l'autorisation du patient tende à lui permettre de préserver son intimité, la confidentialité de ses informations, cette brèche vient affaiblir la garantie que lui procurait le recueil préalable de son consentement.

En dehors de la dérogation susmentionnée, existe une autre exception à la règle du recours au consentement du patient pour l'hébergement de ses données. Elle est issue de la loi du 10 août 2011 modifiant la loi du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires. L'article 29 de ladite loi dispose : *« pour l'application de l'article L 1111-8 du code de la santé publique, le consentement exprès des personnes concernées est, à compter de la promulgation de la présente loi, réputée accordée pour ce qui concerne le transfert des données de santé à caractère personnel actuellement hébergées par les établissements publics de santé et par les établissements de santé privés. »* Il s'ensuit donc que les données médicales des patients qui avaient été stockées dans les systèmes d'information des établissements publics de santé et des établissements de santé privés peuvent être déposées auprès d'un hébergeur agréé sans que ces établissements demandent l'autorisation des personnes concernées. Cette loi entrée en vigueur depuis le 10 août 2011

accorde strictement cette exception aux établissements de santé, personnes morales publiques ou privées et non aux professionnels de santé en tant que personnes physiques. Elle permet, désormais, aux établissements de santé de confier les informations personnelles de leurs patients à des hébergeurs à l'insu de ceux-ci. La conséquence de cette situation est l'inversion des positions quant à l'obligation de recueil du consentement. Puisqu'il est de principe qu'il faille recourir à l'accord de la personne qui a déposé les données auprès d'un hébergeur avant tout accès à celles-ci, c'est le patient qui devra obtenir l'autorisation des établissements de santé avant de se les voir communiquer par l'hébergeur.

La loi disposant que le consentement est « *réputé accordé* », le législateur considère que le consentement du patient est tacite par le fait d'avoir été accordé pour le traitement automatisé desdites données. Cette déduction n'entre pas en conflit avec le deuxième alinéa de l'article L 1111-8 du code de la santé publique qui impose que le contrat d'hébergement mentionne, entre autres, que les modalités de transmission des données de santé soient subordonnées à l'accord de la personne concernée en ce sens que cette disposition ne précise pas la forme de l'acceptation du patient (expresse ou tacite). De ce fait, le contrat qui liera les établissements de santé et l'hébergeur agréé pourra valablement indiquer que le consentement du concerné a été reçu pour le transfert de ses données sans que cette mention soit en contradiction avec l'article L 1111-8.

Toutefois, cette exception fait craindre une entorse au principe de la finalité car, pour rappel, ce principe exige que le responsable du traitement des données se limite uniquement à l'utilisation qu'elle avait initialement prévue et qui, présentée au patient a obtenu son consentement. Ce dernier avait donné son consentement pour la conservation de ses données au sein du système de l'établissement de santé et non pas forcément pour un transfert vers un hébergeur aussi agréé soit-il. D'ailleurs, les chances que la possibilité de déplacement de ces renseignements ait été mentionnée lors de l'information préalable du patient quant aux conditions de traitement et de conservation de ses données médicales sont minimes et presqu'inexistantes.

En somme, le cadre juridique qui entoure l'hébergement de données de santé dans le dossier médical personnel est plus souple s'agissant de recueil du consentement de l'individu probablement pour deux raisons principales. La première résiderait dans le fait que le patient, en général, ignorant des techniques informatiques ne dispose pas de connaissances suffisantes pour se prononcer sur la qualité des services d'un hébergeur au point de pouvoir refuser qu'il conserve ses données personnelles. La seconde raison est le fait que l'Asip santé, en charge du

déploiement du dossier médical personnel, fait au préalable, un travail de prospection de nature à rassurer les patients et les professionnels. L'agence s'assure des garanties de confidentialité qu'offre un hébergeur avant que l'agrément ne lui soit accordé.

Section 2: la gestion du DMP: Les garanties de la confidentialité dans le DMP

Les données médicales étant personnelles, confidentielles et très sensibles, le dossier médical personnel est censé bénéficier d'une protection hautement sécurisée. Le titulaire des données contenues dans le dossier médical personnel bénéficie d'une protection issue du droit commun organisé par plusieurs textes de loi. Le caractère personnel de ces données induit la protection de l'intimité de la vie privée de l'individu qui oblige les intervenants à un devoir de secret professionnel. La principale source de cette protection est l'article 9 du Code civil qui impose le respect de la vie privée, complété par les sanctions édictées par le code pénal pour réprimer le manquement à l'obligation de secret professionnel.

Techniquement, les autorités en charge du projet comptent, d'une part, sur un identifiant national de santé différent du numéro de sécurité sociale, calculé automatiquement lors de la création du dossier médical personnel qui est unique[954], pérenne[955], non déductible[956] et non signifiant[957]. D'autre part, la carte de professionnel de santé, qui est une carte d'identité professionnelle électronique n'est détenue que par les seuls professionnels de santé habilités. Cette carte qui comporte un code confidentiel qui la protège et sans laquelle il est impossible de l'utiliser est le seul moyen par lequel un professionnel peut accéder à un DMP. Grâce aux informations contenues dans cette carte, les traces d'accès laissées dans le DMP permettent

[954] Cet identifiant n'est attribué qu'à un seul individu. Il permet donc de ne pas confondre le DMP d'une personne avec celui d'une autre.

[955] Chaque individu conserve son identifiant toute sa vie.

[956] Il est impossible de retrouver l'identifiant national de santé à partir du numéro de sécurité sociale ou de l'identité.

[957] L'identifiant connu ne génère pas d'informations permettant de remonter jusqu'à l'individu concerné.

d'identifier le professionnel de santé. Le troisième élément technique de garantie est l'environnement sécurisé de l'hébergement assuré par l'État.

Juridiquement, en plus des garanties assurées par les professionnels, une autre est détenue par le patient lui-même en dehors du consentement qu'il a donné pour l'hébergement: c'est son droit légal de limiter l'accès à son dossier médical personnel. Ces deux dernières garanties retiendront notre attention à cette étape de notre étude.

Paragraphe 1 : L'hébergement sécurisé du DMP

Pour garantir la sécurité et la confidentialité des données médicales hébergées, il est nécessaire de conjuguer les actions de deux types de professionnels : les professionnels de l'informatique et les professionnels de la santé.

A. Au niveau de l'hébergeur, professionnel de l'informatique

L'hébergeur est « *l'intermédiaire agissant pour offrir des services de conservation de documents technologiques sur un réseau*[958] ». Il peut être un éditeur de logiciels, un prestataire informatique de la e-santé ou une société dans le domaine du matériel médical. Aux termes de l'article L 1111-8 du code de la santé publique l'hébergeur est la personne physique ou morale chez laquelle les professionnels de santé ou les établissements de santé ou la personne concernée dépose des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins. « *L'activité d'hébergement recouvre plusieurs réalités : elle peut consister en une application associant traitement et archivage des données. Il peut s'agir d'un simple archivage ou de la fourniture d'un site de sauvegarde. Participe à l'hébergement tout opérateur intervenant dans cette*

[958] TRUDEL, Pierre. *Introduction à la loi concernant le cadre juridique des technologies de l'information*. P. 198.

chaîne de valeurs. Seul celui qui contractualise avec les producteurs de soins est soumis à l'agrément, charge à lui de préciser les modalités d'intervention des autres acteurs[959].

Cette dernière phrase amène à s'interroger sur ce qui caractérise l'hébergeur de données de santé qui est tenu de se soumettre à la procédure d'agrément par rapport aux autres, les prestataires de services de santé à domicile par exemple.

L'article 4 de la loi informatique et libertés dispose que celle-ci n'est pas applicable *« aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vertu du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises* ». Il s'ensuit donc que les prestataires de données de santé à caractère personnel qui proposent des services de type réseau de télécommunication, pour lesquels la durée de stockage des informations est limitée à la traversée des équipements actifs des réseaux sans mise en œuvre de traitement des nouveaux applicatifs, ne sont pas considérés comme hébergeurs entrant dans le champ de la procédure de demande d'agrément. Partant de cette logique, l'Asip santé analyse[960] le cas des prestataires de services de santé à domicile (PSAD) sous différents angles : si le PSAD conserve les seules données de santé à caractère personnel qu'il a recueillies ou produites au sein de dossier informatisé conservé localement dans son propre système, il ne peut être considéré comme un hébergeur de données de santé à caractère personnel au sens de l'article L 1111-8 du code de la santé publique. Il demeure un simple responsable du traitement au sens de la loi informatique et libertés. Mais lorsqu'un professionnel de santé ou un établissement de santé dépose des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic ou de soins sur un dossier tenu par le PSAD, ce dernier doit être agréé pour l'hébergement des données de santé à caractère personnel car il se comporte

[959] Asip santé. *L'agrément des hébergeurs de données de santé à caractère personnel*. [en ligne], 7 février 2011. Disponible sur: www.esante.gouv.fr. Consulté le 10 octobre 2013

[960] ASIP. *Note juridique relative à l'hébergement de données de santé à caractère personnel aux dossiers détenus par les PSAD et les distributeurs de DM*. 21 mars 2012. Aux termes de l'article de 5232-10 du code de la santé publique « *Le prestataire de services et les distributeurs de matériel assurent une prestation globale comportant de façon indissociable l'ensemble des éléments définis par arrêté du ministre chargé de la santé*. » L'arrêté du 19 décembre 2006 impose au PSAD et distributeurs de dispositifs médicaux d'assurer le contrôle de la bonne utilisation du matériel, le rappel éventuel des informations, en coordination avec l'équipe médicale et les auxiliaires médicaux en charge de la personne. Ils sont tenus d'assurer le contrôle régulier de l'observance et d'alerter, le cas échéant, le médecin traitant en cas d'anomalies. Disponible sur: Http://esante.gouv.fr/services/reperes-juridiques/note-juridique-relative-a-l-hebergement-de-donnees-de-sante-a-caractere-. Consulté le 1er novembre 2013.

comme un hébergeur au sens de l'article L 1111-8. PSAD peut même recourir aux services d'un sous-traitant pour faire héberger ses dossiers de suivi. Il demeure responsable du traitement et le sous-traitant, l'hébergeur tenu de solliciter un agrément.

«Pour exercer son activité, l'hébergeur doit démontrer sa capacité à mettre en œuvre une politique de sécurité et de confidentialité renforcée, en vue de l'obtention d'un agrément pour l'hébergement des données de santé à caractère personnel[961]*.* » Les hébergeurs sont tenus d'assurer la confidentialité, la sécurité, l'intégrité et la disponibilité des données de santé qui leur sont confiées ; ce qui peut engager leur responsabilité en cas de violation du droit à la confidentialité des titulaires des données.

1. L'agrément des hébergeurs

Conformément aux dispositions[962] de l'article L 1111-8 du code de la santé publique, toute personne physique ou morale hébergeant des données de santé à caractère personnel recueillies ou produites à l'occasion d'activités de prévention, de diagnostic ou de soins pour le compte d'un tiers doit être agréée par décision du ministère en charge de la santé qui se prononce après avis[963] de la CNIL et d'un Comité d'agrément. Il s'ensuit donc qu'il n'est exigé d'agrément que pour une personne qui conserve les données de santé sans en avoir été le producteur. Les informations hébergées doivent avoir été externalisées[964]. Le professionnel ou l'établissement de santé qui conserve lui-même les données de santé de ses patients *« quel*

[961] Asip santé. *L'agrément des hébergeurs de données de santé à caractère personnel*. 7 février 2011. Disponible sur: www.esante.gouv.fr. Consulté le 10 octobre 2013.

[962] « *les conditions d'agrément des hébergeurs de données, quel qu'en soit le support, sont fixées par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés et des Conseils de l'ordre des professions de santé. Ce décret mentionne les informations qui doivent être fournies à l'appui de la demande d'agrément, notamment les modèles de contrat (...) et les dispositions prises pour garantir la sécurité des données traitées (…), en particulier les mécanismes de contrôle et de sécurité dans le domaine informatique ainsi que la procédure de contrôle interne…* »

[963] CNIL. Délibération n° 2006-081 du 21 mars 2006 *portant avis sur la demande d'agrément présentée par la société inVita, candidate à l'hébergement du dossier médical personnel dans le cadre de son expérimentation*. www.cnil.fr.

[964] LAVENUE, Jean-Jacques, BEAUVAIS, Grégory. *La commercialisation des données personnelles, perspectives et prospective : l'exemple des données de santé et du DMP* in La sécurité de l'individu numérisé p. 177

qu'en soit le support papier ou informatique » n'est donc pas soumis à cette procédure. Le décret[965] relatif à l'hébergement des données de santé à caractère personnel prévu par la loi précitée décrit les conditions d'octroi de l'agrément. Il donne les détails de la procédure et du contenu de la demande d'agrément, la composition du Comité d'agrément et les modalités de renouvellement et de retrait de l'agrément.

a. La procédure de demande d'agrément

« *La procédure d'agrément a pour objet d'apprécier la capacité économique et financière, éthique et juridique, et la politique de sécurité de l'organisme candidat*[966]*.*» Le demandeur d'un agrément doit adresser au ministre chargé de la santé un dossier comportant un certain nombre d'éléments définis à l'article R 1111-12. Le ministre transmet le dossier à la Commission nationale informatique et libertés qui apprécie les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données. La Commission rend son avis dans un délai de deux mois à compter de la réception du dossier ; ce délai peut être reporté une fois sur demande motivée de son président. Dès que la Commission s'est prononcée ou à l'expiration du délai qui lui est imparti, elle transmet la demande d'agrément accompagnée, le cas échéant, de son avis, au Comité d'agrément[967]. Ce Comité se prononce sur tous les aspects du dossier, en particulier sur les garanties d'ordre éthique, déontologie, technique, financière et économique qu'offre le candidat. Il émet son avis dans le mois qui suit la réception du dossier transmis par la CNIL. Il peut, toutefois, demander un délai supplémentaire d'un mois. Finalement, le ministre chargé de la santé dispose d'un délai de deux mois suivant l'avis du Comité d'agrément, pour rendre sa décision au demandeur. Passé ce délai, son silence vaut décision de rejet[968]. Le décret ne précise pas les voies de recours qui s'offrent aux candidats à l'agrément en cas de rejet mais l'on peut envisager que s'agissant d'une décision administrative, le candidat pourra toujours exercer un recours pour excès de pouvoir devant la juridiction administrative. L'engagement de cette procédure par les professionnels informatiques n'empêche pas l'exercice des formalités de déclaration préalable

[965] 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 (dispositions réglementaires). JORF n° 4 du 5 janvier 2006. NOR: SANX0500308D.

exigées par la loi informatique et libertés[969] de toute personne responsable de traitement automatisé de données à caractère personnel que sont, ici, les professionnels et/ou établissements de santé.

Concrètement, les démarches à entreprendre par les candidats à l'agrément sont recensées sur le site de l'Asip santé, au sein d'un référentiel de constitution de demande d'agrément. L'Asip santé assurant le secrétariat du Comité d'agrément depuis le 1er mars 2010 par délégation à la stratégie des systèmes d'information de santé, est chargée de la gestion des candidatures. À ce titre, l'agence est responsable de la retranscription pas écrit des avis du Comité d'agrément et de l'envoi de ces avis au ministre chargé de la santé. « *L'Asip santé a défini le référentiel de constitution des dossiers de demande d'agrément pour l'hébergement des données de santé à caractère personnel. Chargée par le ministère en charge de la santé de la pré instruction des dossiers de candidature et du secrétariat du Comité d'agrément des hébergeurs, elle joue un rôle central pour assurer l'application des dispositions du décret du 4 janvier 2006, pour observer et mesurer les évolutions de l'activité d'hébergement de*

---

[966] ASIP santé. *Hébergement de données de santé : le point sur le renouvellement de l'agrément* .17 septembre 2013. http://esante.gouv.fr/en/node/4201. Consulté le 21 janvier 2014.

[967] Le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel fixe la composition du Comité d'agrément: Article R.1111-11: «- I. - *Le Comité d'agrément comprend : Un membre de l'inspection générale des affaires sociales nommé sur proposition du chef de l'inspection générale des affaires sociales ; deux représentants des associations compétentes en matière de santé, agréées au niveau national dans les conditions prévues à l'article L. 1114-1 ; deux représentants des professions de santé, l'un nommé sur proposition du Conseil national de l'ordre des médecins et l'autre sur proposition de l'Union nationale des professions de santé; trois personnalités qualifiées (une personne choisie en raison de ses compétences dans les domaines de l'éthique et du droit et une personne choisie en raison de ses compétences en matière de sécurité des systèmes d'information et de nouvelles technologies, une personne choisie en raison de ses compétences dans le domaine économique et financier). Le directeur général de la santé, le directeur de l'hospitalisation et de l'organisation des soins, le directeur des Archives de France, le directeur général des entreprises et le directeur général de la concurrence, de la consommation et de la répression des fraudes, ou leurs représentants, assistent aux séances du Comité avec voix consultative.*
« II. - Les membres du Comité d'agrément, dont celui qui, parmi eux, exercera la présidence du Comité, sont nommés pour cinq ans par arrêté du ministre chargé de la santé. Leur mandat est renouvelable une fois.» http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000264665&dateTexte=&categorieLien=id. Consulté le 21 janvier 2014.

[968] Article R 1111-10. 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 (dispositions réglementaires).

[969] Article 26 de la loi informatique et liberté.
Les formalités des professions médicales et paramédicales sont simplifiées. Elles consistent en une déclaration de conformité de leur traitement à la norme simplifiée n° 50 établie par la CNIL. Ces normes simplifiées peuvent être consultées sur le site de la CNIL.

données de santé et les évolutions possibles de la procédure[970]. » La mise en place d'un tel référentiel assure aux candidats un traitement équitable et efficace de leur candidature car il fixe des normes qui permettent une formalisation stricte du contenu du dossier de demande d'agrément. Ce dispositif élaboré en concertation avec les industriels, la CNIL et le Comité d'agrément des hébergeurs favorise une auto évaluation par les candidats. L'Asip santé tient sur son site Internet une liste des hébergeurs agréés[971]. Le 9 décembre 2014, elle comptait 76 hébergeurs agréés de données de santé à caractère personnel[972] après décisions d'agrément rendues par le ministre en charge de la santé. Par exemple, le groupement Santeos Atos Worldline Extelia est agréé pour l'hébergement du dossier médical personnel par décision du ministre chargé de la santé du 10 novembre 2010 ; après avis de la CNIL du 30 septembre 2010 et du Comité d'agrément placé auprès du ministre du 1er octobre 2010[973]. L'article R 1111-15 du décret dispose que l'agrément est délivré pour une durée de trois ans ; les hébergeurs ayant la possibilité de demander un renouvellement aux plus tard six mois avant la fin de la période d'agrément.

Aux termes de l'article R 1111-12 du décret, le dossier de demande d'agrément comprend les éléments suivants :

« *1° L'identité et l'adresse du responsable du service d'hébergement et, le cas échéant, de son représentant ; pour les personnes morales, les statuts sont produits ;*

---

970 Asip santé. *Le rôle de l'agence des systèmes de santé dans la procédure d'agrément*. 23 novembre 2011. http://esante.gouv.fr/services/reperes-juridiques/le-role-de-l-agence-des-systemes-d-information-partages-de-sante-dans-la. Consulté le 11 octobre 2013.

971 Dans le cadre du DMP deux catégories d'hébergeurs sont à distinguer : un hébergeur dit « de référence », à compétence nationale, dont le rôle sera de garantir la continuité du service, la reprise et la transférabilité inter-opérateurs des dossiers ; dans ce cadre, cet hébergeur n'aura pas d'activités commerciales liées à cette mission et sera sélectionné à l'issue d'un appel d'offres ouvert. Il sera rémunéré proportionnellement au nombre de dossiers gérés sur la base d'un prix administré, avec un minimum garanti (5 millions de dossiers). Les hébergeurs « agréés » (au sens de la loi Kouchner), en compétition nationale, opèrent selon les normes d'interopérabilité de l'hébergeur de référence et rémunérés proportionnellement au nombre de dossiers hébergés en fonction d'un tarif administré issu du retraitement du tarif de l'hébergeur de référence. Cet hébergeur pourrait offrir l'accès gratuit au DMP dans le cadre d'une offre de bouquets de services payants ou rétribués. L'hébergeur de référence est donc un hébergeur agréé, qui n'offre pas de services mais bénéficie d'un tarif spécifique. Mission interministérielle de revue de projet sur le DMP. *Rapport sur le dossier médical personnalisé*. n° 2007-M-068-01. 8 novembre 2007. p. 37. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000713/0000.pdf. Consulté le 10 décembre 2013.

972 Asip santé. *Hébergeurs agréés*. [en ligne], disponible sur: http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees. Consulté le 21 mai 2014.

973 BACHELOT-NARQUIN Roselyne. *Décision du 10 novembre 2010 portant agrément du groupement constitué entre les sociétés* Santeos Atos Worldline Extelia en qualité d'hébergeur de données de santé à caractère personnel. [en ligne], NOR: SASX1030992S. Disponible sur http://www.sante.gouv.fr/fichiers/bo/2010/10-12/ste_20100012_0100_0081.pdf. Consulté le 10 juillet 2014.

2°Les noms, fonctions et qualifications des opérateurs chargés de mettre en œuvre le service ainsi que les catégories de personnes qui, à raison de leurs fonctions ou pour les besoins du service, ont accès aux données hébergées ;

3° L'indication des lieux dans lesquels sera réalisé l'hébergement ;

4° Une description du service proposé.,

5° Les modèles de contrat devant être conclu, en application du deuxième alinéa de l'article L 1111-8 (…)

6° Les dispositions prises pour assurer la sécurité des données et la garantie des secrets protégés par la loi, notamment la présentation de la politique de confidentialité et de sécurité prévue au 2° de l'article R. 1111-9 ;

7° Le cas échéant, l'indication du recours à des prestataires techniques externes et les contrats conclus avec eux ;

8° 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.

L'hébergeur déjà agréé informe sans délai le ministre chargé de la santé de tout changement affectant les informations mentionnées ci-dessus et de toute interruption, temporaire ou définitive, de son activité. »

Ce contenu exigé du candidat à la demande d'agrément vise à vérifier que ce dernier remplit les conditions prévues par les dispositions de l'article R 1111-9 marquées par l'insistance sur la capacité à assurer la sécurité et la confidentialité des données.

b. Les conditions d'octroi de l'agrément

L'article R 1111-9 fixe 6 conditions pour l'octroi de l'agrément de l'hébergement des données de santé à caractère personnel. La première et les trois dernières ont trait à la fiabilité de l'organisation du système d'information qu'offre le candidat. Mais, ensemble, elles conduisent au même objectif que la seconde condition qui impose à l'hébergeur de définir et mettre en œuvre une politique de confidentialité et de sécurité.

i. Les conditions ayant trait à la fiabilité du système d'information

Le demandeur doit offrir toutes les garanties pour l'exercice de cette activité notamment par le recours à des personnels qualifiés en matière de sécurité et d'archivage des données et par la mise en œuvre de solutions techniques, une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution de données confiées, ainsi qu'un usage conforme à la loi[974]. En somme, le candidat doit démontrer qu'il aura un comportement responsable vis-à-vis des données qui lui seront confiées. Cette première condition pourrait suffire à résumer l'esprit de la législation en matière d'hébergement de données de santé à caractère personnel mais, compte tenu de la sensibilité desdites données, le législateur estime nécessaire de compléter la liste des conditions avec des détails qui viendront renforcer cette première.

Dans le cas où le candidat serait établi hors des frontières françaises, il devra identifier son représentant sur le territoire national c'est-à-dire une personne physique ou morale établie sur le territoire français, ou qui, sans être établie sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne recourt à des moyens de traitement situé sur le territoire français à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de l'Union[975]. Afin d'ouvrir le marché de l'hébergement à un plus grand nombre de candidats notamment ceux qui résident en dehors de la France, les entreprises qui ont recours au système de *"cloud*[976]*"* peuvent présenter leur dossier. Les avantages de la simplicité et du faible coût des solutions *"cloud"* intéressent de nombreuses entreprises mais peuvent poser des problèmes au niveau de la protection des

[974] *« La détention et le traitement sur des supports informatiques de données de santé à caractère personnel par (…) des hébergeurs de données de santé à caractère personnel sont subordonnés à l'utilisation des systèmes d'information conformes aux prescriptions adoptées en application de l'article L 1110-4 et aux référentiels d'interopérabilité et de sécurité arrêtée par le milieu chargé de la santé après avis du groupement mentionné à l'article L 1111-24 ».*Article L 1111-8, alinéa 4 du code de la santé publique.

[975] Article 5 de la loi informatique et libertés.

[976] le "cloud computing" expression anglaise qui se traduit littéralement par "informatique dans le nuages" est la forme la plus évoluée des externalisations, dans laquelle le client ou l'utilisateur dispose des services en ligne dont l'administration et la gestion opérationnelle sont effectués par un sous-traitant (externe ou interne). Le cloud se caractérise également par une facturation à la demande et une disponibilité quasi immédiate des ressources. Dans de nombreux cas, le client ne connaît pas la localisation des données. La simplicité et le faible coût des solutions cloud intéresse de nombreuses entreprises mais peut poser des problèmes au niveau de la protection des données personnelles et notamment sur les questions de responsabilité du sous-traitant, de sécurisation du traitement des données personnelles ou de transfert de données vers des pays ne disposant pas d'une législation protectrice des données personnelles.

données personnelles et notamment sur les questions de responsabilité du sous-traitant, de sécurisation du traitement des données personnelles ou de transfert de données vers des pays ne disposant pas d'une législation protectrice des données personnelles. Cette externalisation représentant un enjeu économique majeur[977] a fait l'objet d'une consultation[978] de la CNIL auprès des parties prenantes (clients, prestataires, conseils) d'octobre à novembre 2011[979]. Désormais, la Commission encadre cette activité dans le but d'offrir un haut niveau de protection, gage de garanties à la confidentialité des données à caractère personnel ; c'est pourquoi elle a publié des recommandations[980] pratiques à destination des entreprises françaises, et notamment des PME, qui souhaitent avoir recours à des prestations de *"cloud"* en juin 2012. Sept étapes préalables ont été définies afin de déterminer la qualification juridique du prestataire, de délimiter les responsabilités des cocontractants et d'évaluer le niveau de protection assuré par le prestataire aux données traitées. La CNIL veille à éviter que le *"cloud"* n'aboutisse à une diminution du niveau de protection des données, particulièrement s'agissant des données sensibles.

Pour pallier les difficultés de détermination de la loi applicable aux solutions de cloud computing, les parties prenantes de la consultation de 2011 devaient se prononcer sur l'utilisation des moyens proposés par l'article 69 de la loi informatique et libertés qui prévoit expressément les outils permettant d'encadrer ce type de transfert de données. Il s'agit de clauses contractuelles types, des règles internes d'entreprise (ou BCR). Si ces moyens ont été

---

977 « *Ce marché représenterait déjà 6 milliards d'euros au niveau européen, avec une croissance annuelle de l'ordre de 20 %.*» CNIL. *Cloud computing: la CNIL engage le débat*. 11 Octobre 2011. www.cnil.fr

978 Une copie de la fiche de consultation (CNIL. Consultation cloud computing) est accessible par la page web de l'article: *Cloud computing: la CNIL engage le débat*. 11 Octobre 2011. www.cnil.fr.

La synthèse des réponses des parties prenantes à la consultation est accessible sur le lien suivant: http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Synthese_des_reponses_a_la_consultation_publique_sur_le_Cloud_et_analyse_de_la_CNIL.pdf. Consulté le 10 décembre 2013.

979 CNIL. *Cloud computing: la CNIL engage le débat*. 11 Octobre 2011. www.cnil.fr.

980 CNIL. *Cloud computing. Les 7 étapes pour garantir la confidentialité des données*. 1er Juillet 2013.
« Avant tout engagement commercial, l'organisme souhaitant recourir à une prestation d'externalisation devra mener une réflexion spécifique afin :
1. D'identifier clairement les données et les traitements qui passeront dans le cloud ;
2. De définir ses propres exigences de sécurité technique et juridique ;
3. De conduire une analyse des risques afin d'identifier les mesures de sécurité essentielle pour l'entreprise ;
4. D'identifier le type de cloud pertinent pour le traitement envisagé ;
5. De choisir un prestataire présentant des garanties suffisantes ;
6. De revoir la politique de sécurité interne ;
7. De surveiller les évolutions dans le temps. »
www.cnil.fr. Consulté le 11 octobre 2013.

adoptés, ils ne règlent pas définitivement le problème de l'insécurité de données personnelles causée par les différences de législation en la matière. La révélation de l'existence du programme de surveillance américain PRISM[981] relance le débat et révèle l'urgence d'une solution qui clarifie l'encadrement juridique de la protection des données personnelles au plan international. En mars 2013, le G29, regroupant l'ensemble des autorités de protection des données personnelles s'est saisi de cette question. Quant à la CNIL, elle a constitué, en mars 2013, un groupe de travail sur la question de l'accès des autorités étrangères aux données personnelles. Les débats se poursuivaient encore le 10 juillet 2014, des rencontres sont organisées avec les acteurs concernés dont les avocats, les opérateurs, les institutions, la société civile afin de recueillir leurs avis. Le premier bilan devait être fait depuis septembre 2013.

Il est également attendu du candidat qu'il isole l'activité d'hébergement et les moyens qui lui sont dédiés, dans son organisation de la gestion des stocks et des flux de données. Il devra définir et mettre en place des dispositifs d'information sur l'activité d'hébergement à destination des personnes à l'origine du dépôt, notamment en cas de modification substantielle des conditions de réalisation de cette activité. Le premier intérêt de cette condition réside dans le fait qu'un hébergeur peut avoir à exercer plusieurs activités qui ne nécessitent pas toutes un agrément. C'est la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé qui a créé un statut « *d'hébergeur agréé* ». Le ministre en charge de la santé ne délivre pas d'agrément général ; c'est pourquoi les dossiers présentés par les candidats doivent clairement identifier le type de prestation d'hébergement de données de santé à caractère personnel pour lequel est demandé l'agrément. L'organisme peut donc être agréé autant de fois qu'il y a de prestations différentes proposées. Quelquefois, la différence entre les activités menées par le même organisme n'est pas facile à faire et cela a des

[981] « *PRISM est un programme de surveillance mis en place par les États-Unis pour suivre de manière étendue l'activité en ligne d'un très grand nombre de personnes. Il permet à la NSA de collecter des informations auprès d'entreprises américaines, dont la plupart des géants du Web. Le système PRISM collecte courriels, fichiers, photos, le contenu des communication audio et vidéo par internet, des informations sur les réseaux sociaux et des événements comme la connexion à certains sites. Les entreprises doivent aussi être en mesure de répondre à des requêtes spéciales, selon les documents révélés par "the guardian"*.» Le monde. *Comprendre le programme "prism"* . 11 juin 2013. www.lemonde.fr. Consulté le 2 mai 2014.

répercussions sur la recevabilité des demandes par le Comité d'agrément qui relate un cas dans son premier rapport d'activité 2006-2011[982].

« *L'exemple des « Contract Research Organisation » (CRO) ou sociétés de recherche sous contrat en est une illustration :*

Ces sociétés ont pour mission, sous l'autorité du promoteur d'une recherche biomédicale, de gérer la collecte, la conservation et l'exploitation des données recueillies dans le cadre de la recherche auprès des investigateurs.

Ces sociétés peuvent-elles être considérées comme hébergeurs des données relatives à l'état de santé des patients se prêtant à la recherche et conservées exclusivement à cette fin?

Les données collectées dans ce cadre sont, en général, indirectement nominatives, le patient étant identifié par des initiales et/ou un numéro, mais elles demeurent des données à caractère personnel.

Le Comité d'agrément a débattu de cette question, afin de savoir si les CRO devaient déposer un dossier de demande d'agrément pour l'hébergement de données de santé à caractère personnel recueillies à l'occasion de recherche dans le domaine de la santé.

Les avis ont été divergents au sein du Comité. Selon certains membres du Comité d'agrément, dans la mesure où les données sont indirectement nominatives et que la table de correspondance est conservée par le médecin instigateur de la recherche, les risques pour la confidentialité des données sont très limités et l'agrément ne serait pas nécessaire. En outre, ces données, pour la plupart, recueillies à l'occasion d'activités de soins sont déjà soumises à des mesures de protection spécifiques.

Le code de la santé publique encadre, précisément la conduite de ces études (articles L 1121-1 et suivants) et la loi Informatique et Libertés a défini les conditions de leur autorisation dans le chapitre IX relatif aux traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé. La CNIL a, en outre, en concertation avec les milieux de la recherche, défini les caractéristiques des traitements propres à ces recherches biomédicales dans une méthodologie de référence (Méthodologie de référence MR-001 pour les traitements de données personnelles opérées dans le cadre de recherches biomédicales – octobre 2010). Aussi, selon ces membres, soumettre les bases de données de santé à caractère personnel créées dans le cadre d'une recherche dans le domaine de la santé à l'agrément prévu

[982] Comité d'agrément. *Premier rapport d'activité du Comité d'agrément des hébergeurs : 2006-2011 sous la présidence du Dr Philippe BICLET*. Rapport publié par l'Asip santé le 7 Septembre 2011. p. 12-13. http://esante.gouv.fr/sites/default/files/Rapport_CAH_4.08.11_VF.pdf. Consulté le 28 mai 2014.

par l'article L 1111-8 du code de la santé publique, alourdirait les démarches déjà très pesantes des acteurs de la recherche.

Pour d'autres membres du Comité d'agrément, l'article L1111-8 du code de la santé publique s'applique aux CRO, en raison de la conservation de données de santé à caractère personnel par un tiers qui n'est pas le producteur des données. A cet égard, il ne serait pas justifié d'exonérer ces activités d'hébergement de l'agrément prévu par la loi, la personne dont les données sont ainsi conservées devant pouvoir bénéficier des mêmes garanties que les autres.

Face à ces divergences de position, la Mission Juridique du Conseil d'État auprès du ministère en charge de la santé a été saisie. Dans sa réponse du 10 mai 2011, la Mission juridique a d'abord insisté sur la nécessité d'assurer la sécurité des données de santé à caractère personnel en raison de leur sensibilité :

« *Ces données font partie des catégories particulières dont la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel prévoit qu'elles ne peuvent être traitées à moins que le droit interne ne prévoie des garanties appropriées* ».

Se fondant sur la protection assurée en droit interne par la loi du 6 janvier 1978 informatique et libertés, la mission juridique a conclu dans les termes suivants que les bases de données de santé constituées à l'occasion de recherches biomédicales n'étaient pas soumises à la procédure d'agrément prévu à l'article L1111-8 du code de la santé publique et précisée par le décret 2006-6 du 4 janvier 2006 :

« En application de l'article 53 de la loi du 6 janvier 1978 informatique et libertés, les traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé sont soumis aux dispositions de cette loi, à l'exception des articles 23 à 26, 32 et 38. […] Nous avons donc bien deux régimes exclusifs l'un de l'autre, celui de l'hébergement des données de santé au sens de l'article L 1111-8 et celui du traitement des données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, sur le fondement de l'article L 1121-1 et de la loi du 6 janvier 1978. Les organismes qui veulent conserver des données de santé à des fins de recherche n'ont pas dans l'état des textes à recueillir un agrément sur la base de l'article L 1111-8 qui ne concerne que ceux répondant à la définition donnée par cet article[983]*. »*

[983] Idem

Dans l'hypothèse où l'hébergeur offrirait plusieurs services en dehors de la conservation des données à caractère personnel, cette condition tendrait également, à exiger de lui de séparer l'activité d'hébergement des autres dans le but de limiter les risques d'accès non autorisé ou de confusion d'informations. Dans ce contexte, il est judicieux d'informer les responsables de traitement de sa situation et de toute autre modification ultérieure touchant aux conditions de conservation des données qu'ils lui ont confiées. Ceux-ci auraient alors toute latitude de contracter avec ce prestataire de service informatique ou de poursuivre leur collaboration en toute connaissance de cause. Cette condition défend donc le droit à l'information en faveur des responsables de traitement de données à caractère personnel. Cette recherche de clarté trouve également son importance dans le fait qu'elle servira à déterminer plus facilement les responsabilités en cas d'incident pouvant aboutir à une perte ou une divulgation de données. En plus, le propriétaire sera tenu informé de toutes les opérations dont son dossier a fait l'objet grâce aux traces de ces interventions imposées par le dispositif.

L'identification des personnes en charge de l'activité d'hébergement, dont un médecin, en précisant le lien contractuel qui les lie à l'hébergeur est la dernière condition. C'est une garantie réglementaire qui marque par son caractère apparemment spécial. Exiger l'intervention de médecins dans un organisme dont l'activité est purement informatique paraît étrange, mais cela se justifie par le caractère tout aussi spécial des données de santé hébergées. Cette nouvelle fonction instituée par le décret 2006-6 impose au médecin d'exercer ses missions dans le cadre de l'organisation prévue dans le contrat qui lie l'hébergeur au responsable du traitement tout comme dans le cadre de l'exécution de son contrat de travail[984]. Le Conseil national de l'ordre des médecins a précisé que l'indépendance du médecin recruté par l'hébergeur impose qu'il soit tenu au secret vis-à-vis de l'hébergeur et que « *les missions qui lui sont confiées doivent être exclusives de toute activité de soins, de prévention ou de contrôle de l'organisme, quel qu'il soit* »[985]. Dès lors, il exerce une mission particulière avec une subordination hiérarchique à l'hébergeur mais une indépendance déontologique conformément à l'article 95[986] du code de déontologie médicale (article R 4127-95 du code de

[984] Le médecin doit être lié contractuellement à l'hébergeur mais il n'est pas obligatoire qu'il en soit le salarié.

[985] CRESSARD, P. *L'actualité de notre secret médical*. Bulletin de l'ordre des médecins. Février 2006. n°2, Éditorial.

[986] *« Le fait pour un médecin d'être lié dans son exercice professionnel par un contrat ou un statut à un autre médecin, à une administration, une collectivité ou tout autre organisme public ou privé n'enlève rien à ses devoirs professionnels et en particulier à ses obligations concernant le secret professionnel et l'indépendance de ses décisions. En aucune circonstance, le médecin ne peut accepter de limitation à son indépendance dans son*

la santé publique). Selon le Comité[987] d'agrément, cette exigence vise à interdire au médecin de l'hébergeur d'exercer des fonctions de direction associée à une rémunération proportionnelle au chiffre d'affaires de l'organisation. Le Conseil national de l'ordre des médecins a publié sur son site un modèle de contrat type du médecin de l'hébergeur établi à partir de clauses types élaborées par l'Asip santé. Ce modèle de contrat permet d'offrir un texte correspondant au mieux aux exigences professionnelles. Le contrat du médecin impliqué dans l'activité d'hébergement doit être soumis au contrôle de l'ordre des médecins car, au sein de cette organisation, il est le garant du respect du secret médical. Le médecin évalue, en fonction des données auxquelles il accède, la conduite à tenir dans l'intérêt du patient concerné et rend compte de son action à son employeur et aux clients sans rupture de confidentialité. Ses missions ont été définies après une concertation entre le Conseil national de l'ordre des médecins et la CNIL. Le médecin veille à la confidentialité des données de santé hébergées et au respect de conditions d'accès à celles-ci telles que définie dans la prestation d'hébergement. A cette fin, il peut faire des recommandations et peut être saisi de toute demande du responsable du traitement ou de toute personne habilitée visant à procéder aux vérifications de cohérence en cas de soupçon de divergence d'informations ou de doublon au sein des dossiers médicaux. Il est autorisé à y accéder en cas de besoin et c'est le seul chez l'hébergeur à en avoir le droit. Il peut être sollicité en cas de demande de copie ou de destruction d'un document ou de toute autre demande de la part du titulaire. En tant que professionnel de santé, il est également tenu d'utiliser la carte de professionnel de santé pour effectuer ses accès conformément à l'article R 1110-3 du décret[988] *"confidentialité"* du 15 mai 2007. En accord avec la personne dépositaire de données et le correspondant informatique et libertés, s'il en existe au sein de la structure d'hébergement, il veille au respect des droits de la personne dont les données de santé à caractère personnel sont hébergées, en particulier en s'assurant de l'exercice effectif des droits couverts au titre de la loi informatique et libertés. Dans ce cadre, il est habilité à élaborer des règles de bonnes pratiques.

---

exercice médical de la part du médecin, de l'entreprise ou de l'organisme qu'il emploie. Il doit toujours agir, en priorité, dans l'intérêt de la santé publique et dans l'intérêt de personnes et de leur sécurité au sein des entreprises ou des collectivités où il exerce ».

[987] Comité d'agrément. *Premier rapport d'activité du Comité d'agrément des hébergeurs : 2006-2011 sous la présidence du Dr Philippe BICLET*. Rapport publié par l'Asip santé le 7 Septembre 2011. p. 19. http://esante.gouv.fr/sites/default/files/Rapport_CAH_4.08.11_VF.pdf. Consulté le 28 mai 2014.

[988] 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. Texte n° 210. NOR: SANP0721653D.

Après analyse de cette procédure, force est de constater qu'elle comporte quelques éléments de lourdeur et de redondance. La double instruction des demandes par le Comité d'agrément et la CNIL génère des coûts humains et financiers importants tout comme la double contrainte de calendrier du Comité et de la CNIL qui complique le respect des délais prévus par les textes. Le texte du décret reprend, à plusieurs reprises, des conditions qui ramènent définitivement, au même esprit de politique de sécurité et de confidentialité. Dans son premier rapport, le Comité d'agrément a relevé que la procédure de demande d'agrément souffre de lourdeur et a préconisé un allégement pour la rendre plus fluide et une révision du référentiel afin d'éviter des redondances et aller dans le sens d'une stricte économie dans la gestion des fonds publics[989]. D'ores et déjà, la CNIL et le Comité d'agrément disposent d'un cahier des charges type élaboré par l'Asip santé qui renseigne les candidats et assure la pré-instruction des dossiers. Ensuite, les deux procédures se déroulent de manière indépendante, *sans préjudice d'un éventuel échange d'informations*. Une réécriture du décret du 4 janvier 2006 a même été envisagée.

ii. La politique de confidentialité et de sécurité

Le candidat doit définir et mettre en œuvre une politique de confidentialité et de sécurité, destinée notamment à assurer le respect des exigences de confidentialité et de sécurité prévues par les articles L 1110-4 et L 1111-7 du code de la santé publique, la protection contre les accès non autorisés ainsi que la pérennité des données, et dont la description doit être jointe au dossier d'agrément dans les conditions fixées par l'article R 1111-14 du décret.

Cette condition, lourde de conséquences par ce que constituant le but réel de toute la procédure fait l'objet d'un article plus détaillé du décret : l'article R 1111-14 et consiste en un document spécial qui vient en « *appui de la demande d'agrément*[990] ».

Aux termes du décret relatif à l'hébergement, la politique de confidentialité et de sécurité doit apporter des précisions concernant quatre domaines : le respect des droits des

[989] Comité d'agrément. *Premier rapport d'activité du Comité d'agrément des hébergeurs : 2006-2011 sous la présidence du Dr Philippe BICLET*. Rapport publié par l'Asip santé le 7 Septembre 2011. p. 27. http://esante.gouv.fr/sites/default/files/Rapport_CAH_4.08.11_VF.pdf. Consulté le 28 mai 2014.

[990] Article R 1111-14, alinéa 1. Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel.

personnes concernées par les données hébergées, la sécurité de l'accès aux informations, la pérennité des données hébergées et l'organisation et la procédure de contrôle interne.

S'agissant du respect des droits des personnes concernées par les données hébergées, la présentation doit comporter des précisions sur :

«- les modalités permettant de s'assurer de l'existence du consentement de l'intéressé à l'hébergement des données le concernant ;

- les modalités retenues pour que l'accès aux données de santé à caractère personnel et la transmission éventuelle n'aient lieu qu'avec l'accord des personnes concernées et par les personnes désignées par elles ;

- les conditions dans lesquelles sont présentées et prises en compte les éventuelles demandes de rectification des données de santé à caractère personnel hébergées ;

- les moyens mis en œuvre pour assurer le respect des dispositions de l'article L 1111-7 relatives à l'accès des personnes à leurs informations de santé, notamment en termes de délais et de modalités de consultation;

- les procédures de signalement des incidents graves, dont l'altération des données ou la divulgation non autorisée des données personnelles de santé ;

- la fourniture à la personne concernée par les données hébergées, à sa demande, de l'historique des accès aux données et des consultations ainsi que du contenu des informations consultées et des traitements éventuellement opérés.»

Ces dispositions tendent à promouvoir le respect de la volonté de l'individu dont les données sont hébergées et son droit à l'information à travers les mesures techniques prises par le candidat dans ce sens. L'accent mis sur le respect de la volonté de l'individu dans l'hébergement de ses données par un professionnel informatique donne un peu plus de valeur à l'avis du patient dans ses relations avec ce dernier par rapport à l'importance accordée à sa volonté dans les accès des professionnels de santé à son dossier. Cela paraît logique en ce sens que le professionnel de santé a plus d'influence sur la vie du patient que le professionnel informatique qui ne fait que conserver ses informations de santé.

Mais, ce serait illusoire de croire que dans cette relation la volonté du patient est réellement prise en compte et qu'il est effectivement éclairé sur tous les traitements dont ses informations hébergées feront l'objet. En effet, si, en général, le patient donne son consentement aux professionnels de santé simplement par confiance ou par sentiment d'impuissance, il donne plus sûrement, son accord à l'hébergement de ses données par pur formalisme et comprend

encore moins les informations que lui délivre l'hébergeur compte tenu du problème récurrent de l'absence de culture informatique de la majeure partie de la population.

En ce qui concerne la sécurité de l'accès aux informations, le document doit comporter :
«- *les dispositions prises pour garantir la sécurité des accès et des transmissions de données de santé à caractère personnel vis-à-vis des établissements ou des professionnels de santé à l'origine du dépôt et de personnes concernées par ces données ;*
- *les mesures prises en matière de contrôle des droits d'accès et de traçabilité des accès et de traitement ;*
- *les conditions de vérification du contenu des traces des accès et de traitement afin de détecter les tentatives d'effraction ou d'accès non autorisés ;*
- *les modalités de vérification du registre des personnes habilitées à accéder aux données hébergées tenant compte des éventuelles mises à jour ;*
- *les procédés techniques retenus en matière d'identification et d'authentification ; en ce qui concerne les professionnels de santé, ces procédés techniques doivent avoir été agréés par le groupement d'intérêt public mentionné à l'article R 161-54 du code de la sécurité sociale.* »
La CNIL préconise l'adoption de mesures de sécurité physique et logique qui doivent être adaptées en fonction de l'utilisation qui est faite du système d'information, de sa configuration, de l'existence ou non d'une connexion à Internet. Pour sécuriser les données, la Commission propose l'utilisation, dans la mesure du possible, du codage des données nominatives et le chiffrement de tout ou partie des données et de la communication (exemple : chiffrement SSL avec une clé de 128 bits) dans le cadre de la réglementation française et européenne. Concernant leur intégrité, il faut mettre en place des protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises. Pour la connexion à un réseau Internet, il faudra prévoir des mesures de sécurité particulières comme la séparation physique des réseaux, la mise en place d'un firewall ou de barrières de protection logicielles. La mise en place d'un dispositif permettant l'indication systématique aux utilisateurs lors de la connexion, sous forme d'un affichage sur l'écran, des date et heure de la dernière connexion sous les mêmes codes utilisateur et mot de passe, apparaît être un moyen intéressant pour permettre au patient de prendre connaissance d'une éventuelle intrusion. Toutes ces mesures viennent en complément de l'utilisation de la carte de professionnel de santé (CPS) pour les professionnels de santé et de l'identifiant national de santé (INS) pour les patients.

Le décret *« confidentialité »* du 15 mai 2007 a posé le principe de l'obligation d'utilisation de la carte de professionnel de santé ou d'un dispositif équivalent agréé. Conformément à l'article 2 de la convention constitutive approuvée par arrêté ministériel du 28 novembre 2009 modifié, l'Asip santé est l'autorité de certification qui délivre les certificats électroniques à tous les acteurs du domaine de la santé pour leur permettre d'utiliser une carte CPS agréée[991]. L'Asip santé compte parmi ses missions prévues par l'article 2 de ladite convention : *« la certification, la production, la gestion et le déploiement de la carte de professionnel de santé et, plus généralement, des dispositifs assurant la fonction d'identification, d'authentification, de signature et de chiffrement permettant aux professionnels de santé de faire reconnaître, dans les conditions de sécurité de confidentialité requises, leur identité et leurs qualifications professionnelles dans les systèmes d'information et d'échanges électroniques qu'ils utilisent* ».

L'identifiant national de santé (INS) demeure actuellement le moyen légal d'authentification du patient. En effet, l'article L 1111-8-1 du code de la santé publique dispose : *« 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. (...). 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.»*

Mais ces dispositions ne peuvent être efficaces que si l'hébergeur met en place des solutions logicielles qui permettent d'organiser des accès différenciés aux informations contenues dans le dossier médical selon le statut de chaque intervenant. Il incombe donc à l'hébergeur de permettre d'horodater les accès et les mises à jour et interdire des modifications par des personnes non habilitées.

Relativement à la pérennité des données hébergées, le candidat doit présenter :

«- les procédés visant à assurer, au moment du transfert des données vers l'hébergeur, la réception sécurisée des données et l'intégrité de celles-ci, leur prise en compte dans le système d'information de l'hébergeur et le suivi de cette prise en charge ;

- les modalités de prise en compte et d'enrichissement tout au long de la durée de l'hébergement, de l'ensemble des informations concernant les données depuis la création,

[991] Asip santé. *Les certificats CPS*. 12 juin 2012. Disponible sur: http://esante.gouv.fr/services/espace-cps/les-certificats-cps. Consulté le 22 octobre 2013.

telles que les données permettant de les identifier et de les décrire, de les gérer, de déterminer leurs propriétés techniques et d'en assurer la traçabilité ;

- les modalités de surveillance des supports en vue d'anticiper les changements technologiques et, le cas échéant, d'opérer des migrations de supports dans des conditions en garantissant la traçabilité ;

- les procédures liées à la réplication des données sur les différents supports informatiques en des lieux distincts ;

- les conditions de mise en œuvre de l'alerte concernant les formats d'encodage de données, destiné à avertir la personne à l'origine du dépôt en cas d'obsolescence de ce format et, éventuellement, la procédure visant à réaliser, avec l'autorisation de la personne à l'origine du dépôt, des migrations de formats des données, si ces derniers ne permettent plus d'assurer la lisibilité des informations et à assurer la traçabilité de ces migrations. »

L'esprit de cette condition est la volonté du gouvernement d'organiser le dépôt et la conservation des données de santé dans des conditions de nature à leur garantir leur pérennité et leur confidentialité, de les mettre à la disposition des personnes autorisées selon des modalités définies par contrat, et de les restituer à la fin dans toute leur intégrité initiale. Ainsi, l'hébergeur agréé du DMP conserve-t-il les données sous forme chiffrée sur un serveur national.

S'agissant, enfin, de l'organisation et des procédures de contrôle interne en vue d'assurer la sécurité des traitements et des données, la politique du candidat à l'hébergement devra prévoir :

«- la désignation d'un responsable sécurité et d'un responsable qualité ;

- la définition des missions, des pouvoirs et des obligations des personnels de l'hébergeur et de ses éventuels sous-traitants, habilités à traiter les données de santé à caractère personnel ;

- les spécifications techniques des logiciels et des mécanismes de sécurité propre à garantir la confidentialité des transmissions, notamment en ce qui concerne le mode de chiffrement des flux d'information ;

- les modalités retenues pour l'évaluation périodique de ces risques et l'audit des mesures de protection mise en place afin de garantir la sécurité des données et en vue d'apporter des modifications nécessaires en cas de détection de défaillances ;

- les dispositifs de simulation régulière de défaut de fonctionnement pour vérifier l'efficacité des mécanismes destinés à garantir la continuité des services ;

- les moyens mis en œuvre pour sensibiliser et former le personnel aux mesures de protection mises en place et à leurs obligations en matière de confidentialité et de respect du secret professionnel ;

- les conditions de mise en œuvre de la sécurité physique des sites informatiques, des mesures de protection de l'infrastructure technique, notamment en termes de sécurité des réseaux, des serveurs et des postes de travail ;

- les dispositions prises en ce qui concerne l'exploitation de l'infrastructure technique ;

- les conditions de mise en œuvre du plan de secours informatique comportant notamment les dispositions prises pour informer du déclenchement de ce plan les personnes physiques ou morales à l'origine du dépôt des données de santé à caractère personnel ainsi que les dispositions prises pour la reprise des activités. »

Pour que le contrôle soit efficace, un audit régulier paraît être le moyen adéquat. Dans sa délibération[992] du 6 octobre 2011, la CNIL fixe les exigences auxquelles doit répondre une procédure d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel. Elles sont regroupées dans un référentiel[993] d'évaluation des procédures d'audit établi par la Commission. Les auditeurs techniques et juridiques doivent avoir un certain niveau de formation dans leur domaine respectif et de l'expérience dans le domaine informatique et libertés. Ils doivent être habilités à effectuer l'audit portant sur des données pour lesquelles cette condition est requise par la réglementation française et communautaire en vigueur. L'audit des mesures de sécurité permet d'évaluer plusieurs aspects de la politique de confidentialité et de sécurité mise en place par un hébergeur. Il permet d'évaluer la politique d'habilitation appliquée à chaque personne ayant un accès légitime aux données. Des contrôles pertinents sur la durée de conservation et la condition d'archivage des données sont ainsi faits. C'est une procédure qui permet d'analyser et d'évaluer la démarche mise en œuvre par les responsables du traitement pour assurer la confidentialité, l'intégrité et la disponibilité des informations, notamment l'identification des principaux risques encourus par les libertés

[992] CNIL. Délibération n° 2011-316 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de procédure d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel. JORF n° 0255 du 3 novembre 2011. NOR: CNIA1100014X.

[993] *«Un référentiel est une liste des exigences ou des spécifications à laquelle le produit ou la procédure doit répondre afin d'obtenir le label. Ces exigences correspondent aux critères permettant d'évaluer la conformité du produit ou de la procédure aux dispositions de la loi informatique et libertés. » (Rapport d'activité annuelle de la CNIL de 2011)*

et la vie privée des personnes dont les données sont traitées en cas d'atteinte à la sécurité des systèmes d'information. Les auditeurs évaluent la pertinence et la conformité de mesures de sécurité mises en œuvre pour faire face aux risques identifiés et estimés et pour gérer les incidents de sécurité. L'audit est l'occasion de vérifier que les titulaires des données disposent bien d'un droit d'accès, d'un droit de rectification et le cas échéant, d'un droit d'opposition, qu'ils peuvent exercer de manière effective, dans des délais raisonnables et qu'ils ont été correctement informés de ces droits. Enfin l'audit permet de savoir si les hébergeurs ont pris les dispositions qui s'imposent, conformément à la loi informatique et libertés aux traitements des données sensibles.

Finalement, les conditions de l'agrément ont pour but de rechercher chez tout hébergeur un système de management de la sécurité de l'information qui assure continuellement l'évaluation objective des risques portant sur la sécurité des données et la mise en œuvre de solutions contractuelles, organisationnelles ou techniques pour faire face aux éventuels risques. La contravention à ces conditions a conduit la CNIL à prononcer quelques sanctions envers des hébergeurs. Un avertissement a été donné (le 18 novembre 2011, non rendu public[994]) à un hébergeur de données de santé au sujet d'une déclaration mensongère contenue dans son dossier de demande d'agrément. En l'espèce, en 2009, une société avait déclaré dans son dossier de candidature qu'elle chiffre l'ensemble des données médicales hébergées, par un procédé dit de *"chiffrage fort"*. Cela constituait l'un des atouts de cette candidature et la société avait donc obtenu l'agrément du ministère de la santé au début de l'année 2010. Mais, au début de l'année 2011 la CNIL a réalisé un contrôle sur place et a constaté que les données médicales n'étaient pas chiffrées et qu'elles étaient accessibles aux administrateurs informatiques de la société et non pas exclusivement au personnel de santé habilité. La société avait uniquement protégé certaines des données de santé par un codage créé en interne. La formation contentieuse de la Commission informatique et liberté a considéré que le traitement de données personnelles était contraire à l'article 6-1° de la loi informatique et libertés qui prévoit que les données doivent être traitées de manière licite elle a estimé que la société n'avait pas respecté le code de la santé publique. En prétendant chiffrer toutes les données médicales, ce qui s'était révélé inexact et mensonger, et en n'informant pas le ministre de la

[994] Voir les sanctions de la CNIL de 2011. www.cnil.fr.

santé d'un tel changement comme l'imposait le code de la santé publique, la société n'avait pas respecté la loi et effectuait donc des traitements de données de manière illicite[995].

La présidente de la CNIL a adopté le 25 septembre 2013 une mise en demeure à l'encontre du centre hospitalier de Saint-Malo pour non-respect de la politique de confidentialité et de sécurité. A la suite d'informations dont elle a eu connaissance, la CNIL a, au mois de juin 2013, effectué un contrôle au centre hospitalier de Saint-Malo. Ce contrôle a permis de relever que le prestataire mandaté par l'hôpital a pu accéder, avec le concours de l'établissement, aux dossiers médicaux de 950 patients (informatisées ou en version papier), méconnaissant ainsi le code de la santé publique et la loi informatique et libertés qui obligent les responsables des traitements à préserver la sécurité des données et empêcher que des personnes non autorisées puissent y avoir accès[996]. Notons que le centre hospitalier ayant mis en place plusieurs mesures[997] pour se conformer à la législation, aucune suite n'a été donnée à cette mise en demeure désormais clôturée sans préjudice de vérifications ultérieures effectuées par la CNIL. La recommandation de la CNIL invite le centre hospitalier à étudier « *la possibilité de désigner un correspondant informatique et libertés, qui constitue un moyen efficace de veiller à la bonne application de la loi, tout en exonérant l'organisme qui s'en est doté de toute obligation de déclaration de ses fichiers*[998]. »

D'abord un avertissement adressé à un hébergeur dont l'identité n'est pas révélée, une décision non rendue publique et ensuite une mise en demeure qui est suspendue à la suite d'une déclaration de mise en conformité de l'organisme incriminé. Si ces sanctions montrent l'importance du contrôle qu'exerce la Commission pour s'assurer de l'adéquation entre la déclaration faite dans le dossier de demande d'agrément et la réalité de la conservation des

---

[995] CNIL. *La CNIL sanctionne la déclaration mensongère d'un hébergeur de données de santé*. 9 janvier 2012. www.cnil.fr.Consulté le 11 octobre 2013.

[996] CNIL. *Décision n° 2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo*. (n° MDM 131040). http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/D2013037_MED_CH_ST_MALO.pdf. Consulté le 22 octobre 2013

[997] *« la suppression de l'accès informatiques par le prestataire aux dossiers médicaux ; la formalisation d'une politique stricte de sécurité des systèmes d'information ; la suppression de l'accès par le prestataire aux dossiers médicaux des patients (informatisé ou en version papier), qui demeure sous la seule autorité du médecin responsable de la formation médicale de l'établissement, conformément au texte de loi. »* CNIL. *Clôture de la mise en demeure adoptée à l'encontre du centre hospitalier de Saint-Malo*. 17 octobre 2013. www.cnil.fr. Consulté le 22 octobre 2013.

[998]CNIL. *Courrier de clôture de la mise en demeure du centre hospitalier Saint-Malo*. Recommandation AR n° 2C054 549 79070. Paris, 17 octobre 2013. Http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/courrier/courrier_de_cloture_MED_CH_ST-MALO.pdf. Consulté le 22 octobre 2013

données, leur souplesse donne une impression d'inachevé. Ces premières décisions ne nous semblent pas suffisamment efficaces pour amener les hébergeurs à offrir une meilleure qualité de prestations. Même si l'objectif initial de ces sanctions n'est pas de faire des exemples, il nous paraîtrait juste de prendre des décisions plus contraignantes compte tenu de la sensibilité des données en jeu. Cela nous semblerait participer davantage au processus normal de la démarche d'amélioration continue de la qualité et de la sécurité qu'impose l'agrément en suscitant une prise de conscience des hébergeurs qui seraient tentés de contrevenir aux règles. Toutefois, cette relative légèreté des décisions est jugée mesurée par certains juristes à partir d'un double constat: premièrement, « *les données de santé ne sont aujourd'hui chiffrées ni par les logiciels les plus utilisés du marché, ni par les cartes CPS ou dispositifs équivalents, et ne sont donc, en conséquence, pas confiées chiffrées aux hébergeurs contraints de multiplier les mesure de sécurité pour pallier à cette carence; deuxièmement, l'hébergeur avait, cependant, pris soin de mettre en place un codage pour les données les plus sensibles. En outre, il est probable que la CNIL n'ait pas voulu se montrer trop sévère à l'égard d'un hébergeur agréé, quand de nombreux prestataires exercent aujourd'hui de telles activités en dehors de tout agrément*[999] »[1000]. De plus, en relativisant, il faut voir dans ces décisions, une étape vers des sanctions plus sévères en cas de persistance dans l'infraction, de récidive ou d'infraction plus grave. A la suite d'un avertissement, la CNIL a compétence pour prononcer une sanction pécuniaire allant jusqu'à « *300000 euros ou, s'agissant d'une entreprise, 5% du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 3000000 euros*[1001] », si le mis en cause ne remédie pas à la situation.

Ces décisions de la Commission informatique et libertés vis-à-vis des hébergeurs de données de santé soulèvent la problématique de la responsabilité des hébergeurs de données de santé et notamment, ceux qui hébergent les dossiers médicaux.

---

[999] Seulement 64 hébergeurs ont été agréés au 18 mars 2014. Asip santé. *Hébergeurs agréés*. Mise à jour au 18 mars 2014. http://esante.gouv.fr/en/node/417. Consulté le 23 avril 2014.

[1000] BRAC DE PERRIERE, Marguérite. DELANNOY, Tiphaine. *Obligation de chiffrement et hébergeur de données de santé* in juristendances informatique et télécoms. n° 120. Février 2012. http://www.alain-bensoussan.com/wp-content/uploads/225044221.pdf. Consulté le 23 avril 2014.

[1001] Article 47 de la loi informatique et libertés.

2. La responsabilité des hébergeurs

La responsabilité des hébergeurs de données de santé connaît un régime juridique spécial du fait de la spécificité des renseignements en jeu. Il est dérogatoire du régime de droit commun de la responsabilité des fournisseurs d'accès et caractérisé par la multiplicité de sanctions légales et réglementaires pouvant être associées à la même infraction.

a. La responsabilité des hébergeurs de données de santé, un régime dérogatoire

Jusqu'en 2000, le régime juridique de la responsabilité des intermédiaires techniques était régi par le droit commun. Le 1er août 2000, la loi modifiant la loi du 30 septembre 1986 relative à la liberté de communication a permis au législateur de créer un régime juridique spécial pour les personnes assurant le stockage de contenus sur des serveurs spécialement dédiés à cet effet et diffusés par l'intermédiaire de sites Internet. Ainsi, a été intégré l'article 43-8 qui dispose : *« les personnes physiques ou morales qui assurent, à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public des signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services, ne sont pénalement ou civilement responsable du fait du contenu de ces services que : si ayant été saisies par une autorité judiciaire, elles n'ont pas agi promptement pour empêcher l'accès à ce contenu*[1002] ». Cet acte consacrait ainsi la quasi immunité des prestataires d'hébergement ayant respecté les conditions fixées par la loi dont la souplesse était justifiée par le caractère exclusivement technique de la prestation. Leur responsabilité s'engageait seulement lorsqu'étant saisis par l'autorité judiciaire ils n'auraient pas agi promptement pour empêcher

[1002] Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication. JORF n° 7 du 2 août 2000. p. 11903. Texte n° 1. NOR: MCCX9800149L.

Le Conseil constitutionnel a déclaré contraire à la constitution la dernière proposition de cette disposition au motif que «*le législateur a subordonné la mise en œuvre de la responsabilité pénale des hébergeurs, d'une part, à leur saisine par un tiers estimant que le contenu hébergé est illicite ou lui cause un préjudice, d'autre part, à ce que, à la suite de cette saisine, ils n'aient pas procédé aux diligences appropriées ; qu'en omettant de préciser les conditions de forme d'une telle saisine et ne déterminant pas les caractéristiques essentielles du comportement fautif de nature à engager, le cas échéant, la responsabilité pénale des intéressés, le législateur a méconnu la compétence qu'il tient de l'article 34 de la constitution*; ». Conseil constitutionnel. Décision n° 2000-433 DC du 27 juillet 2000. JORF n° 177 du 2 août 2000. p. 11922, texte n° 2. NOR: CSCL0004281S.

l'accès à un contenu. Mais cette disposition a suscité des controverses[1003] et à la faveur de la transposition de la directive européenne e-commerce de 2000, la loi pour la confiance dans l'économie numérique de 2004 a redéfini les termes du principe de l'irresponsabilité des hébergeurs. Elle prévoit en son article 6, I -2 que « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.»* Le degré de connaissance nécessaire pour entraîner la responsabilité du prestataire de services n'est pas clairement défini par ces dispositions alors qu'il est déterminant pour l'appréciation de la faute de l'hébergeur. C'est une situation éprouvante pour cet intermédiaire dans la mesure où dans certaines circonstances, la réponse est évidente lorsque le caractère illicite des données est tout aussi évident. Mais dans d'autres cas[1004], l'établissement de la connaissance de cette infraction paraît plus complexe. Pour avoir une bonne appréciation de la situation, l'intermédiaire doit éviter de se précipiter en cas de dénonciation, et de prendre des décisions hâtives. Sur la question, nous partageons le point de vue du professeur TRUDEL qui estime que « *l'attitude appropriée pour l'intermédiaire est d'obtenir une confirmation d'un tiers, tel un expert neutre et d'agir sur la foi d'une telle évaluation. Car il apparaît évident que la connaissance de fait ne commence qu'à compter du moment où la plainte à l'égard d'un document est suffisamment documentée pour écarter les doutes raisonnables quant à son sérieux[1005]*. » Le juge ne pourra donc établir la connaissance

[1003] AMBLARD, Philippe. AUROUX, Jean-Baptiste. Lamy droit des médias et de la communication. Partie 4. Titre 2. Etudes 476-6 et 476-7. *L'hébergeur en application de la loi du 1er Août 2000/ L'hébergeur en application de la LCEN du 21 juin 2004* . http://lamyline.lamy.fr. Consulté le 1er novembre 2013.

[1004] « *Par exemple, l'hébergeur reçoit une notification à l'effet que tel site qu'il héberge comporte des documents qui portent atteinte au droit à l'image d'une personne. Or, on sait qu'il y a plusieurs situations ou la diffusion de l'image d'une personne est tout à fait licite. S'il obtempère et retire le document, il s'érige en juge mais en juge n'ayant pas agi moyennant l'élémentaire obligation d'entendre les prétentions de toutes les parties en cause. S'il ne fait rien, l'intermédiaire s'expose à voir sa responsabilité engagée et à devoir répondre lors d'une poursuite de la part de la victime*. » TRUDEL, Pierre. *La responsabilité civile sur Internet selon la loi concernant le cadre juridique des technologies de l'information in* Développements récents en droit de l'Internet. p. 126.

[1005] TRUDEL, Pierre. *La responsabilité civile sur Internet selon la loi concernant le cadre juridique des technologies de l'information* in Développements récents en droit de l'Internet. p. 127.

de l'illicéité des données par l'hébergeur que si à la fin de ses investigations, ce dernier n'a pas pris les mesures nécessaires pour mettre fin à la diffusion des données incriminées.

Si le régime juridique de la responsabilité des hébergeurs a fait l'objet de beaucoup de débats notamment à l'occasion de la transposition de la directive européenne[1006], devant les tribunaux français[1007] et auprès de la cour de justice de l'Union[1008], les conséquences de la définition[1009] que l'on retire de l'hébergeur de façon générale, ne correspond pas exactement à celles des hébergeurs de données de santé à caractère personnel. En effet, le cadre prescrit par la loi pour la confiance dans l'économie numérique présente l'hébergeur comme celui qui assure le stockage plus ou moins permanent des données et qui pourrait en avoir connaissance et même les modifier. L'hébergeur n'est pas responsable a priori du contenu des services qu'il garde et n'est pas tenu à une obligation de surveillance. Il est tenu d'intervenir a posteriori pour faire cesser la diffusion d'un contenu illicite ou préjudiciable. Les données de santé à caractère personnel ont ceci de particulier que les hébergeurs ne doivent, sous aucun prétexte, en prendre connaissance. Leur rôle se limite donc à un simple stockage dans le but de les rendre " saines et sauves" à la fin du contrat. C'est le fondement du régime juridique de la responsabilité des hébergeurs de données de santé à caractère personnel en ce sens qu'ils sont tenus de conserver les informations dans les meilleures conditions assurant la protection de leur intégrité. En outre, les hébergeurs régis par la loi pour la confiance dans l'économie numérique offrent des services de communication en ligne, au public alors que les données de santé ne doivent être consultées que par les déposants ou les personnes concernées. Elles ne

---

[1006] THOUMYRE, Lionel. *Les hébergeurs en ombres chinoises. Une tentative d'éclaircissements sur les incertitudes de la loi pour la confiance dans l'économie numérique*. Revu Lamy droit de l'immatériel. Mai 2005.n° 5. pp.60 - 61.

[1007] Cass. civ. 1ère, 17 février 2011. 3 arrêts: n° 164, 165, 166. www.courdecassation.fr .
Cour d'Appel Paris. 14 Avril 2010. Omar S. Fred T et a. contre Société Daily Motion. RLDI 2010/62, n°2034. p. 47. Note Har-douin. Tribunal de grande instance de Brest, Chambre correctionnelle, jugement du 11 juin 2013. Http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3842. Consulté le 1er novembre 2013

[1008] CJUE. arrêts du 23 mars 2010, Google France et Google, C-236/08 à C-238/08. ou CJUE, grande chambre. Arrêt du 12 juillet 2011, l'Oréal SA contre eBay international AG, C-324/09. www.eur-lex.europa.ue. Consulté le 1er novembre 2013

Google bénéficie du régime de responsabilité allégée dès lors que l'apparition des liens commerciaux dirige vers des articles portants atteinte à la vie privée d'un acteur. Cour d'appel de Paris, *Google Ireland, Google France / Olivier Martinez.* 11 décembre 2013. LEGALNEWS. Mardi 21 janvier 2014. www.legalnews.fr. Consulté le 1er novembre 2013

[1009] Une définition qui souffre en réalité de plusieurs controverses. Voir à ce sujet : SCHAFFNER, M. et SROUSSI G. *Responsabilité des hébergeurs : une responsabilité sans définition fixe*. Revu Lamy Droit de l'immatériel 2010. 1er octobre 2010., n° 64. p. 33 - 38.

sont "surtout pas" ouvertes au grand public. Contrairement aux autres hébergeurs, les hébergeurs des données du DMP doivent garantir leur bonne conservation et leur communication immédiate afin d'éviter des retards de transmission préjudiciables au patient. Il pèse donc sur ces hébergeurs une obligation de surveillance qui combine à la fois, les caractéristiques des obligations de moyen et de résultat. Enfin, le régime juridique de la responsabilité des hébergeurs tel que prescrit par la législation actuelle met en cause le prestataire de services pour un contenu illicite dont il a le contrôle ou la connaissance. Mais dans le cas de la gestion des données de santé, ce qui pourrait engager la responsabilité d'un hébergeur, ce serait une intrusion ou une divulgation non autorisée du fait de la négligence ou de la complicité de ce dernier. Le débat ne porte donc pas sur le contenu illicite des données stockées- leur licéité ne faisant l'ombre d'aucun doute - mais sur les mesures prises par ces techniciens pour les protéger. C'est pour marquer leur attachement au respect de cette obligation que les autorités publiques françaises ont élaboré des sanctions de différents ordres à l'encontre de tout hébergeur qui néglige de garantir la sécurité des données médicales personnelles.

b. La responsabilité des hébergeurs, un régime multidimensionnel

Le droit applicable à cette responsabilité tire, d'une part, son origine du contrat d'hébergement ; ce qui implique l'application du régime juridique de droit commun de la responsabilité contractuelle. L'hébergeur engage sa responsabilité en cas de mauvaise exécution ou d'inexécution totale ou partielle des obligations nées du contrat conformément à l'article 1147[1010] du Code civil. D'autre part, la source du droit applicable est le cadre général des sanctions aux atteintes aux droits de la personne à l'occasion du traitement automatisé des données personnelles régies par les articles 226-16 à 226-24 du code pénal. Ces sanctions sont issues de la loi informatique et libertés après la modification qu'elle a faite par 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. Indirectement, la protection pénale des données

[1010] « *le débiteur est condamné, s'il y a lieu, au paiement de dommages et intérêts soit à raison de l'inexécution d'une obligation, soit à raison du retard dans l'exécution, toutes les fois qu'il ne justifie pas que l'inexécution provient d'une cause étrangère qui ne peut lui être imputée, encore qu'il n'y ait aucune mauvaise foi de sa part.* »

personnelles de santé est également assurée par les sanctions aux atteintes aux systèmes de traitement automatisé des données régies par les articles 323-1 à 323-7 du code pénal.
Le type de responsabilité engagée diffère selon que les manquements reprochés à l'hébergeur portent sur les clauses du contrat d'hébergement ou sur les conditions de l'agrément même si, en définitive, tous ces éléments se rejoignent dans les mesures prises par celui-ci pour garantir la confidentialité et la sécurité des données depuis leur dépôt, leur conservation jusqu'à leur restitution.

Le contrat d'hébergement dont le contenu est dicté par l'article R 1111-13 du décret de 2006 relatif à l'hébergement des données de santé à caractère personnel oblige le prestataire technique à se conformer aux dispositions de l'article L 1111-8 du code de la santé publique qui fixent le cadre de cette responsabilité. Seuls peuvent accéder aux données ayant fait l'objet d'un hébergement les personnes que celles-ci concernent et les professionnels de santé ou établissements de santé qui les prennent en charge et qui sont désignés par les personnes concernées, selon des modalités fixées dans le contrat, dans le respect des dispositions des articles L 1110-4 et L 1111-7 du code de la santé publique. Les hébergeurs tiennent les données de santé à caractère personnel qui ont été déposées auprès d'eux à la disposition de ceux qui les leur ont confiées. Ils ne peuvent les utiliser à d'autres fins. Ils ne peuvent les transmettre à d'autres personnes que les professionnels de santé ou établissement de santé désignée dans le contrat. Lorsqu'il est mis fin à l'hébergement, l'hébergeur restitue les données qui lui ont été confiées, sans en garder de copie[1011], au professionnel, à l'établissement ou à la personne concernée ayant contracté avec lui. La délibération[1012] de la CNIL de 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel préconisait qu'à la fin de la collaboration, l'hébergeur s'engage à fournir au professionnel de santé les moyens nécessaires pour lui permettre de continuer à gérer sur l'informatique ses dossiers médicaux ou d'effacer les informations nominatives enregistrées avant restitution du matériel informatique à l'organisme. Les hébergeurs de données de santé à caractère personnel et les personnes placées sous leur autorité qui ont accès aux données déposées sont astreintes

[1011] *« le fait, hors les cas prévus par la loi, de mettre ou conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement (...) sont relatives à la santé ou à l'orientation ou identité sexuelle de celle-ci est puni de cinq ans d'emprisonnement et de 300 000 € d'amende »* Article 226-19 du code pénal.

[1012] CNIL. Délibération n° 97-008 du 4 février 1997 portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel. http://www.cnil.fr/documentation/deliberations/deliberation/delib/23/. Consulté le 28 mai 2014.

au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal. Il pèse alors, sur les hébergeurs, une obligation de contrôle et de vérification de l'identité et de la fonction de chaque intervenant afin de prévenir la violation du secret professionnel. Les hébergeurs de données de santé à caractère personnel ou qui proposent cette prestation d'hébergement sont soumis, dans les conditions prévues aux articles L 1421-2 et L 1421-3 au contrôle de l'inspection générale des affaires sociales et des agents mentionnés aux articles L 1421-1 et L 1435-7. Les agents chargés du contrôle peuvent être assistés par des experts désignés par le ministre chargé de la santé. Ainsi, compte tenu de la sensibilité des informations de santé, les hébergeurs de données de santé à caractère personnel font-il l'objet d'un contrôle plus strict malgré la relative passivité de leur activité. Ils sont tenus par leurs engagements non seulement vis-à-vis des clients (professionnels de santé ou établissements de santé ou les personnes titulaires des données) mais également vis-à-vis des personnes dont les données sont stockées même si elles ne sont pas déposantes de celles-ci et la CNIL également.

La mauvaise exécution ou l'inexécution des obligations consiste, à permettre un accès non autorisé, volontairement ou non. En application du droit commun de la responsabilité, la responsabilité civile contractuelle du prestataire de services doit être engagée vis-à-vis du déposant cocontractant (professionnels ou établissements de santé ou personnes concernées par les données). Mais cette responsabilité est délictuelle pour le titulaire des données non déposant qui devra démontrer l'existence d'un dommage et son lien avec la divulgation ou tout autre manquement (transfert de données sans son consentement par exemple) en vue d'obtenir la réparation du préjudice moral sur le fondement de l'article 1382 du Code civil. La responsabilité peut être engagée pour l'hébergeur qui ne fournit pas des prestations présentant des niveaux de sécurité spécifiques aux données de santé qu'il a présentées à la CNIL lors des formalités préalables pour fausse déclaration. Dans son 21ème rapport d'activité[1013] pour l'année 2000, la CNIL recommandait que le contrat passé avec un hébergeur tiers comporte des clauses prévoyant les nécessaires mesures destinées à assurer la sécurité des données ainsi que leur seul accès et utilisation par des personnes habilitées à en connaître. Ces mesures doivent être portées à la connaissance de la CNIL. Ces clauses sont aussi valorisantes pour les hébergeurs en ce sens que ces mesures peuvent constituer un critère prépondérant de choix

[1013] CNIL. 21e rapport d'activité 2000. P. 149. www.ladocumentationfrançaise.fr.

pour les potentiels contractants publics conformément aux règles du code des marchés publics édictées par le décret[1014] n° 2004-15 du 7 janvier 2004 portant code des marchés publics.

Le non-respect des conditions d'octroi de l'agrément est sanctionné par l'article L 1111-8, alinéa 6 du code de la santé publique par un retrait de l'agrément à l'hébergeur. « *L'agrément peut être retiré[1015], dans les conditions prévues par l'article 24 de la loi[1016] n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.* » La procédure est contradictoire. Le ministère chargé de la santé, après avoir prévenu l'hébergeur en cause, lui accorde deux mois pour se défendre avant de procéder au retrait s'il n'a pas été convaincu par les arguments présentés par celui-ci. Une suspension d'activité peut être décidée « *à titre conservatoire, en cas de divulgation non autorisée de données de santé à caractère personnel ou de manquements graves de l'hébergeur à ses obligations mettant notamment en cause l'intégrité, la sécurité et la pérennité des données hébergées[1017] ».*

Force est de constater que cette sanction se fait non pas dans les conditions prévues par le Code civil mais dans celles prévues par des règles de droit administratif avec, toutefois, la particularité du contradictoire avant la prise de la décision. Habituellement, l'administration, usant de ses prérogatives de puissance publique informe le mis en cause de sa décision déjà prise et ensuite, de la possibilité d'un recours. En effet, l'agrément ayant été octroyé par une autorité administrative, le code de la santé publique privilégie les règles applicables dans les relations entre l'administration et les particuliers. Cette solution étant valable dans les rapports entre les autorités publiques et l'hébergeur, le cocontractant du prestataire (l'établissement ou le professionnel de santé) ou la personne concernée par les données stockées s'estimant lésé pourra retenir la solution de l'action en responsabilité pénale.

L'article L 1115-1 du code de la santé publique ajoutent une infraction et complète cette sanction par une peine pénale: « *la prestation d'hébergement de données de santé à caractère personnel recueillies auprès de professionnels ou d'établissements de santé ou directement*

[1014] JORF n° 6 du 8 janvier 2004. p. 37003. Texte n°2. NOR: ECOZ0300023D.

[1015] Si un hébergeur titulaire d'un marché de son agrément par retrait ou non-renouvellement en cours d'exécution d'un marché, le contrat devra être résilié.

[1016] Loi n° 2000-321 du 12 avril 2000 *relative aux droits des citoyens dans leurs relations avec les administrations.* JORF n° 88 du 13 avril 2000 p. 5646. Texte n° 1. NOR: FPPX9800029L.

[1017] Article R 1111-16 du décret hébergement de 2006.

auprès des personnes qu'elles concernent sans être titulaire de l'agrément prévu par l'article L 1111-8 ou de traitement de ces données sans respecter les conditions de l'agrément obtenu est punie de trois ans d'emprisonnement et de 45 000 € d'amende ». Les personnes morales peuvent être déclarées responsables de l'ensemble de ces infractions, ajoute l'article L 1115-2. Il s'ensuit donc qu'un prestataire d'hébergement de données de santé à caractère personnel peut engager sa responsabilité pénale s'il offre ce service sans agrément ou si même étant agréé, il exerce dans des conditions non conformes.

L'hébergeur verra sa responsabilité pénale engagée s'il détourne les informations de leur finalité initiale en les employant à d'autres fins notamment, l'exploitation commerciale[1018]. Cette situation est punie de cinq ans d'emprisonnement et de 300 000 € d'amende aux termes de l'article 226-21 du code pénal. Au regard de l'article 226-18-1 du code pénal, le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est passible d'une peine de cinq ans d'emprisonnement et de 300 000 € d'amende. Lorsque l'hébergeur ou les personnes placées sous leur autorité violent leur obligation de secret professionnel, ils s'exposent à une peine d'un an d'emprisonnement et de 15 000 € d'amende. En effet, le code pénal définit le secret professionnel comme : « *la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire*[1019] ». L'article 226-17 du code pénal punit de cinq ans d'emprisonnement et de 300 000 € d'amende la mise en œuvre du traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles

---

[1018] CNIL. Délibération n° 97-008 du 4 février 1997 *portant adoption d'une recommandation sur le traitement des données de santé à caractère personne*l et délibération n° 01-011 du 8 mars 2001 concernant les sites de santé destinée au public. www.cnil.fr.
Plusieurs arguments juridiques permettent de justifier que les données personnelles ne soient pas du domaine de la propriété et donc doivent être exclues du commerce:
«- *Ces données ne peuvent pas être librement modifiées. Elles dépendent en effet de la loi (état civil).*
- La législation sur l'informatique et les libertés est de davantage basée sur l'idée des droits de l'homme plutôt que sur celle de la propriété. Il faut d'ailleurs reconnaître qu'« un droit de propriété peut être vendu mais les droits de l'homme ne peuvent jamais fait l'objet de transactions ».
- La reconnaissance d'un droit de propriété sur les données personnelles fonderait des relations contractuelles entre les usagers et les services publics.
L'absence de droit de propriété sur les données personnelles est un élément protecteur pour les usagers, complété par les recommandations de la CNIL et l'encadrement législatif sur le traitement des données de santé à caractère personnel. » LAVENUE, Jean-Jacques, BEAUVAIS, Grégory. *La commercialisation des données personnelles, perspectives et prospective : l'exemple des données de santé et du DMP* in La sécurité de l'individu numérisé. p. 177

[1019] Article 226-13 du code pénal.

pour que celles-ci ne soient ni endommagées, ni déformées, ni communiquées à des tiers non autorisés. Par ailleurs, la conservation d'informations nominatives au-delà de la durée prévue indiquée dans la demande d'avis ou la déclaration de fichiers auprès de la CNIL sans satisfaire aux formalités requises est condamnée à cinq ans d'emprisonnement et 300 000 € d'amende aux termes de l'article 226-20 du code pénal. Les articles 323-1 à 323-3 répriment l'accès et le maintien frauduleux dans un système de traitement automatisé de données tout comme l'entrave ou le dysfonctionnement de ces systèmes, et l'introduction frauduleuse de données. La peine varie de deux ans d'emprisonnement et de 30 000 € d'amende à cinq ans d'emprisonnement et 75 000 € d'amende selon la gravité de l'acte ou si le traitement automatisé est mis en œuvre par l'État.

En tout état de cause, l'article L 1111-8 du code de la santé publique met en garde les hébergeurs sur la possibilité d'un retrait de l'agrément dans les conditions prévues par l'article 24 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.

Compte tenu de la multiplicité de sanctions et des risques qu'un même fait soit sanctionné par plusieurs dispositions pénales le juge risque de se retrouver devant des cas de conflits de qualifications légales. En la matière, la règle *non bis in idem* s'applique. En effet lorsqu'un même fait est poursuivi sous des qualifications différentes, les juges ne doivent pas cumuler les peines ni relaxer le prévenu, mais ils peuvent lui appliquer la peine la plus sévère[1020].

Le régime de la responsabilité des hébergeurs de données de santé paraît donc complexe du fait de ses diverses ramifications et nécessite que les autorités compétentes se penchent sur la question pour établir un cadre légal ou réglementaire uniforme. Une autre situation plus

[1020] Cette règle est justifiée par le souci de la protection des libertés individuelles de la personne. En France, elle trouve sa source dans les articles 6, 113-9 et 368 du code de procédure pénale . La convention européenne des droits de l'homme la consacre à l'article 4 du protocole additionnel n°7 tout comme l'article 14 paragraphe 7 du pacte international relatif aux droits civils et politiques. Il en est de même de l'article 50 de la charte des droits fondamentaux de l'Union européenne.
La Cour de Cassation a ainsi jugé, en octobre 2013 que : « *sauf à méconnaître la règle « non bis in idem », les mêmes faits ne peuvent faire l'objet de plusieurs qualifications lorsqu'une d'elles recouvre exactement des faits déjà inclus dans une autre qualification ; qu'ainsi, à supposer établis les faits reprochés à Monsieur Pinho Y., celui-ci ne pouvait être déclaré coupable à la fois de complicité du délit d'exploitation illégale des sites aurifères, pour avoir vendu du gasoil destiné au fonctionnement des sites d'exploitation d'aurifères illégaux, et détention et transport de marchandises fortement taxées, pour les mêmes faits ; qu'il s'ensuit que, en procédant pour les mêmes faits à des déclarations de culpabilité, la cour d'appel a méconnu le principe « « non bis in idem » et violé les textes susvisés ;* » Cour de Cassation, chambre criminelle, 30 octobre 2013 , arrêt inédit. JurisData n° 2013-023970. www.lexisnexis.com. Consulté le 10 décembre 2013.

complexe est celle de la responsabilité des hébergeurs de données de santé établis hors des frontières de la France ou de l'Union européenne. En effet, la loi française n'exige pas que les données soient conservées uniquement en France ; ce qui donne d'envisager que des données de santé à caractère personnel soient hébergées dans tout autre pays de l'Union européenne ou hors des frontières à travers les dispositifs binding corporate rules (BCR[1021]) ou de cloud computing. Le problème des difficultés liées aux différences de législations entre les États se transpose alors dans le cadre du régime juridique de la responsabilité des hébergeurs malgré l'existence de la directive européenne e-commerce de 2000 qui tend à uniformiser[1022] la législation en matière de commerce électronique. L'Union européenne a bien adopté une directive[1023] en 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, mais celle-ci laisse le problème du droit applicable aux relations entre patient et professionnel de santé à la législation de chaque État membre. La question de la responsabilité des hébergeurs de données de santé à caractère personnel n'y est pas traitée. L'article 4 de la directive 95/46/CE est la référence actuelle pour résoudre de tels conflits pour les responsables de traitement y compris les fournisseurs d'accès[1024]. Toutefois, les hébergeurs de données de santé, sont des fournisseurs d'accès d'informations en ligne mais ne sont pas les

[1021] Les BCR constituent un code de conduite définissant la politique de l'entreprise en matière de transfert de données. Ils permettent d'offrir une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers à l'Union au sein d'une même entreprise ou d'un même groupe. www.cnil.fr. Disponible le 10 octobre 2013.

[1022] Cette directive institue un cadre garantissant la sécurité juridique pour les entreprises et les consommateurs pour le commerce électronique. Elle harmonise les règles sur des questions comme les exigences en matière de transparence et d'information imposées aux fournisseurs de services en ligne, la communication commerciale, les contrats par voie électronique ou les limites de la responsabilité des prestataires intermédiaires.

[1023] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins transfrontaliers. JOUE du 24 avril 2011. p. L 88/45. Disponible sur: http://eur-lex.europa.ue. Cette directive devait être transposée dans les États de l'Union au plus tard le 25 octobre 2013 mais, en France, par exemple, des travaux de transposition de ce texte ont eu lieu en 2014. [en ligne], disponible sur: http://www.legifrance.gouv.fr/affichLoiPreparation.do;jsessionid=CAEF1CEBC0D0F067B3FBBA77A3780C83.tpdjo14v_3?idDocument=JORFDOLE000027805397&type=general&typeLoi=&legislature=. Consulté le 10 juillet 2014.
A l'issue de ces travaux, une loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la santé. Loi n° 2014-201 du 24 février 2014. JORF n° 0047 du 25 février 2014. p. 3250, texte n° 4. NOR: AFSX1315898L.

[1024] Groupe de travail « article 29 » sur la protection des données. *Avis n° 8/2010 sur le droit applicable adopté le 16 décembre 2010*. 0836-02/10/FR WP 179 et Avis n° 3/2010 sur le principe de la responsabilité adopté le 13 juillet 2010. 00062/10/FR WP 173. Le groupe de travail de l'article 29 à donné des avis sur le principe de la responsabilité des responsables de traitements et sur le droit applicable en matière de protection des données à caractère personnel et fait des propositions pour les améliorations à apporter à la législation existante. [en ligne], 21p. Respectivement disponible sur. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf et p. 19 e 25. Consulté le 2 mai 2014.

responsables des traitements desdites données car leur rôle se limite uniquement au stockage et à la protection des données avec interdiction d'en connaître le contenu. Ils n'entrent donc pas dans le champ d'application de cette disposition. La question de l'efficacité des poursuites contre des hébergeurs établis hors du territoire de l'Union demeure donc préoccupante.

Une solution est proposée par l'article 81 de la proposition de règlement européen sur la protection des données personnelles[1025] qui dispose : « *(...) Les traitements de données à caractère personnel relatives à la santé doivent être effectués sur la base du droit de l'Union ou de la législation d'un État membre qui prévoit des garanties appropriées et spécifiques des intérêts légitimes de la personne concernée, (...)* [1026]». Lorsque l'État présente les garanties requises, il règne une présomption de sécurité, mais lorsque l'État où doivent être hébergées les données n'assure pas de niveau de protection adéquat, le responsable de traitement s'expose à un risque de carence en matière de sécurité, d'intégrité et de confidentialité des données tout comme à l'inefficacité des actions en justice en vue de faire condamner l'hébergeur. Il est donc tenu de prendre des dispositions pour assurer une protection appropriée. En France, en dehors des instruments juridiques prévus par l'article 69 de la loi informatique et libertés (clauses contractuelles types adoptées par la Commission européenne et des BCR), le responsable de traitement peut se munir de clauses contractuelles types qui pourraient, par exemple, soumettre le règlement d'éventuels conflits à la loi française plus protectrice des données traitées. L'article 5 de la loi informatique et libertés lui en donne le droit dans la mesure où sont soumis à cette loi des traitements de données à caractère personnel dont le responsable est établi sur le territoire français ou même le responsable qui est sans être établi sur le territoire français ou sur celui d'un État membre de la communauté européenne, recourt à des moyens de traitement situé sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un

[1025]Voté par le Parlement européen le 21 octobre 2013, le texte a été adopté en plénière. Il devra être négocié par le Parlement avec les gouvernements de l'Union européenne pour être applicable dans tous les États membres deux ans après. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 2 mai 2014.

[1026] Le Parlement a amendé l'article 81 en proposant la version suivante: «Conformément aux règles établies dans le *présent règlement*, notamment son *article 9, paragraphe 2, point h), les traitements de données à caractère personnel relatives à la santé doivent être effectués sur la base du droit de l'Union ou de la législation d'un État membre qui prévoit des garanties appropriées*, cohérentes *et spécifiques des intérêts* et droits fondamentaux *de la personne concernée*, dans le mesure où ils sont *nécessaires* et proportionnés et où leurs effets sont prévisibles par la personne concernée» Disponible sur *:* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR. Consulté le 10 septembre 2014.

autre État membre de la communauté européenne. Cette disposition laisse une large ouverture à l'application de la loi française ou européenne a tout contrat reliant un responsable du traitement établi sur le territoire de la communauté européenne ou utilisant des moyens de traitement situés dans cette région à un hébergeur quelconque y compris celui qui est établi dans un État situé hors des frontières de l'Union.

S'agissant des questions liées au secret professionnel [1027], l'article 84 du projet de règlement européen relègue la compétence de la réglementation de ces responsabilités à la discrétion des États membres. Sur la base de l'article 28 de la directive 95/46/CE, les articles 73 et 74 du projet de règlement rappellent le droit qu'à toute personne ou association de faire une réclamation auprès de l'autorité de contrôle de son État en cas de violation de ses données à caractère personnel. Les victimes ont le droit de former un recours juridictionnel contre l'autorité de contrôle en vue de la contraindre à donner une suite à leur réclamation. Aux termes de l'article 79[1028], l'autorité de contrôle inflige une amende pouvant s'élever à 1 million d'euros ou dans le cas d'une entreprise, à 2 % de son chiffre d'affaires annuel à quiconque ne respecte pas les règles de protection du secret professionnel conformément à l'article 84. Cette disposition est applicable à la responsabilité des professionnels de santé.

[1027] « *Dans la limite du présent règlement, les États membres peuvent adopter des règles spéciales afin de définir les pouvoirs d'investigation des autorités de contrôle visés à l'article 53, paragraphe 2, en ce qui concerne les responsables du traitement ou les sous-traitants qui sont soumis, en vertu du droit national ou de réglementations arrêtés par les autorités nationales compétentes, à une obligation de secret professionnel ou d'autres obligations de secret équivalentes, lorsque de telles règles sont nécessaires et proportionnées pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret. Ces règles ne sont applicables qu'en ce qui concerne les données à caractère personnel que les responsables du traitement ou le sous-traitant a reçues ou s'est procurées dans le cadre d'une activité couverte par ladite obligation de secret.* » Commission européenne. *Proposition de règlement du Parlement européen et du Conseil relatif à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données (règlement général sur la protection des données).* [en ligne], Bruxelles, le 25 janvier 2012. 2012/0011 (COD). Disponible sur: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 11 novembre 2013.

[1028] Article 79, 6. o) Commission européenne. *Proposition de règlement du Parlement européen et du Conseil relatif à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données (règlement général sur la protection des données).* Bruxelles, le 25 janvier 2012. 2012/0011 (COD). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 11 novembre 2013.

B. Au niveau du professionnel de santé

Le professionnel de santé doit exercer sa mission dans le respect de la vie humaine, de la personne et de sa dignité. Dans cette optique, il est le garant de la confidentialité des renseignements personnels de santé de ses patients à travers son obligation de secret médical. L'alinéa 2 de l'article L 1110-4 du code de la santé publique définit l'étendue de ce secret comme couvrant, à l'exception des cas de dérogation expressément prévue par la loi: «*l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes ou de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé.* » Ils sont tenus de préserver la confidentialité de ce qui leur a été confié, mais aussi ce qu'ils ont vu, entendu ou compris[1029]. Mais le contexte actuel de la télésanté amène les professionnels de santé à partager davantage d'informations relatives à leur patient. C'est pourquoi le cadre législatif a été assoupli pour envisager un secret partagé mais toujours avec le souci de la protection de la vie privée du patient. Les implications de cette obligation de secret deviennent plus complexes lorsque le secret est partagé et le régime juridique de leur responsabilité s'en trouve davantage modifié à l'ère des dossiers médicaux électroniques.

1. Le secret médical partagé

En principe, le professionnel de santé détenant une information concernant une personne ne peut la publier. Mais l'article L 1110-4 du code de la santé publique qui rappelle le principe du secret médical admet le premier assouplissement à son alinéa 3. « *Deux ou plusieurs professionnels de santé peuvent toutefois, sauf opposition de la personne dûment avertie, échanger des informations relatives à une même personne prise en charge, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge possible (...)* »

[1029] Le secret médical a été défini par les tribunaux comme portant sur non seulement ce qui leur a été confié, mais également sur tout ce qui leur a été donné de connaître dans l'exercice de leur activité. Cassation criminelle, 26 juillet 1845. DP 1845,I, p. 340.

Cet assouplissement est dit secret partagé car les personnes à qui il est confié sont toutes tenues d'une obligation de secret professionnel. Il consiste pour le professionnel de santé à révéler les informations couvertes par le secret à un autre professionnel lui-même tenu au secret. Le secret médical n'est donc pas levé mais c'est le cercle des dépositaires des mêmes informations qui s'agrandit. Ce partage permis dans un objectif d'intérêt majeur est soumis à des conditions établies par la loi.

a. L'objectif du partage du secret médical

Le secret professionnel peut être partagé au sein des membres d'une même équipe ou d'un même établissement de santé, mais les dossiers médicaux électroniques et notamment le dossier médical personnel étendent le partage du secret à un plus grand nombre de professionnels et au-delà des limites d'un seul établissement de santé.

Le partage du secret médical se justifie par un objectif de recherche de qualité de soins. C'est donc une atténuation[1030] à l'obligation absolue[1031] de secret dans l'intérêt du patient. Le partage des informations relatives à un patient devient nécessaire dans le contexte de l'évolution du système de santé où l'on a de plus en plus recours aux services des spécialistes pour assurer un meilleur suivi médical à l'individu. Le traitement d'une même pathologie peut faire l'objet de plusieurs consultations par différents professionnels. Le législateur, conscient de cette situation essaie d'adapter les textes aux nouvelles réalités.

Admis depuis le décret[1032] portant règlement d'administration publique pour l'application de la loi sur la réorganisation des hôpitaux et des hospices publics de 1943, le secret partagé a été consacré par le Conseil d'État en 1953. L'article 38 du décret précité prévoyait que « *le dossier médical du malade est conservé dans les services de l'hôpital, sous la responsabilité du médecin chef du service. Il peut être communiqué aux autres services de*

[1030] Les premières dérogations au secret professionnel médical ont été admises dès le 30 novembre 1892 au nom de la préservation de la santé publique. RENE. Louis. *Le secret dans le nouveau code pénal*, Editorial. Bulletin de l'Ordre des médecins. Décembre 1992, n° 12, p. 229-230.

[1031] Dès le XIXe siècle la jurisprudence a proclamé le caractère général et absolu du secret médical. Les arrêts de la chambre criminelle de la Cour de Cassation (l'arrêt Watelet du 19 décembre 1885, Droit pénal 1986-I. p.347 et ensuite l'arrêt Degraene du 8 mai 1947, Dalloz 1948- 109) affirmaient que « *l'obligation du secret professionnel s'impose aux médecins comme un devoir de leur état. Elle est générale et absolue et il n'appartient à personne de les en affranchir* ».

[1032] Décret n° 43-891 du 17 avril 1943 portant règlement d'administration publique pour l'application de la loi du 21 décembre 1941 sur la réorganisation des hôpitaux et des hospices. JORF du 27 avril 1943. P. 1156.

l'hôpital ou du groupement hospitalier ; et peut-être examiné sur place à la demande du malade par son médecin traitant. » Cette première étape de la légalisation du secret partagé limitait la communication des informations au sein du groupement hospitalier où le patient était pris en charge. Et même en cas de besoin, le dossier médical devait être examiné "*sur place"* par le médecin traitant. Cette disposition reconnaissait la possibilité du partage sans en justifier les finalités. C'est le Conseil d'État qui, en 1953[1033], permet le partage d'informations à la condition d'être nécessaire pour assurer la continuité des soins. Le Conseil d'État ajoute ainsi la condition de la nécessité d'une continuité de soins. Cette position est renchérie en 1973 par une circulaire ministérielle[1034] qui déclare que « *le caractère collectif revêtu par le secret professionnel dans le cadre du service public hospitalier a pour conséquence de permettre la circulation du dossier médical (…) entre les différents services du même établissement* ». L'article L 1110-4 du code de la santé publique issu de la loi du 4 mars 2002 qui constitue le fondement légal actuel du secret partagé reconduit la finalité prônée par la jurisprudence et ajoute un objectif thérapeutique dans l'intérêt du patient. Le partage doit se faire afin *de déterminer la meilleure prise en charge possible.* D'ailleurs, le Conseil Constitutionnel, saisi au sujet de la loi relative à l'assurance maladie, confère à toute démarche en vue d'améliorer la qualité des soins ou de réduire le déséquilibre financier de l'assurance maladie une valeur constitutionnelle[1035]. C'est pourquoi tout partage d'informations médicales n'allant pas dans ce sens est considéré comme une violation du secret médical au sens de l'article 226-13 du code pénal.

Le dossier médical personnel ayant été créé pour assurer la continuité des soins dans l'intérêt du patient, la loi du 13 août 2004 relative à l'assurance-maladie autorise tout professionnel intervenant dans le parcours de soins à consulter les informations consignées dans le dossier médical personnel. C'est un partage à une plus grande échelle qui est susceptible d'aller au-delà des limites d'une équipe de soins, d'un hôpital de ville ou même d'un État. Or, les articles L 1111-14 et suivants du code de la santé publique qui régissent le DMP ne posent pas d'autres conditions que l'accord du patient pour autoriser le partage de

[1033] Conseil d'État, section sociale. 2 juin 1953. Bulletin de l'ordre des médecins 1952-1954. P. 194.

[1034] Circulaire ministérielle n° 1796 du 20 avril 1973 relatif au secret professionnel dans les établissements d'hospitalisation publics. http://portail-web.aphp.fr/daj/public/index/display/page/433/id_fiche/3401. Consulté le 26 mai 2014.

[1035] Conseil constitutionnel. 12 août 2004. Décision n° 2004-504 DC relative à la loi sur l'assurance maladie. Considérant n° 8.

données de santé entre professionnels de santé. On n'ignore, cependant, pas que les risques grandissent proportionnellement à l'étendue du partage. Didier SICARD[1036] avait dénoncé les risques d'atteinte encourus avec les changements sociaux et les innovations technologiques. Le secret médical partagé devient un secret « *propagé* », « *un secret de Polichinelle* » car « *il devient difficile de savoir où s'arrête vraiment l'intérêt thérapeutique et la limite de ce qui est transmissible* ». Il avait écrit : « *le danger est en effet d'arguer des principes de précaution au service d'une démocratie d'opinion à l'appui de la rupture du secret et d'introduire l'extension du secret partagé au nom du principe lui-même. Le caractère fallacieux de ce partage d'informations peut aboutir à une perversion de ce principe. Ceci d'autant plus que la médecine a changé. La médecine d'autrefois était une médecine du rapport à la personne, au corps, très individuelle : ce qui était confié par le malade par la parole constituait une sorte d'engagement à être tu. En revanche, actuellement, le rapport au corps est manifestement en voie de disparition : on assiste à un véritable transfert sur les examens biologiques, l'imagerie, et finalement à une certaine indifférence à considérer que les documents peuvent être communiqués. On transgresse moins facilement le secret d'un corps ou d'une parole*[1037]. »

Cette inquiétude se justifie encore plus dans la mesure où avec le dossier médical personnel le secret médical risque d'être partagé entre les professionnels de santé et les hébergeurs, sans oublier les médecins des hébergeurs. La situation du médecin de l'hébergeur constitue une dérogation supplémentaire au principe du partage des informations médicales entre les professionnels de santé prenant le patient concerné en charge. Le médecin de l'hébergeur est autorisé à accéder au dossier médical personnel comme indiqué ci-dessus en cas de demande de copie ou de destruction d'un document ou de toute autre demande de la part du titulaire. Son rôle est de veiller à la protection de la confidentialité des données de santé au sein de l'organisme de l'hébergeur. Il n'intervient pas dans la phase pratique du processus de continuité des soins ni dans la recherche de la meilleure qualité de soins. La lecture de l'article L 1110-4 du code de la santé publique, stricto sensu, exclut donc un secret partagé avec le médecin de l'hébergeur même si celui-ci est lié par le secret médical du fait de sa fonction. Mais, son intervention a une origine réglementaire qu'on ne peut ignorer. C'est donc une dérogation d'une dérogation qui nous semble être une violation du secret médical

[1036] SICARD, Didier fut Président d'honneur du Comité consultatif national d'éthique de 1999 à 2007.

[1037] SICARD, Didier. *Quelles limites au secret médical partagé ?* Dalloz 2009. p. 2634.

que l'on justifie par la recherche d'un meilleur suivi thérapeutique tout en contribuant à réduire les dépenses des soins de santé de l'assurance maladie. De plus, on ne peut que s'incliner devant cette situation quand le Conseil d'État a admis qu'une atteinte au secret médical peut être jugée légale si elle est la conséquence nécessaire d'une disposition législative[1038]. Le secret médical partagé ne tient sa raison d'être que parce qu'il répond à des conditions instituées par la loi.

b. Les conditions du partage du secret médical

Le secret médical partagé tel qu'admis au sein du « colloque singulier[1039] » est soumis à la condition du consentement du patient. Au risque de friser la redondance, plusieurs dispositions du code de la santé publique reprennent la condition du recours à l'accord du patient avant de pouvoir partager ses informations.

« *Les informations concernant une personne prise en charge par un professionnel de santé au sein d'une maison ou d'un centre de santé sont réputées confiées par la personne aux autres professionnels de santé de la structure qui la prenne en charge, sous réserve : 1° du recueil de son consentement exprès, par tout moyen, y compris sous forme dématérialisée. Ce consentement est valable tant qu'il n'a pas été retiré selon les mêmes formes ; 2° de l'adhésion des professionnels concernés au projet de santé mentionné aux articles L 6323-1*[1040] *et L*

[1038] Conseil d'État. 8 février 1989, n° 54494. Conseil national de l'Ordre des médecins et autres. Recueil Lebon 1989.

[1039] Ce colloque qui devient pluriel dans le cadre du secret partagé du fait de la multiplicité des intervenants est, en médecine la relation, en principe, de confiance établie entre un médecin et son patient. C'est une expression française de l'écrivain Georges Duhamel en 1934. Médecin, il défendait, dans La revue des deux mondes, la médecine libérale contre l'étatisme et la médecine sociale au lendemain des premières assurances sociales. Il y décrit la relation entre le médecin et le malade comme un duo se jouant dans un espace clos. L'expression a été reprise par Louis PORTES, Président du Conseil national de l'Ordre des médecins de 1943 à 1949. Il lui a associé la formule célèbre d'une « *confiance qui rejoint librement une conscience* », qui promeut une relation ouvertement déséquilibrée. De plus, il entre dans le secret : « *il n'y a pas de médecine sans confiance, de confiance sans confidence et de confidence sans secret* ». CANNASSE, Serge. Entretien de Hardy Anne-Chantal. *Le colloque singulier, un mythe français*. Carnets de santé. Juin 2013. http://www.carnetsdesante.fr/Hardy-Anne-Chantal. Consulté le 20 novembre 2013.

[1040] *« Les centres de santé élaborent un projet de santé incluant des dispositions tendant à favoriser l'accessibilité sociale, la coordination des soins et le développement d'actions de santé publique.* »

6323-3[1041]*. La personne, dûment informée, peut refuser à tout moment que soient communiquées des informations la concernant à un ou plusieurs professionnels de santé*[1042]*.* » Et l'article 4127-68 du code de la santé publique de préciser : « *avec l'accord du patient, les médecins échangent avec les autres membres des professions de santé les informations utiles à leur intervention*[1043] *»*. Si la première disposition ajoute à l'autorisation du patient la condition de la participation du professionnel destinataire au processus de soins, la seconde insiste davantage sur l'utilité des informations pour les récepteurs. Ces conditions sont donc cumulatives car les renseignements personnels de santé ne peuvent être divulgués sans aucune raison légitime. Seules les informations portant sur les éléments indispensables aux soins du patient doivent être échangées. Le secret partagé porte alors sur les informations entre les personnes qui concourent directement aux soins du patient. Les personnels de soins ne disposant d'aucune compétence juridique ni professionnelle pour prendre part aux décisions de l'équipe soignante ne sont alors pas habilitées à partager le secret. C'est le cas des agents des services hospitaliers qualifiés (ASHQ) ou non (ASH) et des brancardiers, par exemple. Cette exigence de l'utilité de la communication des informations a été privilégiée par la jurisprudence avant même la loi de 2002. Le Conseil d'État avait déclaré en 1972 « *lorsqu'un malade s'adresse à un organisme qui (...) pratique la médecine collective, c'est nécessairement à l'ensemble du personnel médical que, sauf prescription particulière de la part de ce malade, le secret médical est confié ; que, dès lors, un tel organisme ne peut, sans le consentement du malade intéressé, se dessaisir, au profit d'un médecin qui aurait cessé d'exercer ses fonctions en son sein, des fiches médicales (...) établies par les médecins attachés à cet organisme*[1044] ».

Le consentement du patient peut être reçu de différentes manières. Le législateur envisage un accord qui peut être exprès, ou reçu par tout moyen y compris la forme

---

[1041] « *La maison de santé est une personne morale constituée entre des professionnels médicaux, auxiliaires médicaux ou pharmacien. Ils assurent des activités de soins sans hébergement de premier recours au sens de l'article L 1411-11 et le cas échéant, de second recours au sens de l'article L 1411-12 et de participer à des actions de santé publique, de prévention, d'éducation pour la santé et à des actions sociales dans le cadre du projet de santé qu'ils élaborent et dans le respect d'un cahier des charges déterminé par arrêté du ministre chargé de la santé.* »

[1042] Article L 1110-4, alinéa 4 du code de la santé publique.

[1043] L'article L 4127-45 émet la même disposition entre médecins : « *à la demande du patient ou avec son consentement, le médecin transmet aux médecins qui participent à la prise en charge ou à ceux qu'il entend Consulté les informations et documents utiles à la continuité de soins.* »

[1044] Conseil d'État, Section. 11 février 1972 n° 76799. Recueil des décisions du Conseil d'État 1972, p. 138.

dématérialisée ou encore un consentement tacite. La suite de l'alinéa 3 de l'article L 1110-4 du code de la santé publique dispose *: « 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 »*. Le consentement implicite est donc admis en milieu hospitalier tandis que l'autorisation expresse convient le mieux dans le cadre de la médecine de ville. Dans ce dernier cas, le consentement pourra être tacite si la personne dûment avertie ne s'oppose pas au partage de ses données avec d'autres professionnels. En pratique, il n'est pas évident de croire qu'une absence d'opposition équivaille véritablement à un consentement car, en général, le patient suit le mouvement dans l'attente d'une meilleure prise en charge. Le consentement dématérialisé donné à la création du dossier médical personnel est une autorisation de secret partagé que donne l'assuré sans véritablement mesurer l'étendue de cette diffusion.

Tous ces textes accordent une place privilégiée au droit de refus que pourrait exercer le patient par rapport à la transmission de ses données à un professionnel de santé. Le secret partagé peut donc se heurter au droit d'opposition du patient car les données médicales lui sont propres et personnelles et qu'il peut en disposer comme il l'entend. Le recours au consentement doit être précédé d'une information claire du patient afin de lui laisser la possibilité d'exercer ce droit d'opposition. Le consentement déjà accordé peut même être retiré à condition que cela soit fait dans les mêmes formes que celles dans lesquelles il a été donné.

Le secret médical ayant été proclamé par la loi du 4 mars 2002 comme droit de la personne[1045], *« l'on passe d'une obligation du médecin sanctionnée au titre d'un délit pénal par le code pénal, a un droit du patient garanti par le code de la santé publique*[1046] », et qui lui permet de décider du cercle des bénéficiaires du secret partagé. Mais, la reconnaissance d'un tel pouvoir au titulaire des données suscite des interrogations : le patient a-t-il les capacités nécessaires pour décider de la pertinence de la communication de ses informations à un autre professionnel de santé ? En cas de refus, le médecin peut-il passer outre le consentement de la personne s'il estime le partage indispensable à la qualité des soins sans risque d'engager sa responsabilité pénale ? La réponse à cette seconde question est négative.

[1045] « *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé, ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant* ». Article L 1110-4, alinéa 1 du code de la santé publique.

[1046] BACACHE-GIBEILI, Mireille. *Le secret médical partagé*. Gazette du palais, 30 décembre 2008 n° 365. P. 44.

Pour autant, s'il est indéniable que le droit de refus constitue un élément de la liberté d'expression, fondamentale à l'individu, le permettre dans ces conditions peut être source de blocage pouvant desservir les intérêts du patient. « *Peut-être aurait-il pu être suggéré au législateur de soumettre le refus du patient à une obligation de motivation de sa part. Celle-ci aurait certainement pu permettre au médecin qui le soigne de comprendre la position de son patient et de créer à nouveau un dialogue*[1047]*»*.

Le secret partagé est un assouplissement du secret médical fondé sur plusieurs textes législatifs et une base jurisprudentielle abondante. Mais le législateur n'a pas encore pu adapter les textes à l'évolution technologique pour endiguer les craintes d'atteinte aux données personnelles de santé des patients. Le droit positif prévoit plusieurs autres hypothèses de dérogation au secret médical[1048] justifiées par l'intérêt général sur lesquelles nous ne nous attarderons pas dans le cadre de cette étude.

« *L'informatique introduit dans notre monde un mode nouveau de gestion et d'exploitation des renseignements sans modifier les données du problème du secret*[1049] ». Le secret partagé n'exonère pas les professionnels de santé de leur responsabilité liée à leur obligation de secret mais il peut l'influencer.

[1047] WILLIATE-PELITTERI, Lina. *Les autres risques du doit. L'impact du décret du 7 mai 2012 sur la relation médecin - patient : un retranchement à regretter ? Décret n° 2012-6947 du 7 mai 2012 portant modification du code de déontologie médicale* in Droit et risque *n°4 (1ère partie).* Les petites affiches, 14 janvier 2013 n° 10, p. 6.

[1048] La liste n'est pas exhaustive:
– Article 226-14 du code pénal. Révélation du secret relative à l'accueil et à la protection de l'enfance.
– Conseil d'État deuxième et septième sous-section réunies, 17 octobre 2012. Décision n° 353576. Considérant n° 6. « *considérant, (...), qu'en énonçant que les centres d'accueil informent les médecins de l'agence régionale de santé et de l'Office Français de l'immigration et de l'intégration des situations portées à leur connaissance susceptibles de présenter un risque de santé publique, la circulaire attaquée, qui a mis en œuvre les dispositions du code de la santé publique qui organisent la transmission d'informations aux autorités sanitaires, n'a pas eu pour objet ou pour effet de déroger aux dispositions applicables régissant le secret médical ou le secret professionnel ;* » au sujet de la légalité d'une circulaire traitant du pilotage du dispositif national d'accueil des demandeurs d'asile émise par le ministre chargé de l'immigration. Recueil Lebon 2012.
– Article L 1110-4 code de la santé publique, information des proches de la personne
– Article L 1142-12 alinéa 5 du code de la santé publique. Le secret est partagé de façon obligatoire et automatique sans recourir à l'autorisation du patient dans un but d'intérêt indemnitaire.
– Article L 1413-5 du code de la santé publique. Dans ce cas le partage vise la maîtrise des dépenses de santé et d'amélioration de la qualité des soins à travers la recherche et l'évaluation
– Article L 6113-7 alinéa 2 du code de la santé publique. Les praticiens transmettent les données médicales nominatives nécessaires à l'analyse de l'activité et à la facturation au médecin responsable de l'information médicale.

[1049] GALLOUEDEC-GENUYS, Françoise. Le secret des fichiers. préface. IFSA. CUJAS. 1976

2. La responsabilité des professionnels de santé

Un avis de l'académie de médecine de 1834 affirmait : « *le médecin ne reconnaît pour juge, après Dieu, que ses pairs et n'accepte point d'autre responsabilité que celle, toute morale de sa conscience*[1050] ». Malgré l'éloquence de cette citation, le droit positif la contredit en reconnaissant une responsabilité du médecin devant les autorités publiques justifiée par la protection du droit du patient au secret de ses informations médicales. La divulgation de données de santé engage la responsabilité civile du professionnel de santé pour préjudice moral dès lors que le patient démontre sur le fondement des articles 1382 et 1383 du Code civil le lien entre le dommage, le préjudice et le lien de causalité entre les deux. Le secret médical[1051] est un devoir d'intérêt autant privé vis-à-vis de la personne du patient que public du fait de l'impact de la discrétion du professionnel de santé sur la société. Chacun a droit au respect de sa vie privée et les juges peuvent prescrire toutes mesures propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée[1052]. C'est pourquoi la responsabilité du professionnel de santé est régie non seulement par son code de déontologie mais également par le code pénal. Le dossier médical personnel encadré par un régime particulier influence le régime de la responsabilité des professionnels de santé.

a. La responsabilité du professionnel de santé relative à la gestion des données de santé à caractère personnel

Le professionnel de santé jouit d'une indépendance dans l'exercice de sa profession. L'article R 4127-5 du code de la santé publique pose le principe concernant les médecins en ces termes : « *le médecin ne peut aliéner son indépendance professionnelle sous quelque*

[1050] Cour de cassation. Requête, 18 juin 1835,S. 1835, I, 26, P. 401. Dalloz 1835,1, P. 300, conclusions Dupin.

[1051] Les jurisprudences du Conseil d'État et de la Cour de Cassation retenant le caractère général et absolu du secret médical en ont tiré les conséquences suivantes : le patient ne peut délier le médecin de son obligation de secret; cette obligation ne cesse pas après la mort du patient; le secret s'impose même devant le juge; le secret s'impose à l'égard d'autres médecins dès lors qu'ils ne concourent pas à un acte de soins;. le secret s'impose à l'égard de personnes elles-mêmes tenues au secret professionnel (agents des services fiscaux); le secret couvre non seulement l'état de santé du patient mais également son nom : le médecin ne peut faire connaître à des tiers le nom des personnes qui ont eu recours à ses services. Conseil d'État, arrêt d'Assemblée du 12 avril 1957 - Deve; 6 février 1951 et 2 juin 1953. Cour de Cassation arrêt Watelet de 1885 précité.

[1052] Article 9 du code civil.

forme que ce soit. » La règle est reprise par l'article R 4127-209 pour les chirurgiens-dentistes, l'article R 4312-9 pour les infirmiers et infirmières et l'article 4127-307 pour les sages femmes. Ces dispositions ont été introduites au code de la santé publique, respectivement par les articles 5, 6, 9 et 7 des codes de déontologie de ces différents corps de métiers. Ce principe donne une pleine liberté de décision et d'action aux professionnels de santé et constitue le fondement de la relation de confiance qui existe entre leur patient et eux. Mais il a pour corollaire la responsabilité personnelle des professionnels de santé car leurs actes sont censés dénués de toute influence extérieure et ne peuvent engager qu'eux. Ainsi, face à une action en responsabilité, un médecin même salarié, ne peut se réfugier derrière les principes régissant la responsabilité des commettants du fait de leurs préposés pour se soustraire à ses engagements. Le tribunal des conflits l'a rappelé dans une affaire mettant en cause un anesthésiste ayant commis des fautes dans le cadre de son service. « *eu égard à l'indépendance professionnelle dont bénéficie le médecin dans l'exercice de son art qui est au nombre des principes généraux du droit, il est loisible au patient, indépendamment de l'action qu'il est en droit d'exercer sur un fondement contractuel à l'encontre de l'établissement privé de santé de rechercher, sur le terrain délictuel, la responsabilité du praticien lorsque, par la réalisation d'actes médicaux, celui-ci a commis une faute*[1053] ».

S'agissant des médecins, l'article R 4127-69 du code de la santé publique (article 69 du code déontologie médicale) apporte cette précision en indiquant que l'exercice de la médecine est personnel et chaque médecin est responsable de ses décisions et de ses actes. De ce fait, il a l'obligation de veiller à la protection de son nom, sa qualité ou ses déclarations. Pour assurer l'authenticité de ses interventions aux données de santé à caractère personnel de ses patients et éviter l'usurpation de son identité, il est recommandé des moyens comme la signature électronique et les mots de passe. Sa responsabilité personnelle ne sera donc engagée que s'il est fait la preuve qu'il n'a pas pris les dispositions requises pour assurer cette protection de son identité ; l'identité qui est d'autant plus essentielle dans l'exercice des professions de santé que le code de la santé publique interdit l'usage d'un pseudonyme en son article L 4113-3. Cette interdiction est absolue pour les médecins mais plus souple pour les sages femmes et les

[1053]Tribunal des conflits. 14 février 2000, n° 02929, Les petites affiches 2000, n° 196, p. 8, note. WELSCH S.. Revue française de droit administratif 2000, p. 1232 note POUYAUD, D.

chirurgiens-dentistes[1054] mais la violation de cette interdiction expose le contrevenant à une amende de 4500 € et la récidive à six mois d'emprisonnement et 9000 € d'amende[1055].
Le 9 mars 2010 la Cour de Cassation, chambre criminelle, a rejeté un pourvoi[1056] portant sur un cas d'exercice de la médecine sous un pseudonyme. La Cour d'Appel de Toulouse, chambre criminelle avait condamné le prévenu pour l'exercice de la médecine sous un pseudonyme au motif que cela est prohibé par le code de la santé publique pour *« des raisons évidentes de sécurité pour les patients, qui doivent savoir à qui ils confient leur santé »*.

La responsabilité personnelle du médecin peut également être mise en cause du fait de la divulgation de correspondance. Si, les correspondances entre professionnels de santé, sont nécessaires pour assurer la prise en charge et le meilleur traitement du patient, les informations qu'elles comportent nécessitent à la fois le respect du secret médical et de la vie privée. C'est pourquoi leur transmission doit se faire conformément à un certain nombre d'exigences notamment techniques et déontologiques. L'article R 4127-71 du code de la santé publique prescrit que « *le médecin doit disposer, au lieu de son exercice professionnel, d'une installation convenable, de locaux adéquats pour permettre le respect du secret professionnel et de moyens techniques suffisants en rapport avec la nature des actes qu'ils pratiquent ou de la population qu'il prend en charge (...)* ». Même s'il est admis un secret partagé du fait de l'évolution technologique et pour les besoins d'une meilleure prise en charge, le professionnel de santé doit faire preuve de tact et de mesure avec ses confrères dans la transmission de ces informations. Il doit se limiter aux seules données « *nécessaires, pertinentes et non excessives*[1057]». En l'état actuel du droit positif, aucun texte ne permet de délimiter le niveau d'information susceptible d'être transmis ni le niveau de continuité des soins à partir duquel l'échange de correspondance peut s'avérer abusif. Le praticien devra alors, en son âme et

[1054] Le chirurgien-dentiste se servant d'un pseudonyme pour des activités se rattachant à sa profession est tenu d'en faire la déclaration au Conseil départemental de l'ordre. Aux termes de l'article R 4127-225 du code de la santé publique. L'article R 4127-308 du même code dispose également que si la sage-femme se sert d'un pseudonyme pour des activités se rattachant à sa profession, elle est tenue d'en faire la déclaration au Conseil départemental de son ordre.

[1055] Article L 4163-5 du code de la santé publique.

[1056] Cour de cassation, chambre criminelle. Formation restreinte. X... Philippe. 9 mars 2010. Pourvoi n° 09-81.778.

[1057] Cour de Cassation, chambre criminelle, 6 juin 1972, n° 70-90. 271. Bulletin criminel n° 190, Gazette du palais 1972, II, jurisprudence, P. 668.

conscience, décider de l'opportunité de la communication des informations de santé des patients.

b. La responsabilité du professionnel de santé dans le cadre du dossier médical personnel

La responsabilité médicale des professionnels de santé n'a pas été modifiée, dans son fondement, par la loi du 13 août 2004 instaurant le dossier médical personnel, mais le caractère dématérialisé influence l'appréciation de leur faute. Contrairement au dossier médical traditionnel, le dossier médical personnel est une base de données dématérialisée au sens de l'article L 112-3 alinéa 2 du code de la propriété intellectuelle qui définit la base de données comme : *«un recueil d'œuvres, de données ou d'autres éléments indépendants, disposées de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen ».* Ce statut engendre des effets qui n'étaient pas prévus pour le dossier médical traditionnel avec le déplacement de l'objet de l'obligation des professionnels de santé sur la gestion des données des patients. Alors qu'ils sont tenus de constituer un dossier médical pour chaque patient à l'occasion de chaque acte ou consultation, les professionnels de santé sont seulement obligés de reporter et de mettre à jour des informations «*nécessaires à la coordination de soins de la personne prise en charge»* dans le dossier médical personnel[1058]. Cette obligation, relativement moins contraignante par rapport à la constitution du dossier peut, néanmoins, engager la responsabilité des professionnels de santé. Le cas des médecins traitants est particulièrement marquant.

La première responsabilité du professionnel de santé pourrait provenir de son obligation d'informer et de requérir le consentement du patient avant de lui ouvrir un dossier médical personnel. Le patient devra rapporter la preuve de ce manquement et le professionnel pourra se prémunir de la traçabilité des actions dans le dossier pour se défendre. Après l'ouverture du dossier, toute consultation réalisée sans l'autorisation du patient expose le professionnel à une peine d'amende et/ou d'emprisonnement conformément à l'article 323-1 du code pénal pour accès frauduleux dans tout ou partie d'un système automatisé de données. Mais si un professionnel de santé ne consulte pas le dossier médical personnel et établi un diagnostic

[1058] Article L -36-2 du code de la santé publique.

erroné ou des traitements inadaptés, il peut encourir une sanction. En effet, la consultation du dossier étant obligatoire pour le professionnel de santé lors d'une auscultation, il peut voir sa responsabilité engagée pour négligence s'il est démontré que le dommage subi par le patient est dû à cela. La preuve de la diligence du professionnel de santé pourra être faite par la traçabilité de ses actions de consultation du DMP.

« *(…) Chaque professionnel de santé, exerçant en ville ou un établissement de santé, quel que soit son mode d'exercice, reporte dans le dossier médical personnel, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge. (…)*[1059] »

La tenue d'un dossier médical est une obligation qui a été formalisée par la loi[1060] du 18 janvier 1994 relative à la santé publique et à la protection sociale. Instituant le dossier de suivi médical, ce texte a mis à la charge de chaque professionnel de santé l'obligation de tenir une fiche d'observations pour tous les patients. Plus tard, la loi[1061] du 13 août 2004 a subordonné l'adhésion aux conventions nationales régissant les rapports entre les organismes d'assurance-maladie et les professionnels de santé et son maintien par le médecin à la consultation ou à la mise à jour du dossier médical personnel de la personne prise en charge[1062]. D'une part, Il est tenu, d'insérer dans le DMP tous les documents qui permettront à la Sécurité sociale d'évaluer la situation du bénéficiaire afin de procéder au remboursement requis. Le cas échéant, sauf à prouver que l'indisponibilité du service est imputable à l'hébergeur, le professionnel de santé verrait sa responsabilité engagée et le patient pourrait alors demander la réparation de son préjudice économique occasionné par l'absence de mise à jour de son dossier. L'incidence financière de la tenue du dossier médical a été mise en exergue dans un arrêt de la Cour de Cassation le 10 mai 2012. En l'espèce, plusieurs médecins avaient été condamnés, dans le cadre d'une procédure de répétition de l'indu, à payer une somme d'argent à la Caisse primaire d'assurance maladie du fait des carences relevées dans la tenue de dossiers médicaux. *« Ont été observées l'absence d'identification des psychiatres, l'absence de médicalisation des observations, le dossier se présentant sous la forme d'une liste de remarques brèves et d'ordre*

[1059] Article L -1111-15 du code de la santé publique.

[1060] 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. NOR: SPSX9300136L .

[1061] Loi n° 2004-810 du 13 août 2004 relative à l'assurance-maladie. Article 3. JORF du 17 août 2004. p. 14598. Texte n° 2. NOR: SANX0400122L. www.legifrance.fr

[1062] Article L 161-36-1 du code de la sécurité sociale, alinéa 3.

général jour après jour, dont l'ensemble constituait un mémento soulignant quelques points particuliers mais non médicaux, le seul substrat étant la consigne thérapeutique jamais motivée, destinée au personnel infirmier [1063]». D'autre part, les professionnels de santé sont liés par les contenus qu'ils insèrent dans les dossiers médicaux. En effet, dans le parcours de santé, chaque professionnel se sert des informations de ses prédécesseurs pour établir la situation pathologique de leur patient. De ce fait, des omissions ou des mentions erronées affectent sérieusement les diagnostics des professionnels de santé suivants. Ainsi, le professionnel de santé dont les notes auraient négativement influencé les décisions de ses confrères pourrait voir sa responsabilité professionnelle engagée et le patient serait bien fondé à rechercher la responsabilité de chacun des intervenants successifs. Dans l'arrêt[1064] époux V de 1992, le Conseil d'État avait retenu, qu'à la suite d'une succession d'erreurs et d'imprudence de la part de divers intervenants médicaux d'un hôpital, la faute médicale de cet établissement était de nature à engager sa responsabilité. De même, le manquement au respect de l'obligation réglementaire de faire figurer dans les dossiers médicaux les comptes rendus opératoires qui auraient dus être joints au dossier médical du patient constitue une faute déontologique et engage la responsabilité du chirurgien[1065].

Le risque de déconventionnement encouru par les professionnels de santé qui ne consulteraient pas ou ne mettraient pas à jour le dossier médical personnel constitue une sanction d'un maniement délicat. La loi instituant le dossier médical personnel n'ayant pas prévu de contrepartie financière ou de tout autre nature pour le travail supplémentaire que constitue la gestion de ce nouveau dossier, il paraît injuste de brandir une telle menace. À notre sens, tout comme a été retirée du dispositif, la condition de remboursement des soins du patient la création de son dossier médical personnel, les autorités compétentes auraient dû, également, se pencher sur cette question. Cela pourrait constituer une source de démotivation pour les professionnels de santé qui se voient contraints de faire un travail supplémentaire pour éviter de subir la sanction. Le risque pour le projet de déploiement du DMP et pour les patients c'est de voir certains professionnels de la santé consulter et reporter des informations de façon partielle ou désinvolte, juste pour remplir une obligation.

[1063] Cour de Cassation, chambre civile 2, arrêt inédit du 10 mai 2012. Pourvoi n° 10-28.767.

[1064] Conseil d'État, Assemblée. 10 avril 1992. N° 79027. Publié au recueil Lebon 1992.

[1065] Conseil d'État, quatrième et sixième sous-sections réunies, 28 avril 2003, n° 238181. Publié aux tables du recueil Lebon.

Alors que le dossier médical traditionnel est conservé sous la garde des professionnels de santé, le dossier médical personnel est entretenu par les professionnels de santé mais gardé par les hébergeurs. C'est pourquoi, en cas de divulgation des informations contenues dans le DMP, le professionnel de santé ne devrait pas être inquiété ; à la limite, un partage de responsabilité pourrait être envisagé avec l'hébergeur ; sauf s'il est prouvé que la fuite est de son fait. De plus, cette situation allège l'obligation de communication[1066] des professionnels de santé dans le DMP, vis-à-vis des patients puisque ces derniers ont un accès direct à leur dossier et qu'ils peuvent prendre l'initiative de communiquer le contenu à des tiers. Ils gèrent, dans une certaine mesure, le partage du secret médical en fixant les limites du contenu communicable en ce sens que c'est sur leur autorisation et pour les informations qu'ils voudront bien mettre à leur disposition que les intervenants ultérieurs pourront consulter le dossier. Le patient devenant ainsi un acteur de sa prise en charge et disposant du droit de révéler des informations de son dossier médical en devient plus responsable que les professionnels de santé. Mais ces derniers ne sont pas, pour autant, complètement exonérés de leur obligation. Le professionnel de santé reste tenu d'une obligation de moyens que le juge appréciera, en cas de contentieux, en vérifiant qu'il a mis en œuvre tous les moyens nécessaires pour apporter au patient les soins adéquats. Il ne pourra pas lui être reproché de ne pas avoir eu connaissance des renseignements dissimulés par le patient et il pourra en faire la preuve par les traces des accès au dossier médical personnel. En revanche, le mode de communication et de stockage dématérialisé propre au DMP, même s'il restreint les possibilités d'erreur de diagnostic grâce à la grande étendue des informations auxquelles un

---

[1066] « *Les établissements de santé, publics ou privés, sont tenus de communiquer aux personnes recevant ou ayant reçu des soins sur leur demande, les informations médicales définies à l'article L 1111-7. Les praticiens qui ont prescrit l'hospitalisation ont accès sur leur demande, à cette information. Cette communication est effectuée au choix de la personne concernée, directement ou par l'intermédiaire d'un médecin qu'elle désigne*.» Article L 1112-1 du code de la santé publique.

L'article L 1111-7 du 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'examens, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mises en œuvre, 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. Elle peut accéder à ces informations directement ou par l'intermédiaire d'un médecin qu'elle désigne et en obtenir communication, dans des conditions définies par voie réglementaire au plus tard dans les huit jours suivant sa demande et au plus tôt après qu'un délai de réflexion de 48 heures aura été observé. Ce délai est porté à deux mois lorsque les informations médicales datent de plus de cinq ans ou lorsque la Commission départementale de soins psychiatriques est saisie en application du quatrième alinéa.»*

professionnel peut accéder sur l'état de santé d'un patient, fait peser, par la même occasion, une présomption défavorable de connaissance du dossier rendant les jugements plus sévères en cas d'erreur. L'erreur de diagnostic est assimilée à la faute professionnelle. La dématérialisation entraîne également l'apparition de nouvelles incriminations pénales à leur charge, notamment des infractions relatives à l'informatique, aux fichiers et aux libertés précitées. Elles prévoient des sanctions aggravées s'agissant de la violation du secret professionnel.

Dans le dispositif du dossier médical personnel le professionnel de santé qui tient à jour le dossier agit en tant que mandataire du patient. Il est tenu de consulter et de mettre à jour DMP après l'accord du patient. Le professionnel de santé agit donc au nom et pour le compte du patient, mais il peut engager sa responsabilité sur le contenu du dossier car il dispose seul des compétences requises pour honorer son obligation de mise à jour. Dès lors, le professionnel doit, non seulement répondre de ses agissements dans l'exécution du contrat de mandat à l'égard du patient, mais il risque, également, sa responsabilité du fait de l'exercice de son art. Les mentions qui figurent dans le dossier restent l'expression de son indépendance professionnelle. D'ailleurs, le refus par un professionnel de santé de reporter dans le dossier médical personnel les éléments issus de chaque acte ou consultation, dès lors que le patient ne s'y est pas explicitement opposé , peut faire l'objet d'une pénalité prononcée par le directeur de l'organisme local de l'assurance-maladie ou de la caisse d'assurance retraite et de la santé au travail[1067].

La loi du 13 août 2004 relative à l'assurance maladie désigne le médecin traitant comme participant à la mise en place et à la gestion du dossier médical personnel[1068]. Parmi les personnes autorisées à consulter le dossier médical personnel, le médecin traitant dispose d'un statut particulier. Il dispose de droits supplémentaires au regard des autres médecins et assiste le patient dans la gestion de son DMP et l'exercice de ses droits à défaut d'accès direct par Internet. Selon le portail dédié au dossier médical personnel, cela lui permet, de consulter l'historique des accès y compris ceux des autres professionnels de santé, d'accéder à tous les documents (même masqués), de bloquer, à la demande du patient l'accès de son dossier à un professionnel de santé antérieurement autorisé et même de transférer le statut de médecin traitant à un autre, à la demande du titulaire du dossier. Toutes ces prérogatives ont pour

[1067] Article L 162-1-14 du code de la sécurité sociale.

[1068] Article 7. Article L 162-5-3 du code de la sécurité sociale.

conséquence de faire peser sur ce professionnel de santé une plus grande responsabilité non seulement quant au contenu du DMP mais également à sa confidentialité comme tous les intervenants dans le système.

Initialement, le médecin traitant est comme tous ceux qui embrassent la fonction, celui qui procure des soins et conseille le patient. Limité à ce rôle, ce professionnel de santé n'engage pas plus de responsabilité civile[1069] que les autres sauf s'il est démontré que sa négligence a eu un effet néfaste sur la continuité des soins de son patient par un de ses confrères[1070]. Le médecin traitant doit aussi tenir à jour une fiche d'informations sur chaque patient comme tout médecin ou professionnel de santé. Dans le DMP, la première responsabilité du médecin traitant découle des informations qu'il y inscrit et de leur actualité. En effet, il pourrait faire l'objet de poursuites en cas de retard dans la mise à jour ou d'erreurs dans les renseignements qu'il a inscrits dans le dossier de son patient si cela avait une répercussion sur la coordination des soins du patient. Avant le déploiement du DMP, l'arrêté du 3 février 2005[1071] rappelait pour tous les médecins conventionnés, l'obligation de mettre à jour le dossier médical personnel des patients qu'ils prennent en charge. Il préparait particulièrement les médecins traitants à cette tâche en prescrivant : «*dans l'attente de la mise en œuvre du DMP, le médecin traitant établit son dossier médical en conformité avec le parcours de soins coordonné. A cet effet, ce dossier comporte les éléments d'information suivants : une synthèse actualisée des éléments du dossier nécessaires à la continuité des soins; les protocoles de soins, (...) ; les documents transmis par les professionnels participants à la continuité et à la coordination des soins (...); les éléments ainsi colligés dans le dossier doivent permettre d'attester de la réalité de la coordination assurée par le médecin traitant*.[1072] »

[1069] Depuis l'arrêt Mercier du 20 mars 1936, il est établi une relation contractuelle (contrat médical) entre le soignant et le soigné engageant la responsabilité civile du médecin en cas de faute. Le juge évalue pécuniairement le dommage en tenant compte de la gravité de l'atteinte à la vie privée, du caractère confidentiel des faits révélés et des personnes auxquelles la divulgation a été faite. Cour de Cassation, chambre civile, 20 mars 1936. Droit pénal, 1936, 1, p. 88.

[1070] Cour de Cassation, 25 mai 1971. n° 69-14266. Bulletin des arrêts de la Cour de Cassation chambre civile 1 N. 171. p. 144. La Cour de Cassation a rejeté le pourvoi formé contre l'arrêt qui jugeait le Dr X responsable du décès d'une patiente des suites d'une hémorragie survenue après sa huitième couche parce qu' en sa qualité de médecin traitant, le Dr X. connaissait parfaitement les antécédents de la patiente et qu'il lui appartenait d'assurer la continuité de ses soins.

[1071] Arrêté du 3 février 2005 *portant approbation de la convention nationale des médecins généralistes et des médecins spécialistes.* JORF n° 35 du 11 février 2005. p. 2275. Texte n° 4. NOR: SANS0520354A.

[1072] Point 1.4.3 de l'arrêté du 3 février 2005 *portant approbation de la convention nationale des médecins généralistes et des médecins spécialistes.*

La responsabilité du médecin traitant en tant que garant de la coordination des soins aurait pu faire peser sur celui-ci une obligation d'information et une responsabilité supplémentaire due au contenu ajouté par ses confrères. Mais, l'article L 161-36-2 du code de la sécurité sociale l'exonère de cette responsabilité supplémentaire en indiquant « *(...), Chaque professionnel de santé, exerçant en ville ou en établissement de santé, quel que soit son mode d'exercice reporte dans le dossier médical personnel, à l'occasion de chaque acte ou consultation, les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins de la personne prise en charge. Entre autre, à l'occasion du séjour des patients, les professionnels de santé habilités des établissements de santé reportent sur le dossier médical personnel les principaux éléments résumés relatifs à ce séjour* ». Il apparaît donc que le médecin traitant n'est pas le seul transcripteur des informations de données de santé dans le dossier médical personnel mais en tant que référent du patient il pourrait bien avoir à lui expliquer les données inscrites par ses confrères. Pourrait-il, dans ces conditions, engager sa responsabilité en cas d'interprétation erronée ? La législation relative au dossier médical personnel ne permet pas de répondre à cette question. Mais, la possibilité de retenir la responsabilité du médecin traitant est envisageable dans la mesure où le code de la santé publique et les règles de déontologie médicale imposent à celui qui exerce la médecine d'avoir les connaissances requises ou, à tout le moins, de diriger le patient vers une personne plus qualifiée.

Le sujet de la responsabilité du médecin traitant par rapport aux transcriptions de ses confrères mérite d'être clarifié par le droit positif. Le texte de la loi du 13 août 2004 et celui de l'arrêté du 3 février 2005 qui fondent les missions du médecin traitant dans le processus de déploiement du dossier médical personnel semblent véhiculer deux idées divergentes. Alors que la loi autorise chaque professionnel de santé à *reporter dans le dossier médical personnel les éléments diagnostiques et thérapeutiques nécessaires à la coordination des soins,* l'arrêté cite au nombre des missions[1073] du médecin traitant le fait de *favoriser la coordination par la*

[1073] « *Les missions du médecin traitant :*
- *assurer le premier niveau de recours aux soins ;*
- *orienter le patient dans le parcours de soins coordonnés et informer tout médecin correspondant des délais de prise en charge compatibles avec l'état de santé du patient ;*
- *assurer les soins de prévention (dépistage, éducation sanitaire, etc.) et contribuer à la promotion de la santé;*
- *contribuer à la protocolisation des soins de longue durée, en concertation avec les autres intervenants ; la rédaction de protocole est faite par le médecin traitant (généraliste ou spécialiste) en liaison ou selon la proposition du ou des médecins correspondants participant à la prise en charge du malade;*
- *favoriser la coordination par la synthèse des informations transmises par les différents intervenants et l'intégration de cette synthèse dans le DMP;*

synthèse des informations transmises par les différents intervenants et l'intégration de cette synthèse dans le dossier médical personnel. L'interprétation de ce second texte donne à déduire que, les autres intervenants ne peuvent pas transcrire directement des informations dans le dossier médical personnel. Ils doivent les transmettre au médecin traitant qui aura la charge d'en faire une synthèse et de les intégrer au dossier. Il s'ensuit que l'étendue de la responsabilité du médecin traitant diffère d'une disposition à l'autre. En principe, l'arrêté est une décision exécutoire censée donner des précisions quant à l'application d'une loi, mais en cas de discordance, l'interprétation de la loi en tant que règle supérieure devra l'emporter. Dès lors, nous retiendrons que le médecin traitant ne devra pas engager sa responsabilité pour les informations introduites dans le dossier médical personnel par ses confrères.

L'obligation d'information qui pèse sur le médecin traitant induit une obligation de conseil vis-à-vis du patient. Or, le médecin traitant a accès à toutes les données du patient et compris celles qui sont masquées par ce dernier dans le DMP. Si, en usant de son droit de masquage à l'égard d'un autre médecin le patient subit des préjudices dans le traitement prescrit par le professionnel de santé du fait du manque d'information, un médecin traitant peut-il voir sa responsabilité engagée sur la base de son obligation de conseil ? Le dispositif mis en place pour la gestion du dossier médical personnel rend, désormais le patient responsable de la garde de ses informations personnelles de santé contrairement à l'ancienne conception du dossier médical placé sous la responsabilité des professionnels et établissements de santé. De ce fait, le médecin traitant peut se dédouaner s'il prouve que le patient a eu recours aux services de ce confrère sans le consulter ou qu'il a masqué ces informations sans son avis alors qu'elles étaient importantes pour une meilleure prise en charge. Compte tenu de la grande responsabilité du médecin traitant dans la gestion du DMP et pour permettre au patient d'être en mesure d'exercer pleinement ses droits, la CNIL a insisté sur la nécessité d'informer clairement ce dernier du rôle et des prérogatives de son médecin traitant dans le cadre d'un DMP et de la portée de la désignation d'un médecin traitant[1074].

– *apporter au malade toute information permettant d'assurer une permanence d'accès aux soins aux heures de fermeture du cabinet.*»

1.1.1 de l'arrêté du 3 février 2005 portant approbation de la convention nationale des médecins généralistes et des médecins spécialistes.

[1074] CNIL. *Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel*. [en ligne], disponible sur: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516. Consulté le 20 décembre 2013.

Finalement, notons que pour garantir la confidentialité des données médicales dans le contexte des nouveaux enjeux que soulève le dossier médical personnel, par le large partage du secret professionnel, les règles qui régissent la responsabilité médicale n'ont pas véritablement changé. Mais force est de constater que dans leur application, les causes de responsabilisation des professionnels (hébergeurs et professionnels de santé) se sont multipliés. Il persiste de nombreuses zones d'ombre entre les textes et dans la plupart des cas c'est la jurisprudence qui devra trancher. Dans ce domaine, également l'on pourrait être mieux fixé avec le décret d'application relatif au dossier médical personnel s'il était pris. Le retard que prend cette disposition ayant un impact sur le déploiement du DMP, les droits des patients et les responsabilités des intervenants, l'État pourrait engager sa responsabilité. Le Conseil d'État a déjà prononcé des sanctions allant dans ce sens à l'encontre de l'État, notamment en juillet 2000, relativement à la prise tardive par le Premier ministre de décrets prévus par la loi du 3 janvier 1986[1075]. « *En dépit des difficultés rencontrées par l'administration dans l'élaboration de ce texte, son abstention à le prendre s'est prolongé très largement au-delà d'un délai raisonnable (...)* » Pour être fondé, le requérant devra prouver que le retard du décret d'application concernant le DMP lui a porté un préjudice spécial et grave.

La limitation des accès au dossier médical personnel participe de la garantie de confidentialité de son contenu car plus les accès sont nombreux plus grands sont les risques de divulgation.

Paragraphe 2 : l'accès limité au DMP

L'article L 1110-4 alinéa 4 du code de la santé publique dispose que « *la personne, dûment informée, peut refuser à tout moment que soient communiquées des informations la concernant à un ou plusieurs professionnels de santé* ». En dehors de la solution d'un refus express communiqué au professionnel de santé qui le prend en charge, le patient peut exercer cette faculté en bloquant l'accès à son dossier médical personnel à certaines personnes.

L'article L 1111-15, alinéa 2 du code de la santé publique prévoit que l'accès au dossier médical personnel des professionnels mentionnés au premier alinéa est subordonné à

[1075] Conseil d'État, 6/4 SSR, du 28 juillet 2000, n° 204024 publié au recueil Lebon.

l'autorisation du patient d'accéder à son dossier. L'article L 1111-16 d'ajouter que le médecin coordonnateur des établissements mentionnés à l'article L 313-12 du code de l'action sociale et des familles a accès au dossier médical personnel de la personne hébergée dans l'établissement sous réserve de l'accord de celle-ci ou de son représentant légal. Autrement dit, la loi donne, implicitement, la possibilité au patient de refuser l'accès de son dossier médical personnel à un professionnel de santé tout comme à toute autre personne. Les conditions et modalités d'exercice de ce droit reconnu au patient de limiter les accès à son dossier sont prévues par le code de la santé publique qui édicte également des limitations d'office sans rapport avec la volonté du concerné.

A.La limitation d'accès par le titulaire du DMP

Le patient est autorisé à refuser de façon expresse l'accès à son dossier médical mais il dispose également d'un droit de refus tacite qu'il exprime à travers son droit de masquage.

1. La limitation par le refus express d'autorisation d'accès

Le droit de refus d'accès à son dossier reconnu au patient est limité par des autorisations légales d'accès.

a. La mise en œuvre du refus express d'autorisation d'accès

Le patient peut limiter l'accès à son dossier médical personnel en temps réel à l'occasion d'un acte ou d'une consultation. Mais il peut exprimer son refus a priori, de sorte que son dossier ne puisse être consulté même après son décès.

A l'occasion d'une consultation, le professionnel de santé demandera au patient son autorisation pour accéder à son dossier médical personnel. Cet accord est requis pour chacun des intervenants lorsque le patient est pris en charge par une équipe. « *Le professionnel de santé recueille, après avoir informé la personne concernée, son consentement pour qu`un autre professionnel de santé à qui il serait nécessaire de confier une partie de la prestation*

accède à son dossier médical personnel et l'alimente[1076].» Le consentement obtenu, le professionnel cochera la case prévue à cet effet dans le dossier et consultera les informations et/ou ajoutera des documents médicaux. Aucun document papier ne sera délivré pour attester de ce consentement exprimé par la remise de la carte vitale 2[1077]. Mais si ce dernier décide d'empêcher qu'un professionnel de santé accède à son dossier, le système met à sa disposition l'annuaire des professionnels de santé habilités et lui donne la possibilité de bloquer l'accès à celui ou ceux qu'il aura indiqué(s) sans avoir à se justifier. Le patient délivre les interdictions d'accès à l'encontre d'un professionnel de santé par l'inscription de celui-ci sur la liste des médecins « *non autorisés* ». Cette faculté s'exerce directement par le patient lorsqu'il en a les moyens, ou par l'intermédiaire du médecin traitant, dans le cas contraire[1078].

Lorsqu'une personne est hospitalisée, elle peut donner l'autorisation à l'établissement qui la reçoit d'accéder à son dossier médical personnel. C'est ainsi, à toute l'équipe de soins qu'elle autorise l'accès conformément aux termes de l'article L 1110-4, alinéa 3 du code de la santé publique. Mais, ce patient est habilité à bloquer l'accès à son dossier médical personnel à une personne appartenant à l'équipe de soins parce qu'elle ne souhaite pas qu'elle puisse y accéder. Les autres membres de l'équipe pourront consulter le dossier et ces accès seront tracés dans le dossier médical personnel. Par contre, dans le cas des malades hospitalisés sans consentement, notamment pour des soins psychiatriques, l'accès aux informations par le patient concerné peut être autorisé, seulement en présence d'un médecin désigné par le demandeur s'il est établi qu'il y a des risques d'une particulière gravité[1079].

[1076] Article L 1111-17, II du code de la santé publique

[1077] Les autorisations d'accès sont valables un an et sont renouvelables. Si le patient dispose d'un accès informatique personnel à son dossier, il pourra lui-même gérer les droits d'accès à son DMP. A défaut la gestion de ses habilitations sera effectuée par les professionnels de santé qui se déclareront autorisées par le patient à sa demande à l'aide d'une case à cocher. CNIL. *Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel*. [en ligne], http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516. Consulté le 15 janvier 2014.

[1078] L'Asip santé envisage de prévoir, dans une version ultérieure du DMP, de notification par mails aux patients qui le souhaitent les ajouts et retraits de la liste des professionnels autorisés et du médecin traitant. Cette mesure sera de nature à améliorer les conditions de contrôle a posteriori des patients qui disposent d'un équipement informatique et d'un accès Internet. CNIL. *Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel*. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516. Consulté le 15 janvier 2014.

[1079] Article L 1111-7 alinéa 4 du code de la santé publique.

Le patient à la possibilité, à tout moment, de mettre fin à une autorisation d'accès précédemment accordée. Il peut également exprimer son opposition a priori comme cela est implicitement admis par l'article L 1111-17 du code de la santé publique. « *Les professionnels de santé accèdent au dossier médical personnel d'une personne hors d'état d'exprimer sa volonté, en présence d'une situation comportant un risque immédiat pour sa santé, sauf si cette personne avait auparavant manifesté son opposition expresse à ce que son dossier soit consulté ou alimenté dans une telle situation.*
Le médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente qui reçoit un appel concernant une personne accède, sauf si cette personne avait auparavant manifesté son opposition expresse à ce que son dossier soit consulté dans une telle situation, au dossier médical personnel de celle-ci.» Mais, il arrive rarement qu'une personne se soucie de l'état de son dossier médical avant de se retrouver dans une situation critique. C'est pourquoi cette possibilité d'expression de son avis, a priori paraît bien plus théorique que réelle. Dans la pratique, les autorités compétentes privilégient l'état de nécessité, l'intérêt général ou l'urgence par rapport à la volonté de l'individu.
Le portail dédié au dossier médical personnel encourage plutôt le patient à autoriser a priori, ces accès pendant les situations d'urgence, au moment de la création de son dossier.

L'expression de la volonté du mineur ou du majeur incapable est exprimée par le titulaire de l'autorité parentale[1080] ou le tuteur. « *L'accès aux informations relatives à la santé d'une personne, (...) détenues un professionnel de santé, un établissement de santé ou un hébergeur agréé en application de l'article L 1111-8, est demandée par la personne concernée, son ayant droit en cas de décès de cette personne, la personne ayant l'autorité parentale, le tuteur ou, le cas échéant, par le médecin qu'une de ces personnes a désigné comme intermédiaire.*[1081] » L'accès au dossier médical du patient mineur est réservé aux seuls titulaires de l'autorité parentale, à l'exclusion du mineur lui-même ou d'un autre adulte désigné

[1080] Si la demande de communication de son dossier émane d'un mineur, l'arrêté du 5 mars 2004 rappelle que l'article L 1111-7 n'a pas prévu que le mineur soit titulaire du droit d'accès aux informations détenues par les professionnels et établissements de santé. Mais la loi (article L 1111-2 du code de la santé publique et article 371-1 du Code civil) prévoit que le mineur a le droit de recevoir lui-même une information et de participer à la prise de décision le concernant d'une manière adaptée à son degré de maturité. Il est donc souhaitable qu'une attention particulière soit portée à une telle demande d'accès aux éléments du dossier. Elle doit permettre au mineur de compléter l'information reçue et de bénéficier d'explications supplémentaires, compte tenu de l'âge atteint lorsqu'il effectue sa demande. Il peut être très utile de reprendre avec lui les éléments de son dossier et leurs incidences sur sa vie d'adulte.

[1081] Article R 1111-1 du code de la santé publique.

par ce dernier[1082]. Par contre, le mineur peut refuser l'accès de ses informations de santé à son représentant légal. L'article L 1111-5 du code de la santé publique permet aux mineurs qui souhaitent garder le secret, d'obtenir que le médecin accepte de pratiquer des soins nécessaires pour sauvegarder sa santé sans avoir le consentement du ou des titulaires de l'autorité parentale. Dans ces conditions l'article R 1111-6 prévoit que le mineur peut s'opposer à la communication des informations correspondant à cette situation particulière aux détenteurs de l'autorité parentale. L'opposition du mineur est alors consignée au dossier et, en cas de demande d'accès par le représentant légal, le professionnel doit s'efforcer de convaincre le mineur de lever son opposition. En acceptant de revenir sur son opposition, le mineur peut demander que le droit d'accès du représentant légal soit exercé par l'intermédiaire du médecin désigné par ce dernier. L'opposition ou la limitation ne peut concerner que l'un des deux parents. Le fait de passer outre à l'opposition du mineur est susceptible d'engager la responsabilité pénale et administrative du professionnel de santé sur la base de la violation du secret professionnel. Le Conseil d'État a confirmé le 17 novembre 2006[1083] la décision de la juridiction administrative rejetant la requête d'une mère voulant prendre connaissance du contenu du dossier médical de sa fille mineure sans son consentement. La décision était fondée sur la considération de droit dont jouit tout mineur au secret des informations concernant sa santé. En juillet 2008, la Commission d'accès aux documents administratifs (CADA) a rendu un avis[1084] précisant, cependant, que le mineur ne pourrait s'opposer à la

[1082] Lorsque le juge des enfants a confié un mineur à un tiers digne de confiance dans le cadre de mesure d'assistance éducative, les parents continuent, en application des dispositions de l'article 375-7 du code civil, d'exercer tous les attributs de l'autorité parentale qui ne sont pas inconciliables avec cette mesure. En principe, la personne désignée tiers digne de confiance n'a donc pas accès, en cette seule qualité, au dossier médical du mineur qui lui a été confié. Il ne pourrait être communiqué à la personne désignée tiers digne de confiance que si celle-ci est en mesure de justifier d'un mandat express consenti par les parents du mineur, détenteurs de l'autorité parentale (Conseil d'État , 6 septembre 2005, Conseil national de l'Ordre des médecins, n° 270234). Le juge des enfants peut décider d'autoriser la personne à qui est confié l'enfant à exercer un acte relevant de l'autorité parentale, en cas de refus abusif ou injustifié ou en cas de négligence des détenteurs de l'autorité parentale, à charge pour le demandeur de rapporter la preuve de la nécessité de cette mesure. Le juge pourrait ainsi autoriser la personne désignée tiers de confiance à accéder au dossier médical du mineur dont elle a la charge sous réserve que les conditions prévues par ces dispositions soient réunies. CADA. Conseil. Centre hospitalier intercommunal Robert Ballanger 20 juin 2013. n° 20130367. Recueil des principaux avis et Conseils 1er semestre 2013. pp. 9-10. www.cada.fr. Consulté le 12 décembre 2013.

[1083] Conseil d'État. 10ème et 9ème sous-section réunies, 17 novembre 2006. Décision n° 270863. Inédit au recueil Lebon. www.legifrance.gouv.fr

[1084] CADA. Directeur général de l'Assistance Publique-hôpitaux de Paris (groupe hospitalier Cochin-Saint-Vincent-de-Paul/Maison de Solenn). Séance du 3 juillet 2008. Avis n° 20082236. http://www.cada.fr/avis-20082236,20082236.html. Consulté le 28 mai 2014.
Seuls les parents mineurs d'un enfant ont le droit d'accès à son dossier médical. Les grands-parents de celui-ci, qui ne sauraient détenir directement l'autorité parentale sur lui et qui, bien qu'ils représentent légalement le père ou la mère mineur n'ont pas vocation à l'exercer en leur nom, n'ont aucun droit d'accès au dossier de l'enfant.

communication de son dossier médical au titulaire de l'autorité parentale que dans les cas où les soins qu'il a reçus ont été dispensés sans son consentement ou à son insu. La Commission a donc fait droit à la demande d'un père qui s'est vu refuser la communication du dossier médical de sa fille, sur demande de celle-ci alors qu'il était présent lors de l'admission au centre hospitalier et s'était entretenu avec plusieurs médecins sur son état de santé.

Seule une personne justifiant légalement de la qualité de tuteur est autorisée à accéder au dossier médical du majeur sous tutelle. La tutelle est la seule mesure de protection de la personne visée par le code de la santé publique. Les dispositions relatives à l'accès au dossier médical du majeur incapable ne concernent pas les autres mesures comme la sauvegarde de justice ou la curatelle. La Commission d'accès aux documents administratifs a précisé que le code de la santé publique ne comporte aucun droit d'accès particulier au profit du curateur d'une personne faisant l'objet d'une mesure de curatelle renforcée. Dans ces conditions le curateur ne peut prétendre exercer de plein droit le droit d'accès de sa pupille à son dossier médical. Ce n'est que si cette dernière lui a délivré un mandat express en ce sens[1085] que son dossier médical peut être transmis au curateur[1086]. Mais il arrive que la personne ne soit en état ni d'accéder directement à ses informations médicales, ni de désigner un tel mandataire. Dans ces conditions, à l'exception des cas dans lesquels le patient a donné un mandat express à un tiers ou fait l'objet d'une mesure de tutelle, aucune disposition du code de la santé publique ne permet à un médecin, ni directement ni par l'intermédiaire de la famille ou des proches du patient de prendre connaissance du dossier médical de celui-ci[1087].

CADA. *Directeur du centre hospitalier René Dubos*. Conseil n° 20103989. Séance du 14 octobre 2010. www.cada.fr

[1085] Dans une décision du 26 septembre 2005, le Conseil d'État statuant au contentieux a interprété les dispositions de l'article L 1111-7 du code de la santé publique comme n'excluant pas la possibilité pour le patient de recourir à un mandataire pour accéder à ses informations de santé dès lors que ce dernier peut justifier de son identité et dispose d'un mandat express, c'est-à-dire dûment justifié. Conseil d'État. 26 septembre 2005, *Conseil national de l'ordre des médecins*. 1ère et 6ème sous-sections réunies. 26 septembre 2005. Décision n° 270234 publié au Recueil Lebon.

[1086] CADA. *Directeur du centre hospitalier de Strasbourg*. Conseil n° 20053559. Séance du 6 Octobre 2005. www.cada.fr
Une mère curatrice de son fils s'est vue refuser la communication du dossier médical de ce dernier en l'absence d'un mandat de sa part l'autorisant à accéder au dossier médical. Saisie de la demande, la Commission d'accès aux documents administratifs a rendu une décision défavorable en rappelant que le curateur ne peut prétendre exercer de plein droit le droit d'accès de sa pupille à son dossier médical. CADA. *Directeur du centre hospitalier spécialisé de l'Yvonne*. Avis n° 20083853. Séance du 9 Octobre 2008. www.cada.fr

[1087] CADA. *Centre hospitalier universitaire (CHRU) de Montpellier*. Conseil n° 20131183. Séance du 28 mars 2013. www.cada.fr

b. Les accès légaux sans recours au consentement du patient

Le consentement du titulaire du dossier médical personnel privilégié dans le pouvoir de limitation des accès est contrebalancé par un certain nombre d'autorisations d'accès légales sans l'accord de ce dernier. Deux hypothèses sont envisagées par l'article L 1111-17 du code de la santé publique du vivant de l'intéressé : la situation où la santé de la personne concernée est en péril alors qu'elle n'est pas en état de donner un avis et dans la situation d'un appel d'urgence. «*Les professionnels de santé accèdent au dossier médical personnel d'une personne hors d'état d'exprimer sa volonté, en présence d'une situation comportant un risque immédiat pour sa santé, (...). Le médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente qui reçoit un appel concernant une personne accède,(...), au dossier médical personnel de celle-ci.*» Bien qu'il soit subtilement permis au patient d'exprimer son opposition avant que la situation ne se présente, le principal motif d'une telle possibilité de contournement de sa volonté est ce qu'on pourrait assimiler à l'état de nécessité face auquel la volonté exprimée pourrait ne pas être prise en compte. C'est une cause exonératoire de responsabilité en ce sens que l'infraction est justifiée par la volonté d'empêcher la réalisation d'un dommage beaucoup plus grave. Dans la situation du patient, son état de santé constitue un intérêt supérieur qui, pour le législateur mérite que l'on viole une liberté fondamentale. Les intentions du législateur sont louables dans la mesure où elles privilégient la vie de l'individu qui est en elle-même, la première valeur fondamentale. Lorsque l'état du patient comporte un risque immédiat pour sa santé, tout professionnel de santé peut consulter son DMP en mode « *bris de glace* ». Le professionnel authentifié avec sa carte CPS justifie techniquement le motif de cette intrusion dans le DMP.

Pour assurer la protection des données du patient, le centre des urgences et le médecin régulateur seront identifiés comme tels par l'hébergeur et toutes les activités sur le dossier seront tracées et communiquées au patient. L'identification du patient par téléphone peut poser des problèmes de disponibilité ou d'erreur de transmission des mentions de son identifiant de santé qui pourraient être à l'origine de difficultés d'accès ou de confusion de dossiers. C'est pourquoi, le médecin régulateur peut accéder au DMP du patient via le logiciel du centre de régulation sans disposer de la carte vitale du patient. Mais, l'on peut craindre des cas d'abus de droit. Des personnes mal intentionnées seraient tentées de profiter de la situation pour accéder à son dossier médical personnel en vue de prendre connaissance de certaines informations qui ne sont pas forcément nécessaires à la prise en charge immédiate. D'ailleurs,

le décret sur la DMP attendu, devrait organiser cette consultation de sorte que ne soient accessibles que les éléments qui sont indispensables pour les soins imminents. En décembre 2010, la délibération de la CNIL déclarait que le patient aurait la possibilité d'interdire l'accès en mode «bris glace» (urgence ou SAMU) à son DMP dans les paramétrages de son compte d'accès Internet ou en s'adressant à un professionnel de santé, conformément aux dispositions de l'article L 1111-17 du code de la santé publique. Aucun détail supplémentaire n'avait été donné quant aux modalités d'application de cette faculté.

Le consentement du titulaire du dossier médical personnel n'est pas requis non plus dans l'hypothèse d'une demande d'accès faite par ses ayants droits après son décès. Aux termes des articles L 1111-18 in fine et L 1110-4 du code de la santé publique, les ayants droits peuvent solliciter l'accès au dossier de la personne décédée si cela leur est nécessaire pour permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits sans préjudice du secret médical. Comme dans les hypothèses précédentes, la loi tient compte de l'opposition exprimée par celui-ci antérieurement à sa mort. L'accès à ce dossier peut également intervenir dans le cadre d'une expertise médicale diligentée aux fins d'administration de la preuve[1088]. Le Conseil d'État[1089] a fait une interprétation stricte de ces dispositions en déclarant que le législateur a entendu autoriser la communication aux ayants droits d'une personne décédée des seules informations nécessaires à la réalisation de l'objectif poursuivi par ses ayants droits, à savoir la connaissance de cause de la mort, la défense de la mémoire du défunt ou la protection de leurs droits. Dès lors, la communication aux ayants droits ne doit porter que sur les informations qui vont dans ce sens et non sur l'ensemble des informations figurant dans le dossier médical du défunt[1090]. Doivent être considérés, en premier lieu comme des ayants droits au sens de ces dispositions les successeurs légaux et testamentaires du défunt à l'exclusion de toute autre catégorie de tiers tels que la famille et les proches conformément aux articles 731 et suivants du code civil. Ainsi, le fait pour la sœur d'une patiente décédée d'avoir été désignée par la défunte comme personne de confiance ne lui

[1088] Article L 1111-18 alinéa 6 du code de la santé publique.

[1089] Conseil d'État. 26 septembre 2005, *Conseil national de l'Ordre des médecins*. 1ère et 6ème sous-sections réunies. 26 septembre 2005. Décision n° 270234 publié au Recueil Lebon.

[1090] « *L'ayant droit qui se trouve dans cette situation a accès aux seuls éléments du dossier médical nécessaires à la réalisation d'un tel objectif* ». Arrêté du 3 janvier 2007, article 2. Arrêté du 3 janvier *2007 portant modification de l'arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès*. JORF n° 13 du 16 janvier 2007 p. 982. Texte n° 32. NOR: SANP0720101A.

confère pas cette qualité lui ouvrant droit à la communication du dossier médical de celle-ci à moins qu'elle ne démontre sa qualité d'ayant droit par tout moyen, notamment, par un acte de notoriété ou par un certificat d'hérédité[1091].

2. Le droit de masquage

L'article 55 de la loi[1092] du 19 décembre 2007 (transféré par la loi[1093] du 21 juillet 2009), a introduit le principe du masquage. L'ancien article L 161-36-4, alinéa 1 du code de la sécurité sociale disposait jusqu'au 22 décembre 2007 : «*un décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé, fixe les conditions d'application des articles L 161-36-1 à L 161-36-3-1 et notamment les conditions d'accès aux différentes catégories d'informations qui figurent au dossier médical personnel* ». Après avoir été complétée par la loi du 19 décembre 2007, cette disposition va être transférée à l'article L 1111-21 du code de la santé publique par la loi du 21 juillet 2009. C'est la codification du choix qu'a un patient de ne pas révéler à son professionnel de santé des informations même si celles-ci peuvent se révéler utiles à l'établissement d'un diagnostic ou à la détermination du meilleur traitement. Ainsi, dispose l'article L 1111-21 du code de la santé publique : « *un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et des conseils nationaux de l'ordre des professions de santé, fixe les conditions d'application des articles L 1111-14 à L 1111-19 et notamment les conditions d'accès aux différentes catégories d'informations qui figurent au dossier médical personnel, les conditions dans lesquelles certaines informations peuvent être rendus inaccessibles par le titulaire du dossier médical personnel ou son représentant légal ainsi que les modalités selon lesquelles le professionnel de santé accédant*

[1091] CADA. *Directeur du centre hospitalier régional d'Orléans*. Avis n° 20100697. Séance du 25 février 2010. www.cada.fr
Les dossiers médicaux deviennent librement communicables à toute personne (y compris celles qui ne justifient pas de la qualité d'ayant droit) à l'expiration d'un délai de 25 ans à compter du décès d'une personne, ou 120 ans à compter de la date de sa naissance si la date de son décès n'est pas connue, en vertu du 2° du I de l'article L 213-2 du code du patrimoine.

[1092] 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. Texte n° 2. NOR: BCFX0766311L.

[1093] 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. Texte n° 1. NOR: SASX0822640L

au dossier médical personnel a connaissance de l'inscription au dossier d'informations rendues inaccessibles par son titulaire ou son représentant légal. » Plusieurs avantages peuvent être vus dans ce droit accordé aux patients mais, sa mise en œuvre suscite de nombreux doutes.

a. La mise en œuvre du droit de masquage

Pour la mise en application de l'article L 1111-21, un avant-projet de décret sur le DMP avait été rédigé par le GIP-DMP, puis mis en ligne sur le portail dédié au DMP pour consultation publique le 31 octobre 2006[1094]. Il précisait en son article 17 : « *le titulaire, ou l'un des titulaires de l'autorité parentale, ou son tuteur, peut rendre des informations inaccessibles à tout ou partie des professionnels de santé susceptibles de les consulter à l'exception de l'auteur de la donnée visée. Cette restriction n'est pas mentionnée dans le dossier médical personnel. Elle peut être levée à tout moment. Si le titulaire, ou l'un des titulaires de l'autorité parentale ou son tuteur le décide, les données relevant de certaines spécialités thérapeutiques sont placées dans des zones du dossier médical personnel qui ne sont accessibles qu'aux médecins exerçant dans ces spécialités. La liste de ces spécialités est définie par arrêté du ministre chargé de la santé et de la sécurité sociale*. » Le droit de masquage dans le dossier médical personnel est donc la possibilité qu'a un patient de pouvoir rendre un document inaccessible dans son dossier. Un document masqué reste, néanmoins visible à son auteur et au médecin traitant du patient tout comme au patient lui-même (ces filtres sont faits automatiquement par le dossier médical personnel et n'ont pas d'impact sur le logiciel de professionnel de santé ou le système d'information hospitalier, car le masquage est masqué). Le masquage peut également être réalisé par tout professionnel de santé à la demande du patient. Le masquage est réversible car le patient peut retirer le masquage d'un document aux professionnels de santé. Quant au démasquage, il peut être réalisé par les médecins traitants pour tous les documents et par les autres professionnels de santé pour les documents dont ils sont les auteurs. Il ne faut pas confondre le masquage et l'effacement de données. Si, le patient peut masquer des données dans le DMP, il ne peut les effacer. Cet acte

[1094] Direction de l'information légale. *Dossier médical personnel: vos avis sur son contenu*. 7 novembre 2006. http://www.vie-publique.fr/actualite/alaune/dossier-medical-personnel-vos-avis-son-contenu.html. Consulté le 27 décembre 2013.

irréversible, contrairement au masquage n'est permis qu'à l'auteur du document et non au patient, ni à un autre professionnel de santé. Le rapport de M. COULOMB de 2004 insistait sur cette distinction. « *La zone rouge doit être une zone masquée et non une zone manquante : aucune donnée ne doit pouvoir être effacée ni par le patient ni par le professionnel de santé*[1095]. » La CNIL, dans un entretien[1096] accordé au Conseil National de l'Ordre des médecins, considère qu'un patient ne peut exiger et obtenir du médecin qui détient son dossier l'effacement de données que si le patient invoque des motifs légitimes conformément à l'article 38 de la loi informatique et libertés. La Commission a, notamment admis comme légitime, le cas d'un patient hospitalisé aux hospices civils de Lyon qui demandait l'effacement des informations relatives à ses différentes hospitalisations conservées sur support informatique. Le motif invoqué était qu'atteint d'une affection qu'il ne souhaitait pas révéler à sa famille et ayant appris qu'un membre de sa famille médecin était amené à occuper un poste à l'hôpital, il craignait que la consultation du système informatique ne permette à son parent de connaître la nature de sa pathologie. En application de l'article 40[1097] de la loi informatique et libertés, le motif de la péremption des données pourrait également, être invoqué. Quant à l'appréciation du caractère périmé d'une information, la CNIL ramène à l'échange entre le médecin et le patient comme étant la voie la plus raisonnable. Mais en cas de conflit, seule l'appréciation souveraine des tribunaux pourrait trancher le litige[1098].

Le droit au masquage constitue pour le patient, une garantie de contrôle de ses informations personnelles de santé dans la mesure où cela lui donne l'impression de pouvoir continuer de délivrer aux professionnels de santé les renseignements qu'il juge nécessaires. Ainsi, pourrait-il taire les informations qu'il estimera gênantes, compromettantes comme c'était le cas antérieurement au dossier médical personnel. L'accès direct au DMP du patient contribue à le mettre davantage en confiance par rapport au dispositif et à s'assurer de la

---

[1095] COULOMB, Alain. *Rapport au ministre de la santé sur les conditions et modalités de mise en œuvre du dossier médical personnel*. Roissy, du 14 au 16 octobre 2004. p. 12. www.esante.gouv.fr.

[1096] Ordre des médecins. Entretien relatif au droit à l'oubli et au dossier médical informatisé. 13 octobre 2005. www.ordredesmedecins94.fr ou http://www.ordredesmedecins94.fr/telecharger.php?file=bfC_Dossier_medical_et_informatique.doc. Consulté le 2 mai 2014.

[1097] « *Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdit* »

[1098] Entretien relatif au droit à l'oubli et au dossier médical informatisé. 13 octobre 2005. www.ordredesmedecins94.fr ou http://www.ordredesmedecins94.fr/telecharger.php?file=bfC_Dossier_medical_et_informatique.doc. Consulté le 2 mai 2014.

confidentialité de ses données à l'égard des tiers car il ne sera pas obligé de recourir aux services d'un intermédiaire pour exercer ce droit de masquage.

Le masquage des informations dans le DMP ne sera pas signalé pour éviter tout soupçon ou éviter de susciter toute curiosité mal placée[1099]. En effet, le signalement du masquage dans une rubrique donnée du dossier peut faire deviner le contenu de l'information dissimulée. Par exemple, masquer le contenu de la rubrique relative à la sérologie fait immédiatement penser que le patient est probablement porteur du virus VIH ou une infection proche. Cependant, en cas de masquage d'un document, celui-ci restera visible à son auteur, au patient, au médecin traitant et au médecin de l'hébergeur. Dans sa délibération de 2010, la CNIL s'interroge sur le caractère étendu de cette exception au droit de masquage et insiste sur la nécessité de délivrer des informations claires et précises sur les modalités d'exercice du droit de masquage au patient. Il serait opportun que le masquage soit signalé à l'auteur de l'information afin qu'il ait la possibilité de donner, si nécessaire, les informations appropriées au patient sur les risques de cette décision. La Commission recommande que l'on s'atèle particulièrement, à faire prendre conscience au patient des prérogatives des médecins sus-cités dans le cadre de l'exercice de ce droit. Pour notre part, s'il est compréhensible que le document reste visible à son auteur, au patient concerné et à son médecin traitant, il est surprenant d'accorder cette prérogative au médecin de l'hébergeur dans la mesure où ce dernier n'intervient pas dans le parcours de soins. Peut-être aurait-il fallu prévoir que le document masqué ne lui soit visible qu'en cas de demande de suppression ou de tout autre traitement portant sur les données concernées adressée à lui par le patient. Ou encore, pourrait-on même envisager que le médecin de l'hébergeur ne fasse pas partie du cercle de ceux qui ont connaissance d'un document masqué car son avis n'est pas requis dans le parcours de soins.

L'état actuel de la législation en matière de droit de masquage ne précise pas les catégories de données pouvant être masquées. Toutes les informations contenues dans le

[1099] Le Parlement n'était pas de cet avis en 2004. Il déclarait : « *nous pouvons très bien concevoir qu'une personne ne souhaite pas voir figurer dans son dossier des données très personnelles bien que celles-ci soient importantes pour sa santé, par exemple une orientation sexuelle, des troubles psychiatriques, un alcoolisme chronique et demande en conséquence qu'aucune mention de ces données ne figure dans son dossier mais, il est nécessaire qu'à ce moment, figure un avertissement indiquant au praticien que le dossier est incomplet et qu'il devra demander des précisions au malade* ». DIONIS DU SEJOUR, Jean, ÉTIENNE Jean-Claude. Rapport sur les télécommunications à haut débit au service des systèmes de santé. Office Parlementaire d'évaluation des choix scientifiques et technologiques. Tome I. n° 370. 23 juin 2004. P. 43. http://www.senat.fr/rap/r04-370-1/r04-370-11.pdf. Consulté le 2 mai 2014.

dossier médical personnel seraient-elles susceptibles de masquage ? Si le rapport FAGNIEZ n'encourage pas à masquer isolément une partie d'un document du fait de la difficulté informatique à dissimuler une partie d'un document numériquement indivisible[1100], il ne règle pas la question du contenu susceptible d'être masqué. A notre sens, toutes les informations du contenu[1101] à l'exception du volet identification pourront être masquées dans la mesure où chacune d'elle peut véhiculer un renseignement ou un indice sur l'état de santé du patient.

Le droit de masquage constitue un élément de responsabilisation du patient et du respect de son autonomie, qui ne devrait pouvoir être levé en dehors du consentement de ce dernier. En 2005, le Dr François STEFANI préconisait que ce droit ne puisse être «*levé que dans le cas de conflits médico-légaux ou sur la demande du malade*[1102]». Pourtant, les documents masqués peuvent être consultés en cas d'urgence par le dispositif « *bris de glace* ». Certains intervenants du rapport FAGNIEZ ont marqué leur opposition à cette exception qu'ils ont justifiée par le fait qu' « *un tel démasquage pourrait* « *brouiller le message » en introduisant une brèche dans le dispositif de masquage et suscite une incompréhension de la part des autres professionnels de santé*[1103].». Néanmoins, cette solution sera acceptable s'il est permis au patient de pouvoir s'y opposer par avance. De plus, « *sa mise en œuvre devrait faire également l'objet d'un signalement à l'attention du médecin traitant*[1104] ». La remarque du rapport FAGNIEZ a été prise en compte par le législateur qui, à travers l'article L 1111-17 du code de la santé publique créé par la loi n° 2009-879 du 21 juillet 2009 a subordonné l'accès du médecin régulateur du centre de réception et de régulation des appels d'aide médicale urgente au dossier d'une personne à l'absence de toute opposition préalable expresse de celle-ci.

Pour certains auteurs, favorables au droit de masquage, l'argument selon lequel la reconnaissance d'un droit de masquage serait de nature à nuire à l'efficacité des soins apparaît sans objet en ce sens que la relation médecin - patient s'est toujours accompagnée de *« non*

[1100] Rapport FAGNIEZ. p. 14

[1101] Le dossier de presse du colloque national DMP fait une synthèse du contenu en six volets : (identification, données générales, soins, prévention, images, espace personnel). GIP-DMP. *DMP, Le dossier médical personnel. dossier de presse du colloque national DMP: éthique et confiance*. 4 décembre 2006. p.21. http://www.unrs.fr/doc/ACTUALITES/dossier_presse_colloqueDMP.pdf. Consulté le 28 mai 2014.

[1102] STEFANI, François. *Le patient doit être maître de son secret*. Bulletin de l'Ordre des médecins n° 3 mars 2005. P. 4.

[1103] Rapport FAGNIEZ. p. 14

[1104] Rapport FAGNIEZ. p. 14

dits » et qu'une information « *cachée* » à un moment donné pourra être révélée à un autre moment de la relation par l'intermédiaire de la nature des soins prodigués[1105]. Cet argument nous convainc peu dans la mesure où cette hypothèse ramène à la période antérieure au DMP qui était marquée par la redondance des actes et analyses médicaux du fait de manque d'informations des professionnels de santé sur la situation réelle de leur patient. Les informations étant masquées, le professionnel ordonnera probablement des examens supplémentaires qu'il n'aurait pas eu à faire s'il avait pris connaissance du document « caché ». Cela représente une perte de temps pour le patient et pour le professionnel de santé, mais aussi une perte d'économie pour l'assurance maladie. Cette position s'inscrit alors comme une antithèse des objectifs visés par la création du DMP : une meilleure coordination des soins en vue de réduire les dépenses de l'assurance-maladie. C'est finalement la remise en question de tout le projet de déploiement du DMP.

Plusieurs autres doutes sont à relever quant à l'efficacité et l'opportunité du dispositif du droit de masquage pour la coordination des soins et la meilleure prise en charge.

b. Les doutes relatifs au droit de masquage

Le pouvoir de masquage accordé au patient fait craindre qu'un individu non conscient de sa situation cache aux professionnels de santé des informations importantes pour le diagnostic et le traitement. Ce droit perçu initialement comme une prérogative, pourrait, alors, constituer, en définitive, un danger pour le patient. Le rapport de M. COULOMB d'octobre 2004 avait conclu qu'il «*faut lier la question du masquage des données à la notion de perte de chance pour le patient*[1106]». Pour le protéger, une formation du patient s'impose mais la question se pose de savoir quel niveau cette formation devrait-elle atteindre pour lui permettre de faire un masquage pertinent. Il faudrait envisager de l'informer sur les données qu'il pourrait masquer sans danger et celles qu'il ne devrait, en aucun cas, dissimuler. Or, cela relève du domaine de la médecine et de la psychologie qui nécessitent, pour sa compréhension, une certaine culture en ces matières ou, à tout le moins, des prérequis ; ce qui

[1105] BOSSI, Jeanne. *Les questions autour du dossier médical personnel* in ADSP n° 58 mars 2007. p.31-32. http://www.hcsp.fr/Explore.cgi/Telecharger?NomFichier=ad583033.pdf Consulté le 10 décembre 2013.

[1106] COULOMB, Alain. *Rapport au ministre de la santé sur les conditions et modalités de mise en œuvre du dossier médical personnel*. Roissy, du 14 au 16 octobre 2004. p. 12. www.esante.gouv.fr.

n'est pas le cas de la majorité de la population. Si une formation portant sur tout le contenu du dossier médical personnel s'avère difficile voire impossible, la solution serait de conseiller au patient qui envisage de procéder à un masquage d'un document précis, de consulter une personne avisée (particulièrement, l'auteur des données), au préalable. « *Comment concevoir que ce dernier puisse modifier a posteriori son DMP sans en parler avec celui qui, d'un commun accord, a inscrit les informations utiles ?* » s'interrogeait le Dr Michel CHASSANG[1107]. Cette solution laisse peu de place « *au masquage solitaire*[1108] » et oblige le patient à opter pour « *l'omission partagée*[1109] ». Pour le Dr Chevillard, « *en plus des informations provenant de diverses sources et en particulier d'un message électronique systématique lors du masquage, (…) cette aide au masquage doit être apportée par un service public gratuit constitué de professionnels de santé : médecins ou infirmières volontaires, compétents et dûment formés. Le professionnel de santé devrait acquérir une formation complémentaire dans le domaine juridique, psychologique et des connaissances nécessaires en informatique qui pourraient être sanctionnées par un nouveau certificat d'études spécialisées*[1110]. »

Tous les acteurs du DMP conviennent qu'il est essentiel de préserver le colloque singulier entre le patient et son médecin. De ce fait, les droits des patients doivent pouvoir cohabiter harmonieusement avec la relation de confiance inhérente à ce colloque. Toutefois, reconnaître un droit de masquage au patient peut faire craindre un sentiment de méfiance de ce dernier vis-à-vis de son médecin. Le praticien peut ressentir une frustration qui pourrait avoir un effet néfaste sur leur relation dans la mesure où un médecin pourrait juger inacceptable qu'il fournisse un travail que le patient saboterait en masquant des données. « *Le masquage ne doit pas reposer sur la défiance vis-à-vis des professionnels de santé.*[1111] » Les

---

[1107] CHASSANG, Michel. *Editorial. DMP: Attention danger!* 28 novembre 2006. http://www.csmf.org/upload/File/Edito/2006/edito_061128.pdf. Consulté le 20 janvier 2014.

[1108] La possibilité du masquage par le patient seul. 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. p. 13. http://www.cngof.asso.fr/D_TELE/rapport_fagniez2007.pdf. Consulté le 20 janvier 2014.

[1109] La possibilité de masquage par le patient accompagné ou assisté par son médecin. 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. p. 12. http://www.cngof.asso.fr/D_TELE/rapport_fagniez2007.pdf. Consulté le 20 janvier 2014.

[1110] CHEVILLARD, Marie. Thèse. *Le droit au masquage par le patient dans le cadre du dossier médical personnel en France*. 31 mai 2007. p. 115.

[1111] BENHAMOU Albert-Claude. *Colloque DMP, éthique et confiance : synthèse des travaux du colloque*. 4 décembre 2006. http://www.portailtelesante.org/article.php?sid=1358. Consulté le 15 décembre 2013.

représentants du Conseil national de l'Ordre des médecins ne semblent pas avoir cette inquiétude dans la mesure où, entendus par le professeur FAGNIEZ en janvier 2007, ils avaient souligné que « le droit au respect de leur intimité est une exigence légitime des patients ; dès lors on ne peut s'opposer à ce qu'ils masquent certaines informations sensibles qu'ils ne souhaiteraient pas voir figurer dans leur dossier ou porter à la connaissance de certains professionnels de santé. Cette revendication du droit au masquage et par extension au « masquage masqué » ne traduit pas nécessairement une perte de confiance envers les professionnels de santé mais plus vraisemblablement l'inquiétude des patients face au droit de consultation de ce dossier ouvert à un trop grand nombre de professionnels de santé[1112] ».

Le refus manifesté par un patient pour l'accès à son dossier médical par un médecin peut engendrer des conséquences qui ne sont pas, à notre sens suffisamment traitées par la loi sur le dossier médical personnel. Refuser l'accès à son dossier médical suppose, pour le patient, de refuser que ce professionnel de santé y reporte des informations à l'issue d'un acte médical. Alors que la CNIL avait adopté une position exigeant que cette opposition soit justifiée par des raisons légitimes[1113], les associations des patients ont désiré une plus grande liberté en n'ayant pas à justifier leur choix. Pour elles, en effet, le risque de voir circuler leurs informations personnelles de santé sur Internet suffisait largement à refuser un report de renseignements médicaux dans le dossier médical personnel. Si la réponse du ministre de la santé et des solidarités à la question[1114] qui rapportait cette inquiétude a été de rappeler leurs conditions du libre choix des patients et des limitations d'accès à leur dossier médical personnel prévues par la loi, nous pensons que le véritable problème a été éludé. Une chose est de laisser le patient masquer des informations mais une autre est de refuser que ces informations soient inscrites. Dans le cas du masquage, il reste possible à un professionnel de santé autorisé de prendre connaissance des informations qui pourraient être utiles pour une

[1112] Conseil national de l'ordre des médecins. *Masquage des données : le CNOM rappelle que le DMP est le dossier personnel du patient*. 7 février 2007. Http://www.Conseil-national.medecin.fr/article/masquage-des-donnees-le-cnom-rappelle-que-le-dmp-est-le-dossier-personnel-du-patient-603. Consulté le 17 janvier 2014.

[1113] En vertu de l'article 38 de la loi informatique et libertés, le patient aura aussi la possibilité de faire supprimer certaines données ou de refuser qu'elles soient inscrites dans son dossier. L'exercice de ce droit à l'oubli, qui va au-delà du droit de masquage est, cependant, soumis à la condition que le patient donne « *des motifs légitimes* ». Contrairement au droit de masquage, qu'il peut exercer directement, le patient ne pourra jouir de ce droit que par l'intermédiaire du médecin de l'hébergeur.

[1114] Assemblée nationale. Question écrite n° 94963 publiée au JOAN du 23 mai 2006. Ministère de la santé et des solidarités. Assurance maladie maternité : généralités-dossier médical personnel-contenu. Question de M. Morel - A- L' Huissier Pierre, Député de Lozère groupe de l'Union pour un mouvement populaire. Réponse publiée au JOAN du 28 novembre 2006, p. 12551. ww.assemblee-nationale.fr.

meilleure prise en charge alors que dans le cas d'un refus d'inscription de l'information, le professionnel qui n'est pas à l'origine de l'acte médical concerné n'a aucun moyen d'en prendre connaissance. Les conséquences sur la santé de l'individu sont faciles à deviner. C'est pourquoi, au risque de limiter les droits du patient sur ses données médicales à caractère personnel, il serait peut-être, préférable, dans son intérêt, de ne pas lui accorder ce droit de refus d'inscription de données dans son DMP.

Pour rétablir un certain équilibre face aux prérogatives conférées au patient (à travers son droit de limitation express d'accès à son DMP et son droit de masquage), le législateur a accordé de l'autorité au médecin sur une partie des informations médicales. L'article R 4127-45-I du code de la santé publique attribue au médecin une fiche personnelle. « *Indépendamment du dossier médical prévu par la loi, le médecin tient pour chaque patient une fiche d'observation qui lui est personnelle ; cette fiche est confidentielle et comporte les éléments actualisés, nécessaires aux décisions diagnostiques et thérapeutiques. Les notes personnelles du médecin ne sont ni transmissibles ni accessibles au patient et aux tiers. Dans tous les cas, ces documents sont conservés sous la responsabilité du médecin.* »
Le décret du 7 mai 2012[1115] qui introduit cette disposition limite donc l'accès du patient à certains aspects de son dossier médical et non à toutes les informations concernant sa santé. Ces renseignements sont conservés hors du dossier médical personnel, *indépendamment du dossier médical*, et le patient n'y a aucun contrôle. A dessein ou non, le législateur réduit ainsi le grand écart qui existe entre les obligations du médecin et les droits qui ont été reconnus au patient par la loi du 4 mars 2002. C'est une limite au droit d'accès illimité du patient à ses données de santé qui, à notre sens, pourrait rehausser l'image du médecin gêné dans la prise de ses décisions par un droit de contrôle trop important du patient sur ses données de santé à caractère personnel. L'accès illimité du patient sur ses données de santé à caractère personnel porte sur « *les informations qui ont été formalisées ou qui ont fait l'objet d'échanges écrits entre professionnels de santé »,* selon les termes de l'article L 1111-7 du code de la santé publique. Les informations formalisées sont celles auxquelles est donné un support (écrit, photographie, enregistrement, etc.) avec l'intention de les conserver et sans lequel elles seraient objectivement inaccessibles. Ces informations sont destinées à être réunies dans ce

[1115] Décret n° 2012-694 du 7 mai 2012 portant modification du code de déontologie médicale. JORF n° 0108 du 8 mai 2012. P 8479. Texte n° 97. NOR: ETSH1207448D

qu'il est habituel d'appeler le dossier de la personne[1116]. Or, la fiche personnelle du médecin est un dossier professionnel dont la rédaction n'est soumise à aucun formalisme. Les informations qui y sont contenues ne sont pas destinées à être conservées, réutilisées ou le cas échéant, échangées, parce qu'elles ne peuvent contribuer à l'élaboration et au suivi du diagnostic et du traitement ou à une action de prévention. Elles peuvent être considérées comme « personnelles », ne peuvent être communiquées et sont donc intransmissibles et inaccessibles à la personne concernée comme aux tiers, professionnels ou non.

Il est donné la possibilité à un professionnel de santé de rendre invisibles des documents au patient, au moment de l'alimentation du dossier médical personnel. L'invisibilité du document sert dans des cas spécifiques comme la consultation d'annonce[1117]. Afin de proposer une meilleure prise en charge au patient, une réunion de concertation précède sa consultation d'annonce. Le compte rendu de la réunion de concertation pluridisciplinaire est intégrée au dossier consultable par l'équipe soignante seulement mais il est également transmis au médecin traitant. Dans ce cas, le document est visible pour les professionnels de santé autorisés sur le dossier médical personnel mais n'est pas visible pour le patient. L'invisibilité d'un document est réversible ; elle est mise en œuvre de façon temporaire et le document peut être, ensuite, rendu visible pour le patient. La fonction devient alors irréversible et ne permet plus de rendre à nouveau, invisible un document rendu visible lors de l'alimentation du DMP. Ce dispositif s'inscrit dans la logique de l'article 35 du code de déontologie médicale qui prescrit que dans l'intérêt du malade et pour des raisons légitimes que le praticien apprécie en conscience, un malade peut être tenu dans l'ignorance d'un diagnostic ou d'un pronostic graves, sauf dans les cas où l'affection dont il est atteint expose les tiers à un risque de contamination. L'invisibilité temporaire permise vise à ménager la sensibilité du patient. Le dispositif d'annonce est une mesure du plan cancer, mise en place à la demande des patients lors des premiers états généraux des malades atteints du cancer en 1998, pour bénéficier de meilleures conditions d'annonce du diagnostic de leur maladie[1118].

[1116] Arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès. JORF n° 65 du 17 mars 2004. P. 5206. Texte n° 16. NOR: SANP0420786A.

[1117] La consultation d'annonce est un des éléments du dispositif d'annonce. Il s'agit d'une consultation dont le but est de renseigner et rassurer les patients et leur entourage. C'est la consultation où l'on va discuter et choisir avec le patient les modalités de sa prise en charge. La mesure 40 du plan cancer en constitue le cadre réglementaire.

[1118] Institut national du cancer. *Recommandations nationales pour la mise en œuvre du dispositif d'annonce du cancer dans les établissements de santé: Mesure 40 du plan cancer*. Novembre 2005. p.2. www.e-cancer.fr

Malgré ces solutions en faveur du médecin qui contrebalancent le pouvoir de contrôle du patient sur ses données, jusqu'en janvier 2014, le droit de masquage dans le dossier médical personnel est sujet à polémique. Face à la proposition de l'institut Montaigne de tolérer un dossier médical personnel complet sans possibilité de masquage, l'avis du ministre du travail, de l'emploi et de la santé est demandé. Reprenant les termes du rapport FAGNIEZ, le ministre rappelle : « *en créant le dossier médical personnel, le législateur a entendu concilier ces deux enjeux : le dossier est confié au patient, qui en maîtrise les accès et en contrôle le contenu. Le pouvoir réglementaire ne peut dès lors que lui donner tous les moyens de ce contrôle, en confirmant un droit de masquage total.* » L'idée est renforcée par le fait que « *la complétude des informations que donne un patient à son médecin repose sur la confiance et non sur un dispositif technique. En outre, on ne peut nier à chaque personne un « droit à l'oubli* [1119]». Toutefois, le ministre a fait remarquer que le dispositif du droit de masquage, même s'il respecte la volonté du législateur et celle du patient, demeure une exception. D'ailleurs, le recours à ce droit n'est pas définitif en ce sens qu'une revue du DMP est en cours après les premiers mois d'utilisation pour faire le point sur les enseignements à tirer des premiers usages et que les évolutions à venir prendront en compte les résultats de cette étude. Le dispositif du droit de masquage peut donc, toujours, être révoqué. Cette éventualité est d'autant plus probable que les craintes qui entourent la mise en œuvre de ce droit de masquage sont plus nombreuses que les certitudes. Non seulement l'exercice de ce droit ne convainc pas la majorité des professionnels à l'intérieur même du DMP mais en plus, il risque de constituer un frein à l'harmonie du dossier du patient lorsque le dossier pharmaceutique alimentera le dossier médical personnel. En effet, dans le dossier pharmaceutique, il est prévu un droit proche du droit de masquage. Le patient a la possibilité de s'opposer à l'alimentation de son dossier s'il ne souhaite pas qu'une information relative à un médicament y figure. Une attestation de refus lui est, alors, remise et le dossier comportera l'indication que des informations n'y sont pas mentionnées. La CNIL considère qu'elle devra réexaminer ce droit d'opposition lorsque le dossier pharmaceutique alimentera le DMP, « *en raison de la dualité de régimes juridiques entre le droit de masquage qui ne serait pas apparent dans le DMP et*

[1119] Assemblée nationale. Réponse publiée au JORF du 1er mai 2012. p. 3391. Question ministérielle n°117101 publiée au JO du 30 août 2011. http://questions.assemblee-nationale.fr/q13/13-117101QE.htm. Consulté le 17 janvier 2014.

l'exercice d'un droit analogue dans le dossier pharmaceutique qui ferait l'objet d'une mention expresse »[1120].

En l'absence de toute solution convaincante trouvée à ce jour pour la mise en œuvre concrète du droit de masquage, les suggestions faites par le rapport FAGNIEZ en 2007 demeurent les meilleures pistes de réflexion sur le sujet. Cinq propositions avaient été exposées :

- L'omission partagée[1121] entre le professionnel de santé et le patient doit être privilégiée : l'intervention d'un professionnel de santé dans le processus de masquage est reconnue comme hautement souhaitable. Seul lui peut mesurer l'utilité d'une information dans le dossier médical personnel et informer pleinement le patient sur le risque qu'il y aurait à la masquer. Ce « masquage partagé » doit donc être la procédure proposée au patient qui souhaite masquer une donnée dans son dossier.

- Le masquage solitaire, s'il doit être évité et dissuadé, ne peut être totalement interdit : malgré les nombreux avantages de l'omission partagée, il est inévitable et impératif de conserver la possibilité marginale du masquage par le patient seul (« masquage solitaire ») pour préserver son droit au secret. Il faut néanmoins minimiser et dissuader l'usage du masquage solitaire et inviter le patient à consulter son médecin traitant.

- Le masquage du masquage est préférable au signalement du masquage : le masquage du masquage s'impose en cas d'omission partagée comme en cas de masquage solitaire et doit être systématique.

- Sans réduire la portée du droit au masquage, des limitations au masquage sont envisageables et sont de nature à renforcer la confiance des professionnels de santé : une donnée masquée devrait rester visible non seulement pour son auteur mais également pour toute l'équipe de soins à laquelle il appartient, le médecin traitant devrait avoir accès aux données masquées avec la condition que le patient puisse s'y opposer et limiter le masquage à la seule donnée souhaitée et non à un document entier. Mais il faudrait éviter la mise en œuvre d'une procédure de démasquage en situation d'urgence.

[1120] CNIL. Délibération n° 2007-106 du 15 mai 2007 *portant autorisation des applications informatiques nécessaires à la mise en œuvre de la phase expérimentale du dossier pharmaceutique*. Http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017652212. Consulté le 28 mai 2014.

[1121] Le rapport distingue deux formes d'omission partagée : l'une consiste à rendre l'information totalement absente du DMP. Elle doit s'appliquer aux informations non pertinentes ou périmées. La seconde se contente de rendre invisible (masquer) une information présente dans le DMP. La donnée inscrite est, aussitôt, masquée avec possibilité pour le patient de changer d'avis ultérieurement (démasquer). Mais cela n'est possible qu'à condition de limiter clairement la responsabilité du professionnel de santé impliqué dans l'omission partagée.

- Il est nécessaire d'assurer une communication envers les professionnels de santé : il faut expliquer et démontrer à l'ensemble des professionnels de santé la plus-value qu'apporte le DMP dans le processus de soins, accompagner la mise en œuvre des propositions formulées dans le rapport par une communication, expliquer aux professionnels de santé leur absence de responsabilité juridique en cas d'implication dans une omission partagée comme en cas d'ignorance fâcheuse d'une donnée masquée et leur annoncer que les choix faits en matière de masquage sont valables pour une période probatoire de deux ou trois ans [1122].

La question de la responsabilité des professionnels de santé est l'un des enjeux majeurs du droit de masquage. L'impact de ce droit sur le régime juridique de la responsabilité est considérable dans la mesure où le professionnel de santé ne sera pas immédiatement visé en cas de préjudice subi par le patient du fait d'un manque d'information dans son DMP. Désormais, il faudrait rechercher si l'information déterminante pour le diagnostic ou le traitement figurait dans le dossier du patient ou si celui-ci l'avait masqué au regard du professionnel de santé. La traçabilité des accès et des masquages pourrait permettre de déterminer la source de l'absence d'information et définir les responsabilités. Pour se dégager de toute responsabilité, les représentants du CNOM avaient exprimé leur opposition à la notion « d'omission partagée » proposée dans le rapport FAGNIEZ. « *Le médecin a bien un devoir d'information et de conseil vis-à-vis des patients. Ceux-ci doivent en effet être éclairés sur l'intérêt d'une donnée, les risques de l'omettre ou de la masquer. Mais la décision de masquer leur revient en propre et elle s'opère sous leur seule et entière responsabilité. La responsabilité des professionnels de santé ne saurait être engagée du fait d'informations ignorées puisque masquées*[1123]. » En prenant plus de responsabilité dans la gestion de son dossier médical personnel, le patient partage les responsabilités du professionnel de santé au point de l'en exonérer[1124] en cas de masquage de données. Finalement, le droit de masquage

[1122] 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. p 12-15. http://www.bdsp.ehesp.fr/Base/353477/. Consulté le 2 mai 2014.

[1123] FRASLIN. *Le CNOM souhaite un néo-DMP sincère et construit par les médecins.* 9 février 2008. www.i-med.fr.

[1124] « *Si le patient entend ne pas faire figurer dans son DMP des informations essentielles à l'amélioration de la coordination des soins, il place le médecin dans l'incapacité de réaliser un acte médical conforme aux données acquises de la science. L'omission constitue, à ce titre, une cause d'exonération de responsabilité du professionnel qui, n'étant pas dûment averti des antécédents médicaux du patient, ne pouvait réaliser un acte dans des conditions satisfaisantes*. » CHEVILLARD, Marie. Thèse. *Le droit au masquage par le patient dans le cadre du dossier médical personnel en France*. 31 mai 2007. p. 131.

dans le DMP pourra permettre de réduire les risques de responsabilisation des professionnels de santé en apportant au juge des preuves factuelles de dissimulation d'informations.

Le code de la santé publique interdit, d'office, l'accès au dossier médical personnel à certaines personnes ou dans certaines circonstances.

B. Les limitations légales d'accès au DMP

L'article L 1111-18 du code de la santé publique dispose : « *l'accès au dossier médical personnel ne peut être exigé en dehors des cas prévus aux articles L 1111-15 et L 1111-16 même avec l'accord de la personne concernée.*» Les situations et les personnes non autorisées sont limitativement citées par la loi. Il s'agit de la conclusion d'un contrat et des médecins du travail.

1. L'interdiction d'accès au DMP lors de la conclusion d'un contrat

« *L'accès au dossier médical personnel est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application.* » Le législateur a prohibé toute consultation du dossier médical personnel pendant la conclusion d'une convention pour laquelle l'état de santé de l'individu peut influer sur la décision de son cocontractant. La lecture du texte donne à croire que cette interdiction concerne uniquement les contrats ayant un lien direct avec l'état de santé de la personne. On pourrait donc déduire que l'accès au dossier médical personnel lors de la conclusion d'un contrat pour lequel l'état de santé du contractant n'a aucune importance est autorisé. Mais, la seconde phrase de cet article donne une impression d'élargissement avec l'emploi du groupe nominal « *d'un contrat* » qui est d'une telle généralité que l'on pourrait comprendre que tous les contrats sont soumis à cette prohibition. L'introduction de l'adverbe « *également* », véhicule une idée d'addition qui nous amène à conclure que l'interdiction concerne autant tous les contrats ayant un lien avec l'état de santé du contractant que tous les autres contrats. Le législateur a probablement fait cette

distinction en prenant le soin de citer en premier les conventions en lien avec l'état de santé pour mieux exprimer son intention protectionniste. Il se montre insistant quant au moment où cette interdiction doit être appréciée. Non seulement il est interdit d'accéder au dossier de la personne avant la conclusion du contrat, mais également durant toute la durée de l'exécution de cette entente. Cette disposition est de nature à protéger l'individu contre toute discrimination portant sur son état de santé. Même si elle paraît injuste vis-à-vis de cocontractant, notamment les maisons d'assurance, il faut y voir la volonté du législateur de défendre la partie la plus vulnérable.

L'article 35 de la loi[1125] 2007-290 du 5 mars 2007 instituant le droit au logement opposable et modifiant l'article 22-2 de la loi[1126] 89-462 du 6 juillet 1989, a pu faire croire qu'il serait possible à un bailleur, dans le cas particulier d'une demande de logement adapté ou spécifique, de demander au candidat à la location de produire son dossier médical personnel. Ainsi, le député ROGEMONT[1127], au sujet de l'analyse de la loi du 13 août 2004, avait-il relevé une incohérence du texte relatif à l'interdiction faite au médecin du travail, docteur en médecine, de coonsulter le DMP alors que le bailleur non soumis au secret professionnel y avait légalement droit. Mais la ministre de la santé a tenu à dissiper le malentendu en précisant que la loi[1128] 2007-1786 du 19 décembre 2007 a, par son article 55 levé la confusion résultant de ces dispositions en supprimant les termes *« sauf en cas de demande de logement adapté ou spécifique* » de cet article 22-2. Le dossier médical personnel reste confidentiel et du seul ressort du monde médical, il ne peut en aucun cas être demandé par un bailleur.

[1125] 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. Texte n° 4. NOR: SOCX0600231L.

[1126] Loi n° 89-462 du 6 juillet 1989 dite MALANDIN, MERMAZ tendant à améliorer les rapports locatifs et portant modification de la loi 861290 du 23-12-1986. JORF du 8 juillet 1989. p. 8541. NOR: EQUX8910174L.

[1127] M. Marcel ROGEMONT, Député socialiste, radical, citoyens et divers gauche-Ille-et-vilaine. Assemblée nationale. Réponse ministérielle publiée au JORF du 20 mai 2008. p. 4261. Question n° 12931 de M. Marcel ROGEMONT. JORF du 18 décembre 2007. p. 7962. Santé, jeunesse, sports et vie associative, assurance maladie maternité: généralités. www.assemblee-nationale.fr.

[1128] 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. Texte n° 2. NOR: BCFX0766311L.

Article 55 . VI: « *Dans le 14e alinéa de l'article 22-2 de la loi n° 89-462 du 6 juillet 1989 tendant à améliorer les rapports locatifs et portant modification de la loi n° 86-1290 du 23 décembre 1986, les mots : «, sauf en cas de demande de logement adapté ou spécifique » sont supprimés*. » .

2. L'interdiction d'accès au DMP dans le cadre de la médecine du travail

Seuls les professionnels de santé autorisés par le titulaire du DMP peuvent accéder à son dossier. L'accès par toute autre personne est formellement interdit. « *Le dossier médical personnel n'est pas accessible dans le cadre de la médecine du travail*.» Même s'il est tenu au secret médical au même titre que ses confrères, le médecin du travail n'est pas autorisé à consulter le dossier médical personnel dans le cadre de sa mission. Cette interdiction rappelle que le dossier médical personnel n'est ouvert qu'aux seuls professionnels de santé participant à l'acte médical, qu'il soit préventif, diagnostique ou de soins. La ministre de la santé avait répondu, à l'Assemblée nationale, en 2008 que l'accès au dossier médical personnel a volontairement été limité aux professionnels de santé délivrant des soins afin d'offrir toutes les garanties en matière d'éthique et de confidentialité et pour que le DMP ne soit pas utilisé dans un contexte qui sortirait de la relation soignant-soigné[1129]. Pourtant, le praticien-conseil de l'assurance maladie peut accéder au dossier médical d'un assuré lorsque cela est *« strictement nécessaire »* pour sa mission alors même qu'il n'intervient pas dans l'acte médical. Le Conseil de l'Ordre des médecins considère que dans la mesure où l'intervention du praticien-conseil permet aux malades d'obtenir des avantages sociaux nécessaires à une bonne prise en charge par le système de soins, il est en droit de bénéficier de cette prérogative. Cet argument est fondé sur l'article 50 du code de la déontologie médicale qui dispose : « *le médecin doit, sans céder à aucune demande abusive, faciliter l'obtention par le patient des avantages sociaux auxquels son état lui donne droit. A cette fin, il est autorisé, sauf opposition du patient, à communiquer au médecin-conseil nommément désigné de l'organisme de sécurité sociale dont il dépend, ou à un autre médecin relevant d'un organisme public décidant de l'attribution d'avantages sociaux, les renseignements médicaux strictement indispensables.* » La contrepartie de cette attribution d'avantages sociaux prévus dans le deuxième alinéa de cet article 50 est l'exercice d'un contrôle possible par la sécurité sociale ou les autres organismes publics qui décident de leur attribution. Tous les renseignements et tous les documents d'ordre médical, individuel ou général, seront communiqués - sauf opposition du patient - au médecin-conseil en charge du contrôle, dans le respect des règles du secret partagé et de la déontologie. Le médecin doit satisfaire à cette obligation mais ne fournit au

[1129] Assemblée nationale. Réponse ministérielle publiée au JOAN du 20 mai 2008. p. 4261. Question n° 12931 de M. Marcel ROGEMONT publiée au JOAN du 18 décembre 2007. p. 7962. Santé, jeunesse, sports et vie associative, assurance maladie maternité: généralités. www.assemblee-nationale.fr

médecin-conseil d'assurance maladie que les documents strictement nécessaire pour mener à bien sa mission conformément à l'article[1130] L 1112-1 alinéa 6 du code de la santé publique[1131].

La loi de mars 2002 a complété les articles L 315-1 du code de la sécurité sociale et L 1414-4 du code de la santé publique par d'autres types d'interdiction moins populaires. L'article L 315-1, V. dispose *« les praticiens-conseils du service de contrôle médical et les personnes placées sous leur autorité n'ont accès aux données de santé à caractère personnel que si elles sont strictement nécessaires à l'exercice de leur mission, dans le respect du secret médical. »* Dans le cadre des contrôles effectués par la Sécurité sociale pour les prestations de l'assurance-maladie, maternité, invalidité ainsi que d'autres prestations prises en charge en application du code de l'action sociale et des familles, des contrôles portant sur des éléments d'ordre médical peuvent être diligentés auprès des assurés et leurs médecins. Les praticiens-conseils à charge de ces enquêtes ne sont, en principe, pas autorisés à consulter les dossiers médicaux des assurés. Exceptionnellement, l'interdiction sera levée si l'accès aux données de santé à caractère personnel s'avère absolument indispensable à la bonne marche de leurs investigations et si cela se fait dans le respect du secret médical. L'autorisation d'accès est accordée uniquement aux médecins-conseils du service médical et non à ceux des services administratifs des caisses. Les missions des médecin-conseils susceptibles de nécessiter un accès aux données de santé à caractère personnel des assurés sont principalement : l'octroi des prestations (ALD, arrêt de travail, ...), le contrôle de la tarification à l'activité (T2A), le contrôle des prescriptions de médicaments ou produits de santé facturés en sus des groupes homogènes de séjours (GHS), l'analyse du fonctionnement d'un établissement à la demande de l'agence régionale d'hospitalisation (ARH) ou de la Direction départementale des affaires sanitaires et sociales (DDASS), la mise sous accord préalable de prescripteurs (MSAP), l'analyse de l'activité d'un professionnel de santé suspecté de faute, fraude ou abus[1132].

[1130] « *Les médecins membres de l'inspection générale des affaires sociales, les médecins inspecteurs de santé publique, les inspecteurs de l'agence régionale de santé ayant la qualité de médecin et les médecins-Conseils des organismes d'assurance maladie ont accès, dans le respect des règles de déontologie médicale, à ces informations lorsqu'elles sont nécessaires à l'exercice de leurs missions.* »

[1131] CNOM. *Article 50, Secret partagé avec les médecins Conseils des organismes d'assurance maladie*. 11 octobre 2012. http://www.Conseil-national.medecin.fr/article/article-50-secret-partage-avec-les-medecins-Conseils-de-la-securite-sociale-274 Consulté le 22 janvier 2014.

[1132] KULLING, Gabriel. *L'accès au dossier médical hospitalier par le médecin-Conseil de l'assurance maladie* in revue générale de droit médical. n° 37. Décembre 2010. P. 230

Le législateur impose les mêmes conditions de nécessité aux médecins experts mandatés par la Haute autorité de santé, dans le cadre des procédures de certification des professionnels et établissements de santé. L'article L 1414-4, alinéa 5 du code de la santé publique dispose : *« Les médecins experts de l'agence n'ont accès aux données de santé à caractère personnel que si elles sont strictement nécessaires à l'exercice de leur mission d'accréditation lors de la visite sur les lieux, dans le respect du secret médical. »*

La violation de ces interdictions légales expose le contrevenant à des peines d'un an d'emprisonnement et de 15 000 € d'amende conformément à l'article 226-13 du code pénal.

Le dossier médical personnel créé pour chaque bénéficiaire de l'assurance maladie en vue de la coordination de soins, de la recherche d'une meilleure qualité de traitement et pour la réduction des dépenses de santé est fondé sur une base légale qui a prévu un mécanisme de protection des droits des patients qui se révèle être des plus singuliers au monde. Depuis la loi Kouchner de 2002, les droits des patients ont été étendus, accordant une large place au consentement. Contrairement à ceux-ci, les professionnels de santé n'ont pas bénéficié de régime de responsabilité plus alléchant. Malgré les arguments avancés par les gestionnaires du projet sur les avantages de la gestion du dossier médical personnel sur le colloque singulier, un très grand nombre de la population, y compris les professionnels de santé demeure sceptique. Un élément d'ordre sociologique qui, ajouté au retard pris par les décrets d'application des dispositions légales sur le dossier médical personnel contribue à ralentir le déploiement généralisé de cet outil de télésanté. Une politique de sensibilisation au dossier médical personnel s'avère donc nécessaire. La vision du professeur BENHAMOU sur la question nous paraît des plus appropriées lorsqu'il envisage que l'on développe une culture du DMP , très tôt, chez chaque individu. « *Une culture sociétale nouvelle est essentielle à cet égard et un nouvel effort doit être accompli en impliquant fortement l'Éducation nationale, les associations de parents, les associations familiales de telle sorte que dès le plus jeune âge, les citoyens soient sensibilisés à la problématique du dossier médical personnel*[1133] ».

[1133] BENHAMOU Albert-Claude. *Colloque DMP, éthique et confiance : synthèse des travaux du colloque*. 4 décembre 2006. http://www.portailtelesante.org/article.php?sid=1358. Consulté le 10 mars 2014.

CONCLUSION

Au terme de cette étude, On doit constater que malgré toutes les réponses juridiques déjà données aux questions posées par l'introduction des nouvelles technologies de l'information et de la communication dans le domaine de la santé, le droit positif est encore loin de résoudre tous les problèmes liés à la protection de la vie privée. Alors, faut-il, pour autant balayer du revers de la main tout le droit existant pour en créer un autre spécifique à cette nouvelle réalité ? Sur la question, les professeurs GAUTRAIS et TRUDEL ne sont pas aussi radicaux. Ils semblent militer en faveur d'une adaptation plutôt qu'un rejet catégorique du droit existant. Selon eux, « *face aux bouleversements technologiques que beaucoup considèrent comme, à juste titre, « révolutionnaires », il n'est d'autres choix que de changer le droit aussi. Suivant des degrés différents, plusieurs considèrent donc que ce domaine en émergence, à l'instar du droit plus englobant qu'est le droit du cyberespace, est différent du droit traditionnel. Le droit de la vie privée devrait par conséquent être au pire remanié, au mieux rebalancé, certains principes étant désuets et d'autres sous-évalués*[1134]». Nous partageons leur position et considérons que le plus judicieux serait « *de concilier situations «nouvelles» et «vieux» droit* [1135]». C'est aussi la politique adoptée par le gouvernement français dans l'encadrement juridique de la gestion électronique des données médicales.

La gestion électronique des données médicales s'inscrit non seulement dans le champ du traitement automatisé de toutes les données personnelles, mais aussi dans celui qui est particulier aux données sensibles, notamment les données de santé. Son encadrement juridique est donc assuré par les règles communes au traitement de toutes les données personnelles tout comme par les règles spécifiques au traitement des données médicales.
Les règles communes concernent les formalités préalables à la mise en œuvre des traitements et les principes généraux qui fondent ces procédures dont la formalité de déclaration préalable au traitement est la règle en la matière. Mais, cette règle de la déclaration admet des assouplissements comme des traitements exonérés de formalités préalables. Certains traitements sont, par contre, soumis à des procédures plus rigoureuses de demande d'autorisation préalable. C'est le cas du traitement automatisé des données médicales. Ces formalités établies par la loi informatique et libertés, trouvent leur fondement dans les principes généraux à valeur constitutionnelle que sont le respect de la vie privée et celui de

[1134] GAUTRAIS, Vincent, TRUDEL, Pierre. *Circulation des renseignements personnels et Web 2.0*. Université de Montréal. Édition Thémis, 2010. p.1.

[1135] Op cit. p. 3.

l'ordre public. Consacrés tant par les traités internationaux que par les droits européen et français, ces principes sont mis en œuvre à travers des exigences légales liées aux obligations qui pèsent sur les responsables de traitement et les droits reconnus aux titulaires des données traitées.

La gestion électronique des données médicales consiste autant dans le simple traitement automatisé des données que dans le partage et l'échange[1136] de ces informations entre les différents acteurs. Le partage des informations des patients engendré par l'utilisation des technologies de l'information et de la communication a pour objectif de favoriser une meilleure qualité de soins et une réduction des dépenses de santé. Cette pratique, la télésanté, se présente sous une forme diversifiée avec des applications médicales (la télémédecine) et des applications médico-sociales. Dans ce cadre, Internet joue un rôle capital , mais le partage ne peut être possible que si les systèmes d'information sont interopérables. Cette interopérabilité, encore en chantier en Europe et en France, connaît des limites que l'État français veille à corriger en nommant un maître d'ouvrage : l'agence des systèmes d'information partagée de santé (Asip santé). Cette agence a, entre autres missions, de favoriser le partage des données de santé en assurant l'interopérabilité et la sécurité des systèmes d'information à travers les référentiels qu'elle homologue. L'Asip santé a également pour attribution de veiller au déploiement du dossier médical personnel (DMP)[1137], principal outil de mise en œuvre de la télésanté. L'agence assure, à cet effet, l'encadrement de la procédure d'agrément à laquelle sont soumis les hébergeurs de données de santé dans l'optique de garantir la sécurité et la confidentialité de ces renseignements.

L'intervention d'Internet dans la mise en œuvre de ces partages d'informations médicales pose des problèmes de sécurité de la vie privée auxquels les autorités compétentes tentent de faire face. La loi informatique et libertés est la principale référence en matière de protection des données personnelles. Modifiée après la transposition de la directive européenne 95/46/CE, cette loi augmente les pouvoirs de la CNIL, autorité indépendante chargée du

[1136] « *L'échange est un transfert unidirectionnel ou réciproque de données, par voie orale ou par le biais de l'informatique (à l'instar de la messagerie électronique). Au contraire, le partage est l'action de rendre des informations accessibles à plusieurs personnes*. » ZORN, Caroline. *Données de santé et secret partagé*. P 27.

[1137] Au 15 juin 2014, on se demande si l'Asip santé demeurera maître d' ouvrage de ce projet car la Ministre actuelle des affaires sociales et de la santé, Mme Marisol TOURAINE envisage nommer un nouveau chef de projet pour le DMP dans le cadre de sa vision du DMP "nouvelle génération". Sénat. *Comptes rendus des auditions de la Commission des affaires sociales*. [en ligne]. 16 octobre 2013. Disponible sur: http://www.senat.fr/compte-rendu-Commissions/20131014/soc.html#toc10. Consulté le 11 juin 2014.

contrôle de son application. Dans cette optique, plusieurs délibérations ont été prises et des sanctions, prononcées par la Commission contre les contrevenants à la loi informatique et libertés.

La loi KOUCHNER de mars 2002 a donné une impulsion aux droits des patients. Le patient est davantage impliqué dans la gestion de son dossier médical personnel. Il lui a, notamment, été reconnu un droit de masquage et un droit d'accès direct avec possibilité de modification de son dossier médical personnel. Aucun acte de gestion électronique de ses données médicales ne peut être effectué sans son consentement. Toutefois, si la reconnaissance de tous ces droits permet au patient d'avoir un meilleur contrôle sur ses données de santé, il n'est pas exclu que, mal exercés, certains l'exposent à de véritables dangers pour sa santé. Le droit de masquage, constituant l'exemple type, est aujourd'hui controversé car non seulement la relation de confiance qui caractérise le "colloque singulier " entre soignant et soigné en pâtit, mais le patient pourrait aussi modifier ou dissimuler des informations capitales pour son suivi médical. Pour l'instant, le droit français n'en donne pas les modalités exactes d'application censées faire l'objet d'un décret en Conseil d'État pris après avis de la CNIL, aux termes de l'article L 1111-21 du code de la santé publique.

Le cadre juridique du dossier médical personnel est en construction depuis 2004, date de sa création. Cette situation influence lourdement son déploiement car de nombreux aspects pratiques restent encore à être précisés par le décret DMP attendu depuis 2007. Quatre décrets étaient prévus pour la définition et la mise en œuvre du dossier médical personnel, clef de voûte de la réforme du système de santé. Alors que deux d'entre eux sont parus (" hébergement de données de santé", décret du 4 janvier 2006, et " confidentialité", décret du 15 mai 2005), les deux autres, qui sont pourtant fondamentaux pour la suite du processus, sont encore en cours de préparation et font l'objet de discussions et d'incertitudes sur différents points capitaux (le décret DMP et le décret relatif à l'identifiant de santé).

Sans doute, plusieurs questions qui restent en suspens pourront-elles trouver leur réponse lorsque ces textes paraîtront, mais la réalité fait qu'il serait illusoire de croire qu'ils suffiront à résoudre les deux dilemmes qui demeurent : celui des libertés individuelles du patient face à sa santé et celui de la confidentialité de ses données médicales face à sa santé. Faut-il privilégier l'extension des droits des patients sur leur dossier médical personnel, malgré les risques que cela se retourne contre eux, ou faut-il préserver leur santé en restreignant leurs libertés individuelles ? Jusqu'à quel point, le partage du secret médical (dans l'intérêt du

patient) augmentant les risques de violation de la confidentialité des données de santé, est-il opportun ?

Face aux risques encourus et au nom du droit suprême à la vie, passant par la santé de l'individu, il serait raisonnable de restreindre certains de ses droits dans son propre intérêt. Il serait difficile de profiter de tous les avantages des technologies de l'information et de la communication dans le domaine de la santé tout en jouissant de toutes ses libertés individuelles. Un choix s'impose dont le plus pertinent serait de privilégier l'intérêt supérieur représenté, dans ce cas, par l'intérêt thérapeutique du patient. Il ne serait pas question d'annihiler le droit à l'autodétermination informationnelle[1138] de l'individu mais les conditions de recueil du consentement du patient devraient être plus rigoureusement réglementées pour s'assurer de recevoir un accord éclairé de ce dernier.

S'agissant de l'opportunité du partage du secret médical, l'antinomie du secret médical partagé est admise par la loi pour l'intérêt thérapeutique du patient. En passant par le système du dossier médical personnel, les professionnels de santé prennent rapidement connaissance de l'essentiel des informations de santé. C'est un gain de temps et une meilleure connaissance du dossier du patient favorables au diagnostic et au traitement à lui administrer. « *Le DMP est au service de la coordination des soins et offre aux professionnels de santé la possibilité d'accéder à une information beaucoup plus complète sur leurs patients. Son utilisation est donc de nature à sécuriser et à renforcer davantage la prise de décision médicale ou l'orientation des soins*[1139].» Du point de vue médical, le partage du secret médical, à travers le dossier médical électronique paraît donc opportun même si des risques de divulgation des données médicales sont plus importants. Certaines dispositions pratiques pourraient permettre de réduire ces risques d'atteinte à la vie privée : Au niveau des techniciens de l'informatique, des dispositions légales et réglementaires devraient exiger que ne soient habilités à intervenir pour la mise en place du dispositif technique de télémédecine que ceux soumis au secret professionnel par leur appartenance à un ordre réglementé. Quant aux patients et aux professionnels de santé, l'ignorance ou le manque de culture informatique constitue une

[1138] « *pouvoir reconnu à l'individu de décider en premier lieu lui-même quand et dans quelle mesure des faits relatifs à sa propre existence sont divulgués* ». ROUVROY, A et POULLET, Yves. *Le droit à l'autodétermination informationnelle et la valeur du développement personnel-une réévaluation de l'importance de la vie privée pour la démocratie.* in État de droit et virtualité. BENYEKHEF, Karim et TRUDEL, Pierre (dir). Thémis 2009.

[1139] Asip santé. *Le DMP et la responsabilité médicale*. [en ligne] 14 juin 2011. Disponible sur http://esante.gouv.fr/services/reperes-juridiques/le-dmp-et-la-responsabilite-medicale. Consulté les 15 mai 2014.

source d'exposition aux intrusions indésirables dans les systèmes d'information. Une formation adaptée des professionnels de santé et des usagers appelés à utiliser les réseaux informatiques pour accéder directement aux dossiers médicaux pourrait leur permettre de contribuer à l'assurance de leur sécurité. Par ailleurs, des efforts supplémentaires devraient être faits du côté du législateur et du gouvernement. Pour rattraper le retard que l'on constate toujours entre l'évolution technologique et celle du droit ou, du moins, réduire l'écart, le législateur devra anticiper certaines réactions des individus pour s'adapter aux nouvelles technologies car le droit met du temps à s'appliquer. Ainsi que l'écrivait François OST : « *le droit, s'il veut exercer sa mission de médiation, a besoin de temps, à la fois au sens de la durée nécessaire à la réflexion, et au sens de la mise en perspective et de la prise de recul, seules susceptibles d'assurer la prise en compte d'une histoire sociale de long terme*[1140] »

D'un point de vue économique, l'objectif poursuivi par le gouvernement en mettant en place les applications de partage des données médicales est la réduction des dépenses de santé de l'assurance maladie. Théoriquement, ce plan est plein de bon sens vu qu'il tend à éviter les redondances d'analyses et de traitements, sources de dépenses supplémentaires inutiles. Mais à ce jour, le constat général dénoncé par les médias[1141], est que le projet dossier médical personnel engagé dans cet objectif a plus fait de dépenses que d'économie sans aucun résultat encourageant. Même si les chiffres ne sont pas concordants entre les données communiquées par l'assurance maladie et celles de l'Asip santé, un rapport de la Cour des Comptes remis à la Commission des finances de l'Assemblée nationale en février 2013 confirme cette thèse. Il estime à au moins 210 millions d'euros le coût du dossier médical personnel entre la loi de 2004 l'ayant instauré et fin 2011. «*Au total, le développement et la mise en place des dossiers médicaux personnels, sous différentes formes a vraisemblablement coûté plus d'un demi-milliard d'euros à fin 2011, essentiellement à la charge de l'assurance maladie*[1142].» Or, il y a

[1140] OST, François. « *Mémoire et pardon, promesse et remise en question. La déclinaison éthique des temps juridiques » in Le temps et le droit*. Actes du quatrième congrès de l'association internationale de méthodologie juridique. Québec. Y. BLAIS 1996, P. 30.

[1141] Par exemple, en s'appuyant sur un document interne du Conseil national de la qualité et de la coordination des soins, organisme qui dépend de l'assurance maladie, le quotidien "le Parisien", paru le 4 janvier 2014, affirme que le coût du dossier médical personnel s'élève à 500 millions depuis sa création en 2004. COFARD, Jacques. *Le dossier médical personnel (DMP) : beaucoup d'argent pour rien*? 23 janvier 2014. http://www.medscape.fr/voirarticle/3600266. Consulté le 15 mai 2014

[1142] Cour des comptes. *Communication à la Commission des finances de l'Assemblée nationale. Le coût du dossier médical personnel depuis sa mise en place.* Juillet 2012. p. 104. Disponible sur http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/134000136/0000.pdf. Consulté le 15 mai 2014.

un défaut d'évaluation et d'anticipation, dans le domaine, de la part du ministère de la santé qui peut déboucher sur des impasses financières et des blocages dangereux dans la mesure où aucune méthodologie rigoureuse d'évaluation médico-économique des gains de performance pour le système de soins et des économies pour l'assurance maladie n'est définie au stade actuel pour permettre d'estimer un retour sur investissement. Face à ce constat et devant les risques lourds d'abandon du déploiement du dossier médical personnel, les recommandations de la Cour des Comptes émises dans le rapport précité, en matière d'identification et de maîtrise des coûts sont à considérer avec beaucoup d'attention par les autorités compétentes. Elles consistent en quatre principaux points[1143] :

«1) Charger la délégation à la stratégie des systèmes d'information en santé, en lien avec l'ASIP et les ARS de rendre compte annuellement des dépenses effectuées pour la mise en place du DMP et de leur financement ;

2) veiller étroitement à la convergence entre le DMP et les derniers dispositifs des dossiers médicaux régionaux, ou à défaut, mettre un terme à tout financement direct ou indirect de ce dernier par l'assurance maladie ;

3) conclure avec l'ordre des pharmaciens et L'ASIP un protocole et un calendrier de rapprochement entre le DMP et le dossier pharmaceutique ;

4) développer une stratégie homogène d'homologation des certifications pour établissements et professionnels de santé incluant le DMP et diffuser les études comparatives de leur prix».

Il ne fait pas de doute que le gouvernement français prend des dispositions pour améliorer le cadre juridique et, de manière générale, toute la politique d'insertion des technologies de l'information et de la communication dans le domaine de la santé. Mais, si de telles dispositions peuvent permettre d'entrevoir des débuts de solutions aux problèmes de protection de la vie privée, au plan national, on a des doutes quant à leur efficacité au plan international. L'évolution du monde moderne favorise le partage des données médicales hors des frontières d'un même État. Idéalement, des mécanismes de régulation internationaux ayant force contraignante devraient permettre leur encadrement juridique en vue de la préservation des libertés individuelles. Pourtant, à ce jour, l'harmonisation des règles de protection des

[1143] Cour des comptes. *Communication à la Commission des finances de l'Assemblée nationale. Le coût du dossier médical personnel depuis sa mise en place.* Juillet 2012. p. 105. Disponible sur http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/134000136/0000.pdf. Consulté le 15 mai 2014.

données personnelles au plan international reste un défi majeur à relever. Des initiatives d'adoption de règlements communautaires comme celles prises par l'Europe sur la protection des données personnelles sont à encourager et à multiplier dans le reste du monde en attendant de trouver une solution universelle. Celle-ci devra commencer par un réexamen des lignes directrices[1144] régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel élaborées par l'OCDE il y a une trentaine d'années. Il faudrait également envisager d'associer tous les États y compris ceux en voie de développement, du fait de l'universalité d'Internet, à l'élaboration de nouvelles lignes directrices sur la protection des données personnelles. Les pays développés y gagneraient dans la mesure où de plus en plus d'hébergeurs ont recours aux services de sous-traitants établis à l'extérieur, dans des pays qui ne disposent pas toujours de législations protectrices de données personnelles.

Pour résoudre le problème de l'absence de législation sur la protection des données personnelles dans tous les États du monde, les États-Unis, par exemple, privilégient l'adoption de mécanismes d'autorégulation à travers des codes de bonne conduite. Une des initiatives les plus populaires est un procédé technique d'autorégulation: le projet du consortium «*World Wide Web plateform for privacy preferences (P3P)*[1145]». Ce projet est essentiellement animé par des entreprises américaines. Il est destiné à offrir à l'utilisateur final la possibilité de gérer lui-même la communication de ses données en fonction de la pratique énoncée et de ses préférences. Il s'agit d'une sorte de charte de bonne conduite adaptée à Internet. Chaque site souhaitant faire partie de cette communauté s'engage à respecter un certain nombre de règles déontologiques. Ces mécanismes sont appelés à être inclus et diffusés mondialement dans les prochaines versions de logiciels de navigation sur Internet. Des initiatives similaires pourraient être introduites dans le processus de sélection des sous-traitants des hébergeurs de données de santé domiciliés hors des États disposant d'une législation sur la protection des données personnelles. Ce serait un début de solution, mais nous pensons avec FENOLL-TROUSSEAU et HAAS que quoiqu'intéressante, cette initiative (même multipliée à travers le monde), ne pourrait réellement protéger l'individu que si « *toutes les personnes qui agissent dans le domaine des traitements de données personnelles sont soumises aux mêmes règles, aux mêmes principes de protection. De plus, ceci ne peut fonctionner, qu'à condition que tout*

[1144] OCDE. *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.* http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelavieprivee etlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm. Consulté le 26 mai 2014.

[1145] Le portail dédié à ce projet est: http://www.w3.org/P3P/. Consulté le 16 mai 2014.

le monde ait la même interprétation de ces règles. Il faudrait donc attendre un accord international adoptant un ensemble de règles précises pour que ces déclarations d'intention aient des effets réels[1146] ». On en revient donc toujours à la solution d'accords internationaux entre tous les États ; ce qui relève plus de l'utopie, en raison des réalités actuelles de disparité entre les législations. D'autant plus qu'il en existe[1147] mais que c'est leur efficacité qui est mise en cause.

Une autre solution serait la mise en place de moyens permettant d'instaurer une interopérabilité internationale sécuritaire entre tous les États en matière de données personnelles. Mais la tâche s'annonce ardue dans la mesure où, comme le précisait le Professeur LAVENUE, traitant de la question de l'interopérabilité en rapport avec la sécurité, il n'y a aucune garantie réelle de contrôle sur l'usage qui pourra être fait hors de l'Europe des fichiers transférés[1148] C'est pourquoi, de profondes réflexions sur la question restent nécessaires.

[1146] FENOLL-TROUSSEAU, Marie-Pierre, HAAS, Gérard. *Internet et protection des données personnelles*. Paris. Litec. 2000. p. 144.

[1147] La convention n° 108 du Conseil de l'Europe, les lignes directrices de l'OCDE adoptée en 1980, les directives conjointes OIT/OMS de 2005, etc.

[1148] LAVENUE, Jean-Jacques: *Administration électronique, interopérabilité et sécurité: les risques de l'ambivalence.* Annales des télécommunications, 2006. Volume 61, n° 7-8. p 819.

BIBLIOGRAPHIE

I. OUVRAGES, MANUELS ET MONOGRAPHIES

- ABADIE, Pascale. *Droits du patient : information et consentement*. Paris : Elsevier Masson, 2004. 158 p. Collection management hospitalier. ISBN : 2-294-01719-6. (br)
- AFNOR. *Lexique*. [en ligne]. Disponible sur: http://www.afnor.org/lexique/%28lettreid%29/n. Consulté le 19 mai 2014.
- ALLA, François, PY, Bruno. *Droits de la santé - textes juridiques.* Paris: PUF, 1997. Collection que sais-je ? Volume 3215. 127 p. ISBN : 2130480519, 9782130480518.
- ANCEL, Marie-Elodie. *La prestation caractéristique du contrat.* Paris : Économica, 2002. 394 p. ISBN : 2-7178-4359-0.
- AUBY, Jean-Marie. *Le droit de la santé*. Paris : PUF, 1981. Collection Thémis. 508 p. ISBN : 2-13-036847-6.
- BARREAU DU QUÉBEC. *Développements récents en droit de l'Internet*. Cowansville: Éditions Yvon Blais, 2001. 278p. ISBN : 2-89451-543-X.
- BENSOUSSAN, Alain, MOLE, Ariane. *Guide juridique du dossier médical informatisé*. Paris : MMI éditions - Masson, 2001. 135 p. Collection MEDIDROIT. ISBN : 2-901227-61-9.
- BENSOUSSAN, Alain. *Informatique et libertés*. Paris : Francis Lefebvre, 2ème édition, 2008. 862 p. ISBN : 978-2-85115-745-4. (rel).
- BUXERAUD, Jacques, CAULIER S., FLORY A. *Informatique et internet à l'officine*. Paris : Elsevier, 2000. Collection Actu Pharma. 127 p. ISBN 2-84299-175-3.
- CABY, Damien. AMIC, Etienne *Le système de santé français peut-il encore être sauvé ?*. Paris : MMI éditions.1ère édition, 1998. 103 p. Collection médistratégies. ISBN : 2-901227-39-2.
- CAMPANA Mireille. *La cryptographie* in TABATONI, Pierre. Groupe d'études société de l'information et vie privée. La protection de la vie privée dans la société d'information : L'impact des systèmes électroniques d'information. Tome 2. Paris : PUF, 2000. p. 54-62. ISBN : 2-13-051097-3. (br).
- CAPRIOLI, Eric A. *Doit international de l'économie numérique*. 2ème édition. Paris : Litec. Pratique professionnelle, 2007. 369p. ISBN : 978-2-7110-0774-5
- CHASSIGNEUX, Cynthia. *L'informatisation des dossiers médicaux et la protection des données de santé ou les enjeux du transfert des données médicales dans une perspective*

internationale. in Xe Séminaire d'actualité de droit médical, Université Paul Sabatier, DIU de droit médical, Toulouse, 9 et 10 juin 2005. Bordeaux : les Études hospitalières, 2007. p.67-86. ISBN : 978-2-84874-072-0

- CLEMENT, Jean-Marie. *Droit des malades : les répercussions de la loi du 4 mars 2002 dans le champ du droit hospitalier*. Bordeaux : Les Études Hospitalières, 2002. 87 p. Collection "essentiel". ISBN : 2-912359-75-9 (br).
- CNIL.
  - *Guide droit d'accès. Les guides de la CNIL*. [en ligne]. édition 2010. Disponible sur : www.cnil.fr. Consulté le 17 avril 2014.
  - *Guide du correspondant informatique et libertés*. [en ligne] Janvier 2006. 24 p. Disponible sur : www.cnil.fr/fileadmin/.../CNIL_Guide_correspondants.pdf. Consulté le 19 mai 2014.
  - *Renseignements pratiques sur les formalités préalables à la création d'un fichier de recherche médicale, chapitre IX*, édition d'Août 2007. [en ligne]. 9 p. Disponibles sur www.cnil.fr. Consulté le 6 mai 2014.
  - *Renseignements pratiques sur la procédure de déclaration de traitements de données à caractère personnel de santé à des fins d'évaluation ou d'analyse des pratiques de soins et de prévention, chapitre X*, édition de juillet 2006. [en ligne] 7 p Disponible sur www.cnil.fr. Consulté le 6 mai 2014.
- CONSEIL DE L'EUROPE. *Recommandation n° R (97) 5 adoptée par le Comité des ministres du Conseil de l'Europe le 13 février 1997.* Strasbourg : Édition du Conseil de l'Europe, 1997. 72 p. ISBN : 92-871-3333-6 (br.) EAN : 9789287133335.
- DE LAMBERTERIE, Isabelle, LUCAS, Henri-Jacques. *Informatique, Libertés et recherche médicale.* Paris : CNRS EDITIONS, 2001. 283 p. ISBN : 2-271-05881-3
- Dictionnaire le petit Larousse 2010.
- Dictionnaire. Le nouveau petit Robert de la langue française 2010. Paris : le Robert, Dalloz 2009.
- DUCROT, Henry. DUSSERRE (Liliane) *L'information médicale, l'ordinateur et la loi*. 2ème édition. Cachan : Éd. médicales internationales : Technique & documentation, 1999. 256 p. ISBN 2-7430-0339-1.
- DUGUET, Anne- Marie. *Dossier médical et données médicales de santé: protection de la confidentialité, conditions d'accès, échanges pour les soins et la recherche* in Xe Séminaire d'actualité de droit médical, Université Paul Sabatier, DIU de droit médical,

Toulouse, 9 et 10 juin 2005. Bordeaux : les Études hospitalières, 2007. 299 p. ISBN : 978-2-84874-072-0.

- DUPUY, Olivier. *L'information médicale 2ème édition ; information du patient et information sur le patient.* Bordeaux : Les Études Hospitalières, 2005. Collection " Tout savoir". 392 p. ISBN : 2-84874-011-6.
- DUPUY, Olivier :
  - *Le dossier médical.* Bordeaux : Les Études Hospitalières, 2002. 116 p. Collection essentiel. ISBN : 2-912359-83-X (br)..
  - *Le dossier médical et dossier médical personnel, supports complémentaires ou concurrents ?* in Xe séminaire d'actualité de droit médical. Université Paul Sabatier, DIU de droit médical, Toulouse, 9 et 10 juin 2005. Bordeaux : Les Études Hospitalières, 2007.
  - *La gestion des informations relatives au patient.* Bordeaux : Les Études Hospitalières, 2005. 224 p. ISBN : 978-2-84874-032-4.
- DUSSERRE, Liliane, ALLAERT, François-André. *La télémédecine est-elle légale et déontologique* ? in Information médicale : aspects déontologiques, juridiques et de santé publique. Volume 8. Paris, Berlin, New York: Springer, 1996. 183p. ISBN: 2-287-59638-0. (br).
- FAUCHOUX, Vincent. DEPREZ, Pierre. *Le droit de l'internet* : *lois, contrats et usages*. Paris : Litec, 2008.. 351 P. ISBN : 978-2-7110-1329-6 (br).
- FELCOURT, Guy de. *L'usurpation d'identité ou l'art de la fraude sur les données personnelles.* Paris : CNRS éditions. 314 p. Collection Ares. ISBN : 978-2-271-07243-6.
- FENOLL-TROUSSEAU, Marie-Pierre. HAAS, Gérard. *Internet et protection des données personnelles*. Paris : Litec, 2000. Collection Litec droit. 206 p. ISBN : 2-7111-3179-3.
- FÉRAL-SCHUHL, Christiane. *CYBERDROIT le droit à l'épreuve de l'internet.* Paris : Dalloz : Novembre 2006. 4ème édition. 732 p. ISBN : 2 247 06117 6.
- FERAUD-CIANDET, Nathalie. *Droit de la télésanté et de la télémédecine : à jour du décret du 19 décembre 2010 sur la télémédecine.* Paris : Dalloz, 2011. 158 p. Collection droit professionnel. ISBN : 978-2-85385-318-7 (br).
- FOREST, David. *Droit des données personnelles*. Paris. Gualino, Lextenso, 2011. 117p. Collection Droit en action. ISBN : 978-2-297-01502-8.

- GALLOUEDEC-GENUYS, Françoise, MAISL, Herbert. *Le secret des fichiers*. Paris: CUJAS, 1976. 328 p.
- GAUTRAIS, Vincent, TRUDEL, Pierre. *Circulation des renseignements personnels et Web 2.0*. Université de Montréal : Édition Thémis, 2010. 231 p. ISBN : 978-2-89400-280-3.
- GENTOT, Michel, Groupe d'études Société d'information et vie privée. *La protection des données personnelles à la croisée des chemins*, in *La protection de la vie privée dans la société d'information*, Tome 3. Paris : PUF. Collection Cah Acad Scien, 2002. 383 p. ISBN : 978-2130525387.
- GLOSSAIRE de l'anonymisation de données du groupe *Référentiels et Labels de l'AFCDP (Association française des correspondants à la protection des données à caractère personnel*) [en ligne]. 23 mai 2007. Disponible sur : http://www.afcdp.net/IMG/pdf/AFCDP_Glossaire_Anonymisation_070523.pdf. Consulté le 19 mai 2014.
- HAGEGE, Claude. *Précis d'informatique en biologie médicale*. Amsterdam: Elsevier, 1997. Collection Option/bio. Volume 1. 160 p. ISBN : 2-84299-004-8 (br)
- HERVEG, Jean, BEYLEVELD, Deryck, DUGUET, Anne- Marie. *La protection des données médicales - The protection of medical data, Les défis du XXIe siècle - Challenges of the 21st century*. Paris : LGDJ, Louvain-la-Neuve : Anthémis, 2008. 217 p, ISBN : 978-2-87455-122-2
- HERVEG, Jean.
  - *Introduction à la protection des données médicales en droit européen : Interdiction de traiter et exceptions* in Dossier médical et données médicales de santé. Paris : Les Études Hospitalières, 2007. p. 183-196.
  - *La gestion des risques spécifiques aux traitements de données médicales en droit européen.* in Système de santé et circulation de l'information, encadrement éthique et juridique. Paris : Dalloz, 2007. p. 79-103.
- HL7 (Health Level Seven). *Guides d'implémentation des normes HL7*. [en ligne]. 6 décembre 2010. Disponible sur http://www.mediboard.org/public/HL7. Consulté le 25 mai 2011.
- INFOROUTE SANTE CANADA. *Guide de l'unité collaborative de normalisation*. [en ligne]. Disponible sur : https://www.infoway-inforoute.ca/flash/lang-fr/scguide/docs/StandardsCatalogue_fr.pdf. Consulté le 26 mai 2011.

- JOLLY, Dominique. LANCRY, Pierre-Jean et LENOIR, Noëlle. *La médecine à l'épreuve de la société d'information*. Paris : IEPS, 1997. Collection Les Dossiers de l'Institut d'études des politiques de santé - 1275-7039. XIII- 71 p. ISBN/ISSN : 2-257-10622-9 (br).
- KAYSER, Pierre. *La protection de la vie privée par le droit, protection du secret de la vie privée*. 3ème édition. Aix-en-Provence : PUAM, Paris : Économica., 1995. 605 p. ISBN : 2-7178-2829-X.
- KIRBY, Michael. *La protection de la vie privée et des droits de l'homme à l'aide du numérique* in Les droits de l'homme dans le cyberespace. Unesco. Paris : Economica, 2005 Collection droit du cyberespace. P. 11-31. ISBN : 92-3-203979-b.
- LACOUR, Stéphanie. *La sécurité aujourd'hui dans la société de l'information.* Paris : L'harmattan, 2007. 279 p. ISBN : 2. 978-2-296-04276-6.
- LAVENUE, Jean-Jacques, BEAUVAIS, Grégory. *La commercialisation des données personnelles, perspectives et prospective : l'exemple des données de santé et du DMP*. in La sécurité de l'individu numérisé. CNRS. Paris : L'harmattan, 2009. P 163-182.
- LELEU, Yves-Henri, GENICOT, Gilles. *Le droit médical : Aspects juridiques de la relation médecin-patient. Bruxelles :* De BOECK université, 2001. 243 p. ISBN : 2-8041-3582-9.
- LEVESQUE, Emmanuelle. *L'accès aux informations de santé à des fins de recherche sans le consentement des patients : mise en parallèle de modèle québécois et français.* in Xe séminaire d'actualité de droit médical. Université Paul Sabatier, DIU de droit médical, Toulouse, 9 et 10 juin 2005. Bordeaux : Les Études Hospitalières. 2007. p. 208-221.
- MALLET-POUJOL, Nathalie. *Traçage électronique et libertés*. Paris : La Documentation française, Dalloz, 2006. 120 p. Collection "Problèmes politiques et sociaux
- MALAURIE, Philippe. *Les personnes, la protection des mineurs et des majeures*. Paris : Defresnois-Lextenso éd, Dalloz, 2009. 364 p. Collection "droit civil". 4ème édition. ISBN : 978-2-85623-153-1 (br).
- MARLIAC-NEGRIER, Claire. *La protection des données nominatives informatiques en matière de recherche médicale.* Aix-Marseille : PUAM, 2001. 2 volumes, 844 p. Collection du droit de la santé 1630-0076. ISBN : 2-7314-0247-4.
- MORANGE, Jean. *Manuel de droits de l'homme et des libertés publiques.* Paris : PUF, 2007. 278 p. ISBN : 978-13-055778-4

- NICOLAS, Guylène. *Le secret médical devant le juge administratif* in La déontologie médicale. Actes du cinquième colloque national de Droit, Histoire, Médecine. Aix-en-Provence (1er et 2 décembre 2006) sous la direction d'Antoine LECA. Aix-Marseille : PUAM, Juillet 2007. P 191-202. ISBN : 978-2-7314-0606-1.
- OST, François. « *Mémoire et pardon, promesse et remise en question. La déclinaison éthique des temps juridiques »* in Le temps et le droit. Actes du quatrième congrès de l'association internationale de méthodologie juridique. Québec : Y. BLAIS, 1996. P.15-31.
- PAUL, Daniel. *Le droit des technologies de l'information au Québec*. Montréal: Butterworths & company (canada) limited, 2008. LexisNexis. 222 p. ISBN : 978-0-433-45514-1.
- PENNEAU, Jean. *La responsabilité du médecin*. Paris: Dalloz, 2004. 3ème édition. 150 p. Collection " connaissance du droit". ISBN : 2-247-05477-3. (br).
- PERROT, Sandrine. *Le dossier médical personnel : un outil de la maîtrise des dépenses de santé souffrant d'imprécisions juridiques* in in Xe séminaire d'actualité de droit médical. Université Paul Sabatier, DIU de droit médical, Toulouse, 9 et 10 juin 2005. Bordeaux : Les Études Hospitalières. 2007. p 25-40.
- POULLET, Yves. ROUVROY, Antoinette. *Le droit à l'autodétermination informationnelle et la valeur du développement personnel une réévaluation de l'importance de la vie privée pour la démocratie* in État de droit et virtualité.[en ligne] Montréal:. Thémis, 2009. p. 157-222. Disponible sur : http://www.crid.be/pdf/public/6050. pdf. Consulté le 29 mars 2014.
- RIVERO, Jean. *Les Libertés publiques*. Vendôme : PUF, 1991. D18 p. Collection Thémis. Droit. 6e éd. (Tome 1)**.** ISBN : 2-13-044219 6.
- ROCHELANDET, Fabrice. *Economie des données personnelles et de la vie privée*. Paris. La Découverte, 2010. 125p. Collection Repères. ISBN : 978-2-7071-5765-2.
- ROCHFELD, Judith. *Les nouveaux défis du commerce électronique.* Paris : LGDJ, 2010. Lextenso éditions. Dalloz 2010. 206 p. ISBN : 978-2-275-03591-8.
- ROGUE, Evelyn*e Dictionnaire pratique de la cybersanté.* Paris: Éditions. médicales spécialisées, 1998. Collection Médistratégies, 1275-2797. 524 p. ISBN : 2901227198.
- ROQUES-BONNET, Marie-Charlotte. *Le droit peut-il ignorer la révolution numérique?* Paris: Michalon éditions, 2010. 606p. ISBN : 978-2-84186-553-6.

- SAISON, Johanne. *Droit hospitalier*. Deuxième édition. Paris : Galindo: Lextenso, 2009. 349 p. Collection " fonction publique concours". ISBN : 978-2-297-01229-4. (br).
- SAVATIER, René, AUBY, Jean-Marie, PEQUIGNOT, Henry et al. *Traité de droit médical*. Paris: Librairies techniques, 1956. 574 p.
- SWARTE, Martin de, BRUNEAU, Pierre,. *Guide pratique de l'informatisation du cabinet médical*. Paris : Éditions. médicales spécialisées, 1997. Collection Médistratégies, 1275-2797. 303 p. ISBN : 2901227112.
- TERRÉ, François. *Introduction générale aux droits.* 8ème édition. Paris : Dalloz, 2009. 656 p. Collection "Précis". ISBN : 978-2-247-08446-3. (br).
- TRUDEL, Pierre.
  - *Introduction à la loi concernant le cadre juridique des technologies de l'information.* Cowansville: Éditions Yvon Blais, 2012. 303 p. ISBN : 978-2-89635-870-0.
  - *La responsabilité civile sur Internet selon la loi concernant le cadre juridique des technologies de l'information.* In BARREAU DU QUÉBEC. *Développements récents en droit de l'Internet*. Cowansville:. Éditions Yvon Blais, 2001. 278p. ISBN :2-89451-543-X. P. 126-127.
- TÜRK, Alex. *La vie privée en péril : des citoyens sous contrôle*. Paris : O. Jacob, 2011. 269 p. ISBN : 978-2-7381--2279-7 (br).
- VIALA, François. *Les grandes décisions de droit médical*. Paris : LGDJ- Lextenso, 2009. 664 p. ISBN : 978-2-275-03470-6. (br).
- YAYA, Hachemi Sanni, RAFFELINI, Chiara. *Des souris et des médecins De la télémédecine à la cybermédecine* : *la science médicale du XXIe siècle entre l'organisation et la technologie.* Paris : Publibook, 2008. 165 p. ISBN : 978-2-7483-3956-7. (br)

II. THESES ET MEMOIRES

- ANAHORY, Michèle, VIALLA, François. *Les aspects juridiques du dossier médical personnel*. Thèse, Droit privé. Montpellier 1, 2006. 274 p.

- BRAMI, Grégory. *Protection des données patientes informatisées en médecine générale*. Thèse, Médecine. Paris VII, 10 juin 2009. 93p.
- CARMONA, Gérald. *Les impacts des nouvelles technologies de l'information sur le système de santé*. Mémoire de DEA. Bordeaux 4, 1996.
- CASSANAS, Geneviève. *Carte à mémoire protégée et dossier santé portable*. Thèse, Pharmacie. Montpellier 1, 1987.79 p.
- CATALA, Olivier. *Le dossier patient informatisé à l'officine*. Thèse, Pharmacie. Lyon 1, 2004.
- CHEVILLARD, Marie. *Le droit au masquage par le patient dans le cadre du dossier médical personnel en France.* Thèse. Médecine. Université Pierre et Marie Curie, Paris, 31 mai 2007. 172 p.
- COURPRON, Julie. *Du dossier médical partagé au dossier médical personnel : l'informatisation du dossier médical ou la question du traitement informatique des données de santé*. Mémoire de DESS, Droit de la santé. Bordeaux 4, 2005.
- CROELS Jean-Michel. *Le droit des obligations à l'épreuve de la télémédecine*. Thèse, Droit. Toulouse 1, 2004. 391 p.
- CROS, Sébastien, HANSEL Sylvie, et Université de Montpellier 1. UFR des sciences pharmaceutiques et biologiques. *Le dossier médical personnel : Réflexions sur le consentement et la confidentialité*. Thèse, Pharmacie. Montpellier 1, 2007. 95 p.
- DEMEAUX, Jean-Louis, CHELLE, Hervé. *Echange de données informatisées en médecine générale*. Thèse. Médecine générale. Bordeaux 2, 1998.
- DOUSSET, Laurent. *SMUR et informatique embarquée*. Thèse, Médecine. Toulouse 3, 2007.
- DURAND, Geneviève. *Communication et archivage des résultats d'analyses de biologie médicale en secteur hospitalier*. Thèse. Paris 11, 2001. 53f.
- FIGLAREK, Christophe. *L'utilisation de la cryptographie dans les échanges de données médico-sociales*.[en ligne] Mémoire, ENSP, Décembre 2000. 84p. Disponible sur : http://ressources.ensp.fr/memoires/2000/edh/ figlarek.pdf. Consulté le 20 mai 2014.
- GOYER, Aurélie. *Donne-t-on aux CIL les moyens de remplir leurs missions ?* [en ligne]. Thèse professionnel. Institut supérieur d'électronique de Paris, 2008-2009. Disponible sur : http://www.formationcontinue-isep.fr/informatiqueetlibertes/informatique-et-libertes-theses. Consulté le 20 mai 2014.

- LE GOFF-PRONOST, Myriam. *TIC, télémédecine et accès aux services : une approche économique***.** Thèse, Sciences économiques. Brest, 2003. 385 p.
- MALAURIE, Philippe. *Les contrats contraires à l'ordre public : Etude de droit civil comparé : France, Angleterre, URSS*. Thèse, Droit. Paris, 1951. Reims: Edition Matot-Braine, 1953. 278 p.
- QUILLATRE, Elisabeth. *Le dossier médical personnel. Du secret professionnel au contrôle par le patient.* Mémoire, Droit, informatique et libertés. Paris I, 24 septembre 2007. 161 p.
- ZORN-MACREZ Caroline. *Données de santé et sécurité partagée : pour un droit de la personne à la protection de ces données de santé partagée*. Presses universitaires de Nancy. Collection « santé, qualité de vie et handicap ». Thèse, Droit privé et sciences criminel remaniée, soutenue le 5 décembre 2009 à l'université de droit de Nancy. Nancy, octobre 2010. 502 p. ISBN : 978 - 2 - 8143 - 00 25-5.

III. ETUDES DOCTRINALES ET ARTICLES

➢ PUBLICATIONS EN VERSION PAPIER

- AUBERT de VINCELLES, Carole. *Compétence internationale en matière de cyberconsommation : précision sur la notion d'activité dirigée. R*evue des contrats n° 2, 1er Avril 2011, LGDJ, Lextenso éditions, p. 511-517.

- BACACHE-GIBEILI, Mireille. *Le secret médical partagé*. Gazette du palais, 30 décembre 2008 n° 365. p. 44.

- BASTIDE, Rémi. BES, Marie-Pierre. DEFOSSEZ, Adrien. *La problématique de l'isolement du patient en hospitalisation à domicile : une approche par l'analyse sociologique des réseaux*. Les cahiers de la télésanté, vers l'âge de raison… Éthique, déontologie, juridiques, économiques, 2009, p. 53-57.

- BENSOUSSAN, Alain, POTTIER, Isabelle. *Le décret du 20 octobre 2005 : l'acte de naissance du correspondant à la protection des données à caractère personnel*. Gazette du palais, 25-26 janvier 2006, p. 13-16.

- BERTRAND, Jean-Marie. *Un cadre juridique pour favoriser le développement de la télémédecine*. Les cahiers de la télésanté, vers l'âge de raison... Éthique, déontologie, juridiques, économiques, 2009, p. 8-12.

- BLAISE Jean-Bernard, HUET Jérôme, *Commerce électronique et code de commerce*. Le bicentenaire du code de commerce. Université de Paris II. Dalloz 2008, p. 9/24

- BLIN, Marc. *Où mènent les nouvelles technologies.* Professions santé infirmier infirmière n° 37, Mai 2002, p. 6.

- BONAÏTI-PELLIE, Catherine, ARVEUX, Patrick. *Traitement de l'information en matière de recherche dans le domaine de la santé, nul n'est censé ignoré la loi*. *M*édecine/Sciences 2009 n°1, volume 25, Janvier 2009, p 93-97.

- BOURCIER, Danièle. *Données sensibles et risque informatique : de l'intimité menacée à l'identité virtuelle*. Questions sensibles. CNRS (CURAPP), PUF, 1998. p. 39-58.

- BRAC DE LA PERRIÈRE, Marguerite, FERRÉ, Elise. *L'hébergement de données de santé : des textes à la pratique*. Gazette du palais, Recueil juillet-août 2011. p 2035-2039.

- CALLENS, Stefaan. *Les questions légales à l'ordre du jour de la télémédecine*. Les dossiers européens. Le défi de télémédecine en Europe, n° 20, Juin-Juillet 2010, p. 40-41.

- CAYOL, Jérôme. *Contenu du dossier médical en psychiatrie*. Gazette du palais, 1er-4 juin 2011, p. 32-33.

- CHAFIOL CHAUMONT, Florence.
  - *Données personnelles Bruxelles reprend la main ! Éclairage sur le projet de règlement de la Commission européenne qui intéresse au plus haut point aussi bien les entreprises que les citoyens.* Expertise des systèmes d'information. n° 367, mars 2012, P. 99.
  - *3 questions. Protection des données personnelles : propositions de la Commission européenne*. Semaine juridique entreprise et affaires,. n° 10 du 8 mars 2012, p. 5.

- CHAVRIER, Géraldine. *Le renforcement des obligations de motivation des arrêtés d'hospitalisation d'office et de celles relatives au respect du droit à la vie privée*. La semaine juridique administrations et collectivités territoriales. n° 30. 19 juillet 2004. p. 1027-1029.
- CRESSARD, Piernick. *L'actualité de notre secret médical*. Bulletin de l'ordre des médecins. Février 2006. n°2, Éditorial.
- DE LAMBERTERIE, Isabelle. *Informatique, libertés et opinions religieuses.* Archives des sciences sociales des religions 1995, n° 91 (Juillet-septembre). p 21-39.
- DECAUX, Emmanuel. *La protection de la vie privée au regard des données informatiques*. Droits fondamentaux, n° 7, janvier 2008-décembre 2009, p. 7.
- DESMARAIS, Pierre. *La télémédecine, source de nouveaux cas de responsabilité in* communication commerce électronique n° 9, septembre 2011, Étude 16.
- DUBOIS, Olivier. *La loi du 1er juillet 1994 et ses conséquences déontologiques.* Informatique de santé. n° 8, 1996, p 3-7.
- EYSENBACH G. *What is e-health?* Journal Medical Internet Research. 2001 April –June, 3(2):E20.
- FALQUE-PIERROTIN, Isabelle. *Les données personnelles représentent le pétrole du numérique.* Expertises des systèmes d'information. n° 366. Février 2012. p 49-54.
- FAURAN, B. *Loi informatique et libertés et données de recherche dans le domaine de la santé*. Gazette du palais 2006,1, Doctrine, p.1698.
- FERRAUD-CIANDET, Nathalie. *L'Union européenne et la télésanté.* Revue Trimestrielle de droit européen, n° 3 du 1er juillet 2010, p. 537-561.
- FERAUD-CIANDET, Nathalie. *Questions juridiques sur la e-santé.* Petites affiches, n° 89. 03 mai 2007, p. 11-14.
- FONTAINE, Marie. *La lente mise en place de la contribution forfaitaire aux frais de gestion due par les professionnels de santé qui ne télétransmettent pas les feuilles de soins*. Gazette du palais. 1er-4 juin 2011, p. 46-47.

- FORGERON, Jean-François, BÉNÉAT, Anne-Lise. *De la santé électronique à l'hôpital numérique*. Gazette du palais, 21 et 22 octobre 2009, p 5-8.
- GAGNEUX, Michel. *Les concepts : dossier patient partagé, dossier du professionnel et dossier médical personnel* Bulletin juridique du praticien hospitalier, Septembre 2008, n° 110. p. 15-21. ISSN : 1625-4104.
- HERVEG, Jean. *Quelle est la nature du consentement du patient dans le traitement de données médicales en droit européen*. Rex Medicinae, n° 10, 2008. p 15-38.
- ISNARD, Michel. *Statistiques et libertés individuelles : les apports récents de la loi*. Courrier des statistiques. Mars-juin 2005, n° 113-114, p. 9-13.
- JOB, Jean -Marie. *La loi informatique et libertés et des données de santé.* Revue Lamy droit de l'immatériel du 1er janvier 2008, n° 34, p.34-44.
- JURISCLASSEUR ADMINISTRATIF. Fasc. 274. *Informatique. Traitement de données à caractère personnel*. Cote : 3,2008. 31 janvier 2008, 10 p.
- KULLING, Gabriel. *L'accès au dossier médical hospitalier par le médecin-conseil de l'assurance-maladie.* Revue générale de droit médical, n° 37, Décembre 2010, p 227-234.
- LAVENUE, Jean-Jacques : *Administration électronique, interopérabilité et sécurité : les risques de l'ambivalence.* Annales des télécommunications, 2006, Volume 61, n° 7-8. p 809-829.
- LECLERC, Xavier. « *Le CIL est celui qui parle toutes les langues de l'entreprise* ». Interview recueilli par Sylvie ROZENFELD. Expertise des systèmes d'information. n° 368, Avril 2012, p. 130-135.
- LE TARNE, Libre. 8 avril 2011. *Plasosoins, pour une meilleure coordination de l'aide à domicile.* Actes de la journée de télésanté 2011 du jeudi 31 mars 2011 en France et en francophonie. p. 38.
- LECOZ. Pierre. *Avis du CCNE à propos des questions soulevées par l'informatisation des données de santé*. Revue générale de droit médical n° 37, décembre 2010, p 198-203.

- LY. Ousmane. *L'Antim : un vrai tournant*. Les cahiers de la Télésanté. Hôpital, patients, santé, territoire. Vers plus de mobilité, d'autonomie et de bien-être ? Télésanté 2010, p. 19.
- MALLET-POUJOL, Nathalie. *La loi du 1er juillet 1994 : contraindre ou convaincre ?*, Revue de droit informatique et télécoms 1995. n° 1, p. 20.
- MICHEL, Laurent. *Secret médical et dossier informatisé*. Louvin médical n° 120. Belgique, 2001. p. S131.
- MOLE, Ariane, BENSOUSSAN, Alain. *La loi informatique et liberté modifiée : les nouveaux pouvoirs de la CNIL sur l'évaluation des pratiques de santé.* Gazette du palais du 19 octobre 1999, II, Doctrine, p 1461-1465.
- NERBONNE S. La loi du 6 Août 2004. *Les régimes d'autorisation pour le secteur privé.* Communication commerce électronique, février 2005, paragraphe II. A. 4.
- NICOLAS, Guylène. *L'accès au dossier hospitalier par le patient et sa famille : les cas particuliers (patients mineurs, majeurs protégés, patients décédés)*. Revue générale de droit médical n° 37, décembre 2010, p. 185-196.
- PATTYNAMA, Peter M. *Aspects juridiques de la télémédecine transfrontalière.* Les dossiers européens. Juin - juillet 2010, n° 20, Le défi de la télémédecine en Europe, p. 38-39.
- PERRAY, R. *Traitement de données personnelles dans le cas des recherches médicales : vers un allégement des formalités.* Revue Lamy droit de l'immatériel, février 2007, p. 64
- POTTIER, Isabelle. *Le traitement des données personnelles dans le cadre des plans de continuité d'activité en période de pandémie grippale*. Gazette du palais, 21 22 octobre 2009, p. 9-10.
- QUANTIN, Catherine, GOYON, Béatrice et al. *Méthodologie pour le chaînage de données sensibles tout en respectant l'anonymat : application au suivi des informations médicales.* Courrier des statistiques, mars-juin 2005, n° 113-114, p. 15-25.
- RENE. Louis. *Le secret dans le nouveau code pénal,* Editorial. Bulletin de l'ordre des médecins, décembre 1992, n° 12, p. 229-230.

- ROUSSET, Dominique. *Le dossier pharmaceutique, une expérience originale d'informatisation en santé*. Gazette du palais, 22-24 novembre 2009, p. 3438-3442.
- SAMUELIAN, Jean-Claude, BOYER, Laurent. *Le dossier en psychiatrie : l'exemple d'un dossier patient informatisé*. Revue générale de droit médical, n° 37, décembre 2010. p. 204-212.
- SCHAFFNER, M. et SROUSSI G. *Responsabilité des hébergeurs : une responsabilité sans définition fixe*. Revue Lamy Droit de l'immatériel 2010, 1er octobre 2010, n° 64, p. 33 - 38.
- SCHOETTL, Jean-Eric. *La réforme de l'assurance maladie devant le Conseil Constitutionnel*. Les petites affiches. 15 septembre 2004, n° 185, p 6-18.
- SEGUR, Philippe. *Confidentialité des données médicales. À propos des enquêtes de santé*. AJDA, 25 avril 2004, p 858-862.
- SICARD, Didier. *Quelles limites au secret médical partagé ?* Dalloz 2009, p. 2634.
- STEFANI, François. *Le patient doit être maître de son secret*. Bulletin de l'ordre des médecins, n° 3, mars 2005, p. 4.
- THOUMYRE, Lionel. *Les hébergeurs en ombres chinoises. Une tentative d'éclaircissements sur les incertitudes de la loi pour la confiance dans l'économie numérique*. Revue Lamy droit de l'immatériel, mai 2005, n° 5. p. 58-65.
- VERNIER, Marie-Hélène. *Médecine à distance. Grand messe de la télémédecine aujourd'hui à travers 16 villes de France et de l'étranger reliées en visioconférence. Dont Besançon.* Télésanté 2011. Actes de la journée internationale de la télésanté du jeudi 31 mars 2011 en visioconférence en France et en francophonie. p. 50.
- VIRALLY, Michel. *La valeur juridique des recommandations des organisations internationales.* Annuaire français de droit international, Volume 2, 1956, p 66 – 96.
- VOISIN, Gabriel. *Protection des données à caractère personnel divulgation : de la proposition de règlement de l'UE*. Expertise des systèmes d'information, n° 365, janvier 2012, p. 15-17.

- WILLIATE-PELITTERI, Lina. *Les autres risques du doit. L'impact du décret du 7 mai 2012 sur la relation médecin - patient : un retranchement à regretter ? Décret n° 2012-6947 du 7 mai 2012 portant modification du code de déontologie médicale. Droit et risque n°4 (1ère partie)*. Les petites affiches, n° 10, 14 janvier 2013, p. 6.

- WORMS, Gérard. *Dans cinq ans, la télétransmission sera devenue un réflexe naturel*. Le quotidien du médecin, n° 6629 du 24 janvier 2000. p. 8 et10.

➢ PUBLICATIONS EN VERSION NUMERIQUE

- ACCENTURE.
  - *Doctors Survey: Us Country Profile*. [en ligne], Novembre-décembre 2012. 30 p. Disponible sur: http://www.accenture.com/SiteCollectionDocuments/PDF/Accen ture-Doctors-Survey-US-Country-Profile-Report.pdf. Consulté le 21 mai 2014.
  - *Étude Accenture menée auprès des médecins : changement de tendance en France en matière d'informatique médicale*. [en ligne], 7 juin 2013. Disponible sur: Http:// www.accenture.com/fr-fr/Pages/insight-acn-doctors-survey-profile-he. Consulté le 2 mai 2014.
- ACPM. *Les dossiers de santé électroniques: perspectives de la responsabilité médicale*. [en ligne], Août 2008. p. 5. Disponible sur: http://www.cmpa-acpm.ca/cmpapd04/ docs/submissions_papers/pdf/com_electronic_health_records-f.pdf. ou sur www.cmpa-acpm.ca. Consulté le 18 septembre 2013.

- AGENCE NATIONALE D'ACCREDITATION ET D'EVALUATION EN SANTE (ANAES).
  - *Le dossier du patient en ergothérapie*.[en ligne], mai 2001 p.16. Disponible sur: http://www.hassante.fr/portail/upload/docs/application/pdf/ergoth_rap.pdf. Consulté le 10 août 2012.
  - *Evaluation des pratiques professionnelles dans les établissements de santé. Dossier patient : Amélioration de la qualité, de la tenue et du contenu*. [en ligne], Juin 2003. p. 3. Disponible sur : http://www.hassante.fr/portail/upload/docs/application/pdf/

200908/dossier_du_patient_amelioration_de_la_qualite_de_la_tenue_et_du_contenu_-_reglementation_et_recommandations_-_2003.pdf. Consulté le 2 septembre 2012.

- AGENCE REGIONALE DE SANTE AQUITAINE. *« Hôpital, patients, santé, territoires » le droit à la croisée de nombreuses attentes*. [en ligne] Septembre 2009. Disponible sur : www.ars.aquitaine.sante.fr. Consulté le 2 mars 2013.

- AMBLARD, Philippe. AUROUX, Jean-Baptiste. *L'hébergeur en application de la loi du 1er Août 2000/ L'hébergeur en application de la LCEN du 21 juin 2004*. [en ligne] Lamy droit des médias et de la communication. Partie 4. Titre 2. Etudes 476-6 et 476-7. Disponible sur : http://lamyline.lamy.fr. Consulté le 20 mai 2014.

- AMELI. *A quel type d'informations le médecin peut-il accéder ?* [en ligne], 1er août 2011. Disponible sur : http://www.ameli.fr/assures/soins-et-remboursements/l-historique-des-remboursements/qu-est-ce-que-l-historique-des-remboursements.php. Consulté le 12 mars 2012.

- ANTOINE, P. *Maîtriser la complexité*. [en ligne], Projet. 1973. p. 1192. in Rapport du sénateur THYRAUD, Jacques. 10 novembre 1977. n° 72. p.3. Disponible sur http://www.senat.fr/rap/l77-072/l77-0721.pdf. Consulté le 25 avril 2014.

- ASIP SANTE

  - *AAPC DMP1 et hébergement*. [en ligne], 11 février 2010. Disponible sur : http://esante.gouv.fr/en/asip-sante/marches-publics/attributions-de-marche/aapc-dmp1-et-hebergement. Consulté le 12 décembre 2013.

  - *Cadre d'interopérabilité des SIS, document chapeau*. [en ligne], 16 novembre 2010. 16 p. Disponible sur : http://esante.gouv.fr/sites/default/files/CI-SIS_Document_Chapeau_v1.0.1.pdf. Consulté le 2 novembre 2011.

  - *Cadre d'interopérabilité des systèmes d'information de santé*. [en ligne], 3 février 2001. Disponible sur : http://esante.gouv.fr/referentiels/interoperabilite/cadre-d-interop erabilite-des-systemes-d-information-de-sante-ci-sis. Consulté le 18 août 2009.

- *Cadre d'interopérabilité des systèmes d'information de santé.* [en ligne], 8 décembre 2013. Disponible sur : http://esante.gouv.fr/contenu/cadre-d-interoperabilite-des-systemes-d-information-de-sante-ci-sis. Consulté le 21 avril 2014.

- *Cadre d'interopérabilité des SIS. Evolutions du CI-SIS depuis la version 1.0.1. Note de version.* [en ligne], 14 novembre 2012. Disponible sur : http://esante.gouv.fr/sites/default/files/CI-SIS_NOTE-DE-VERSION_V1.3.1.pdf. Consulté le 21 avril 2014.

- *Calliope : mettre l'interopérabilité en partage.* [en ligne], 30 juillet 2010. Disponible sur : http://esante.gouv.fr/dossiers/calliope-mettre-linteroperabilite-en-partage. Consulté le 21 mai 2014.

- *Cancérologie et coordination de soins : Déploiement du DCC : l'ASIP santé et l'INCA retiennent les 7 régions pilotes*. [en ligne], Communiqué de presse. Paris, 11 janvier 2011. 3 p. Disponible sur : http://esante.gouv.fr/sites/default/files/Communique_de_presse_11_01_11_regions_phase_pilote_DCC_DMP.pdf . Consulté le 30 avril 2014.

- *CPS 3, une nouvelle étape pour la e-santé.* [en ligne], mars 2011. 10p. Disponible sur : http://esante.gouv.fr/sites/default/files/DP_CPS.pdf. Consulté le 2 janvier 2012.

- *Déploiement du DMP : l'ASIP Santé apporte son soutien à 33 établissements.* [en ligne], 22 décembre 2011 Disponible sur : http://esante.gouv.fr/actus/dmp/deploiement-du-dmp-l-asip-sante-apporte-son-soutien-a-33-etablissements-mise-a-jour. Consulté le 30 avril 2014.

- *Ehealth-interop veut normaliser la e-santé européenne*. [en ligne], 13 juillet 2010. Disponible sur : http://esante.gouv.fr/dossiers/ehealth-interop-veut-normaliser-la-e-sante-europeenne. Consulté le 3 juin 2011.

- *Étude sur la télésanté et télémédecine en Europe.* [en ligne], Mars 2011. Disponible sur : www.esante.gouv.fr. Consulté le 2 octobre 2012.

- *Hébergement de données de santé : le point sur le renouvellement de l'agrément* [en ligne] ,17 septembre 2013. Disponible sur : http://esante.gouv.fr/en/node/4201. Consulté le 21 janvier 2014.

- *Hébergeurs agréés*. [en ligne], 20 mai 2014. Disponible sur : http://esante.gouv.fr/ services/referentiels/securite/hebergeurs-agrees. Consulté le 21 mai 2014.
- *INS compatibilité* : *Liste des logiciels référencés pour le calcul de l'INS-C*. [en ligne], 13 octobre 2013. Disponible sur: Http://esante.gouv.fr/services/referentiels/identi fication/ins-compatibilite-liste-des-logiciels-references-pour-le-calcul. Consulté le 23 octobre 2013.
- *L'essentiel sur la CPS 3.* [en ligne], 2 mars 2011. Disponible sur : http://esante. gouv.fr/sites/default/files/Fiche_LEssentielsurlaCPS3_020311.pdf. Consulté le 21 mai 2014.
- *L'Union européenne investit dans la e-santé de ses États membres.* [en ligne], 21 juin 2010. Disponible sur : http://esante.gouv.fr/dossiers/l-Union-europeenne-sinvestit-dans-la-e-sante-de-ses-etats-membres#comments. Consulté le 15 décembre 2012.
- *La CPS, carte d'identité électronique pour les professionnels de santé.* [en ligne], 26 avril 2010. Disponible sur : http://esante.gouv.fr/espace-cps/guide/la-cps-carte-d-identite-electronique-des-professionnels-de-sante. Consulté le 14 septembre 2011.
- *La m-health permettrait d'économiser 99 milliards d'euros en Europe en 2017*. [en ligne], 3 octobre 2013. Disponible sur : http://esante.gouv.fr/actus/services/la-m-health-permettrait-d-economiser-99-milliards-d-euros-en-europe-en-2017. Consulté le 17 mai 2014.
- *L'agrément des hébergeurs de données de santé à caractère personnel.* [en ligne], 7 février 2011. Disponible sur : www.esante.gouv.fr. Consulté le 10 octobre 2013
- *Lancement du dossier santé Québec dans la région de Montréal*. [en ligne], 21 février 2012. Disponible sur : Http://esante.gouv.fr/actus/politique-publique/ lancement-du-dossier-sante-quebec-dans-la-region-de-montreal. Consulté le 18 septembre 2013.
- *Le DMP et la responsabilité médicale*. [en ligne] 14 juin 2011. Disponible sur : http://esante.gouv.fr/services/reperes-juridiques/le-dmp-et-la-responsabilite-medica le. Consulté le 15 mai 2014.
- *Le Mali, pionnier de la e-santé en Afrique.* [en ligne], Le MAG n° 11. 19 février 2014. Disponible sur : http://esante.gouv.fr/en/node/4321. Consulté le 21 avril 2014.

- *Le Québec à l'honneur des huitièmes journées internationales des industriels*. [en ligne], 15 décembre 2011. Disponible sur : Http://esante.gouv.fr/actus/services/le-quebec-a-l-honneur-des-8emes-journees-nationales-des-industriels. Consulté le 31 mai 2012.

- *Le rôle de l'agence des systèmes de santé dans la procédure d'agrément*. [en ligne], 23 novembre 2011. Disponible sur : http://esante.gouv.fr/services/reperes-juridiques/le-role-de-l-agence-des-systemes-d-information-partages-de-sante-dans-la. Consulté le 11 octobre 2013.

- *Les certificats CPS*. [en ligne], 12 juin 2012. Disponible sur : http://esante.gouv.fr/services/espace-cps/les-certificats-cps. Consulté le 22 octobre 2013.

- *Les raisons d'être et le cadre réglementaire de l'INS-C*. [en ligne], 11 juillet 2010. Disponible sur : http://esante.gouv.fr/referentiels/identification/les-raisons-d-etre-et-le-cadre-reglementaire-de-l-ins. Consulté le 9 octobre 2011.

- *L'identifiant national de santé (INS) prend ses marques et progresse sur le marché des logiciels de santé.* [en ligne], Communiqué de presse du 18 octobre 2010. Disponible sur : http://esante.gouv.fr/sites/default/files/CP_INS_Pointreferencements CNDA_181010.pdf. Consulté le 28 avril 2014.

- *Mise en œuvre du service DCC et DMP cible 2013-2015*. [en ligne], Septembre 2013. 24 p. Disponible sur : http://esante.gouv.fr/sites/default/files/ServiceDCC duDMP_Cible2013_2015_Septembre2013.pdf. Consulté le 30 avril 2014.

- *Note juridique relative à l'hébergement de données de santé à caractère personnel aux dossiers détenus par les PSAD et les distributeurs de DM*. [en ligne], 21 mars 2012. Http://esante.gouv.fr/services/reperes-juridiques/note-juridique-relative-a-l-hebergement-de-donnees-de-sante-a-caractere-. Consulté le 1er novembre 2013.

- *Présentation du répertoire national des référentiels (RNR).* [en ligne], 10 décembre 2013. Disponible sur : http://esante.gouv.fr/services/referentiels/presen tation-du-repertoire-national-des-referentiels-rnr/presentation-du-reper. Consulté le 21 avril 2014

- *Programme de relance du DMP et des systèmes d'information partagée de santé : Orientations stratégiques et principes de mise*[en ligne], Avril 2009. 112 p. Disponible sur : http://esante.gouv.fr/sites/default/files/Programme_de_relance_DMP_et_SIS_Avril_2009.pdf. Consulté le 18 février 2011.
- *Qu'est-ce que la carte CPS?*. [en ligne], 5 mai 2014. Disponible sur : http://esante.gouv.fr/services/espace-cps/qu-est-ce-que-la-carte-cps. Consulté le 21 mai 2014.
- *Référentiels pour les SI de santé : Point de situation, Evolutions, maintenance*. [en ligne], 8 février 2011. Disponible sur : http://esante.gouv.fr/sites/default/files/110208_JNI_JFP_PGSSI_Referentiels_1.pdf. Consulté le 26 mai 2011.
- *Signature de convention de partenariat entre l'ASIP Santé et l'ANAP*. [en ligne], Communiqué de presse du 20 mai 2010. Disponible sur : http://esante.gouv.fr/sites/default/files/CP_ASIPSante_ANAP_200510.pdf. Consulté le 28 avril 2014.
- *Une agence d'Etat*. [en ligne], Publié le 08 mai 2010. Disponible sur : http://esante.gouv.fr/asip-sante/qui-sommes-nous/une-agence-d-etat. Consulté le 15 février 2010.
- *Une nouvelle étape dans la mise en œuvre du dossier médical personnel*. [en ligne], Communiqué de presse, 18 février 2010. Disponible sur : http://esante.gouv.fr/sites/default/files/CP_notification_hebergeur18022010.pdf. Consulté le 12 décembre 2013.
- *Une première étape pour un identifiant national adapté à l'échange et au partage de données de santé*. [en ligne], communiqué de presse, 9 juin 2010. Disponible sur : Http://esante.gouv.fr/sites/default/files/CP_INS_ConventionASIP_CNDA_090610_0.pdf. Consulté le 17 janvier 2011

- ASSOCIATION NATIONALE DE TELEMEDECINE. *Déclaration du docteur ANTEZANA, Fernando en décembre 1998 à Genève.* [en ligne], Disponible sur : http://www.antel.fr/doc/Rapport_final_Telemedecine.pdf. Consulté le 27 février 2011.

- BENHAMOU Albert-Claude. *Colloque DMP, éthique et confiance : synthèse des travaux du colloque*. [en ligne], 4 décembre 2006. Disponible sur : http://www.portailtelesante.org/article.php?sid=1358. Consulté le 15 décembre 2013.

- BERLEUR, Jacques. *Vingt ans de lois relatives à l'informatique. Quels acquis ? Quels défis ? En tout cas, encore un long chemin…*[en ligne], Journal de réflexion sur l'informatique n° 17. 1991. P. 41. Disponible sur : http://www.anthologieprivacy.be/sites/anthology/files/Vingt_ans_de_lois_relatives_%C3%A0_l%27informatique._Quels_acquis%3F_Quels_d%C3%A9fis%3F_En_tout_cas%2C_encore_un_long_chemin_....pdf. Consulté le 28mars 2014.
- BONAÏTI-PELLIE, Catherine, ARVEUX, Patrick. *Traitement de l'information en matière de recherche dans le domaine de la santé : nul n'est censé ignoré la loi.* [en ligne], Médecine/Science. n° 1, volume 25, Janvier 2009, p. 93-101 Disponible sur : http://www.scribd.com/doc/ 31033917/CCTIRS-MS-2009. Consulté le 5 avril 2014.

- BOSSI, Jeanne. *Les questions autour du dossier médical personnel*[en ligne], ADSP n° 58 mars 2007. p.31-32. Disponible sur : http://www.hcsp.fr/Explore.cgi/Telecharger?NomFichier=ad583033.pdf. Consulté le 10 décembre 2013.

- BOUCHARD, Marie, BOURQUE Gilles L., LEVESQUE, Benoît, avec la collaboration d'Élise Desjardins *L'évaluation de l'économie sociale dans la perspective des nouvelles formes de régulation socio-économique de l'intérêt général.* [en ligne], Octobre 2000. 28p. Cahiers du crises. n° ET0013. Disponible sur : https://depot.erudit.org/id/001694dd. Consulté le 20 juillet 2013.

- BOUCHER, Philippe. *Une division de l'informatique est créée à la chancellerie "Safari" ou la chasse aux Français.* [en ligne]. Le Monde. 21 Mars 1974. Disponible sur http://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html?xtmc=safari_ou_la_chasse_aux_francais&xtcr=113. Consulté le 21 mai 2014.

- BRAC DE PERRIERE, Marguérite. DELANNOY, Tiphaine. *Obligation de chiffrement et hébergeur de données de santé* [en ligne], Juristendances informatique et télécoms, n° 120, Février 2012. Disponible sur : http://www.alain-bensoussan.com/wp-content/uploads/225044221.pdf. Consulté le 23 avril 2014.

- BRETON, Pascal. *Réponse ministérielle relative à l'inscription du droit au respect de la vie privée dans la Constitution*. [en ligne], Legalnews.fr, id ref. de l'article : 226777. 18 janvier 2010. Disponible sur : http://www.legalnews.fr/index.php?option=com_content &view=article&id=226777 :inscription-du-droit-au-respect-de-la-vie-privee-dans-la-constitution&catid=1152:protection-de-la-vie-privee&Itemid=646. Consulté le 14 juin 2012.

- CAHUN-GIRAUD, Sévérine. *La téléprescription dans le cadre de la régulation médicale. De nouvelles recommandations*. [en ligne], 17 juin 2010. Disponible sur : http://www.macsf .fr/vous-informer/teleprescription-regulation-medicale.html. Consulté le 27 octobre 2011.

- CANNASSE, Serge. Entretien de Hardy Anne-Chantal. *Le colloque singulier, un mythe français*. [en ligne], Carnets de santé. Juin 2013. Disponible sur : http://www.carnets desante.fr/Hardy-Anne-Chantal. Consulté le 20 novembre 2013.

- CATEL. *Une nouvelle approche du médico-social.* Hôpital, patients, santé, territoires : vers plus de mobilité d'autonomie et de bien-être ? [en ligne], Les cahiers de la télésanté 2010. p. 31 – 32. Disponible sur http://www.catel.pro/pagePresse.php. Consulté le 30 avril 2014.
- CHASSANG, Michel. *DMP : Attention danger !* [en ligne], 28 novembre 2006. Editorial. Disponible sur : http://www.csmf.org/upload/File/Edito/2006/edito_061128.pdf. Consulté le 20 janvier 2014.

- CIL. *Quelques repères juridiques pour les données à caractère personnel dans les banques de données de langues parlées en interaction.* [en ligne]. 24 mai 2012. Disponible sur http://www.cil.cnrs.fr/CIL/spip.php?article1646. Consulté le 6 mai 2014.

- CNIL :
  - *Clôture de la mise en demeure adoptée à l'encontre du centre hospitalier de Saint-Malo*. [en ligne], 17 octobre 2013. Disponible sur : www.cnil.fr. Consulté le 22 octobre 2013.

  - *Cloud computing. Les 7 étapes pour garantir la confidentialité des données.* [en ligne], 1er Juillet 2013. Disponible sur : http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/cloud-computing-les-7-etapes-cles-pour-garantir-la-confiden

tialite-des-donnees/ ? tx_ttnews%5BbackPid%5D=91&cHash=dd8b5d43c25748c47847f5cef5e8417a. Consulté le 2 mai 2014.

- *Cloud computing: la CNIL engage le débat*. [en ligne], 11 Octobre 2011. Disponible sur : http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-la-cnil-engage-le-debat/. Consulté le 2 mai 2014.

- *Conclusions de la Commission de l'informatique et des libertés sur l'utilisation du NIR comme identifiant de santé*. [en ligne], 20 février 2007. Disponible sur http://www. cnil.fr/fileadmin/documents/approfondir/dossier/NIR/Rapport%20NIR. pdf. Consulté le 19 janvier 2011.
- *Courrier de clôture de la mise en demeure du centre hospitalier Saint-Malo*. [en ligne], Recommandation AR n° 2C054 549 79070. Paris, 17 octobre 2013. Disponible sur : Http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/courrier/courri er_ de_cloture_MED_CH_ST-MALO.pdf. Consulté le 22 octobre 2013
- *La CNIL autorise le déploiement du dossier médical personnel sur l'ensemble du territoire*. [en ligne], 14 décembre 2010. Disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-cnil-autorise-le-deploiement-du-dossier-medical-personnel-sur-lensemble-du-territoire/. Consulté le 3 mars 2011.
- *La CNIL demande une utilisation encadrée du NIR pour faciliter la recherche médicale*. [en ligne], 11 janvier 2011. Disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/lutilisation-encadree-du-nir-par-les-chercheurs-et-les-autorites-sanitaires-un-veritable-enje/. Consulté le 12 février 2011
- *La CNIL sanctionne la déclaration mensongère d'un hébergeur de données de santé*. [en ligne], 9 janvier 2012. Disponible sur : www.cnil.fr. Consulté le 11 octobre 2013.

- *Le G 29 publie un avis sur les techniques d'anonymisation*. [en ligne], 16 avril 2014. Disponible sur : http://www.cnil.fr/nc/linstitution/actualite/article/article/le-g-29-publie-un-avis-sur-les-techniques-danonymisation/?utm_source=rss&utm_medium=rss&utm_campaign=le-g-29-publie-un-avis-sur-les-techniques-danonymisation-cnil-Commission-nationale-de-linformatique-et-des-liberts. Consulté le 19 avril 2014.

- *L'état des lieux en matière de procédés d'anonymisation*. [en ligne], 18 juillet 2008. Disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article//letat-des-lieux-en-matiere-de-procedes-danonymisation/. Consulté le 17 Août 2010.
- *Méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales*. [en ligne], Octobre 2010. 17p. Disponible sur : http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/sante/MR-001.pdf. Consulté le 18 avril 2014.
- *Quel identifiant pour le secteur de la santé ? La CNIL propose la création d'un numéro spécifique généré à partir du NIR mais anonymisé*. [en ligne], 20 février 2007. Disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/quel-identifiant-pour-le-secteur-de-la-sante-la-cnil-propose-la-creation-dun-numero-specifiqu/. Consulté le 17 février 2011.
- *Renseignements pratiques sur les formalités préalables à la création d'un fichier de recherche médicale.* [en ligne], Août 2007, 9 p. Disponible sur : http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/sante/chapIX.pdf. Consulté le 21 mai 2014.
- *Séminaire « open data, quels enjeux pour la protection des données personnelles ? »* [en ligne], Compte rendu, 9 juillet 2013. p. 4 Disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/OpenData/CR_Workshop_Open_Data_9_juillet_2013.pdf. Consulté le 13 juin 2014.
- *Un exemple de registre exclusivement destiné à l'information du public : le fichier des démarcheurs financiers.* [en ligne], 25 mars 2005. Disponible sur: www.cnil.fr/.../un-exemple-de-registre-exclusivement-destine-a-linformation-du-public-le-fichier-des-demarcheu/. Consulté le 11 janvier 2010.
- *Un pas vers le droit à l'oubli*. [en ligne], Avril 2005. Disponible sur : http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/un-pas-vers-le-droit-a-loubli-bancaire/. Consulté le 3 mars 2010.

- CNOM.
  - *Article 50, Secret partagé avec les médecins conseils des organismes d'assurance maladie*. [en ligne], 11 octobre 2012. Disponible sur : http://www.conseil-national.

medecin.fr/article/article-50-secret-partage-avec-les-medecins-conseils-de-la-securite-sociale-274. Consulté le 22 janvier 2014.

- *Historique des remboursements de l'assurance maladie : l'ordre des médecins demande des garanties*. [en ligne], 4 septembre 2007. Disponible sur : http://www.conseil-national.medecin.fr/article/historique-des-remboursements-de-l-assurance-maladie-l-ordre-des-medecins-demande-des-garanties-62. Consulté le 12 mars 2012.

- *Masquage des données : le CNOM rappelle que le DMP est le dossier personnel du patient*. [en ligne], 7 février 2007. Disponible sur : Http://www.conseil-national. medecin.fr/article/masquage-des-donnees-le-cnom-rappelle-que-le-dmp-est-le-dossier-personnel-du-patient-603. Consulté le 17 janvier 2014
- *Les préconisations du Conseil national de l'ordre des médecins*. [en ligne], Télémédecine. Janvier 2009. [en ligne] 21 p. Disponible sur : http://www.youscribe. com/catalogue/manuels-et-fiches-pratiques/savoirs/autres/telemedecine-212794. Consulté le 12 mai 2014.

- *Résultats du sondage de mars 2011* [en ligne], *in* Newsletter médecins 8 avril 2011. Disponible sur : http://www.conseil-national.medecin.fr/newsletter/2011/4. Consulté le 29 avril 2014.

- CNOP : *quels sont les droits des patients* ? [en ligne], Dépliant-patient. P. 3. Rubrique du site du Conseil de l'Ordre des pharmaciens : Disponible sur: http://www.ordre. pharmacien.fr/Le-Dossier-Pharmaceutique/Quels-sont-les-droits-des-patients. Consulté le 20 septembre 2011.
- COFARD, Jacques. *Le dossier médical personnel (DMP) : beaucoup d'argent pour rien* ? [en ligne], 23 janvier 2014. Disponible sur : http://www.medscape.fr/voirarticle/3600266. Consulté le 15 mai 2014.

- COMMISSION EUROPEENNE
  - *Consultation concernant une action communautaire dans le domaine des services de santé*. Communication [en ligne], Bruxelles, le 26 septembre 2006. SEC (2006) 1195/4. Disponible sur : http://ec.europa.eu/health/ph_overview/co_operation/ mobility/docs/comm_health_services_comm2006_fr.pdf. Consulté le 2 octobre 2011.

- *Mettre en œuvre le programme communautaire de Lisbonne. Les services sociaux d'intérêt général dans l'Union européenne*. [en ligne], Communication. Bruxelles, le 26 avril 2006. {SEC(2006) 516} ou COM(2006) 177. Disponible sur : http://ec. europa.eu/employment_social/social_protection/docs/com_2006_177_fr.pdf. Consulté le 02 Octobre 2011.

- COMYN. Gérard, Commission européenne. *Compte rendu de la table ronde du 5 décembre 2008.* [en ligne], p. 21. Disponible sur : http://www.eu2008.fr/webdav/site/ PFUE/shared/import/1205_Interoperabilite_medicale/Interoperabilite_medicale_compte_rendu_(FR).pdf. Consulté le 21 mars 2011.

- CONSEIL D'ETAT. *Fichiers informatiques. Communiqué de presse du Conseil d'Etat.* [en ligne], 11 avril 2014. Disponible sur : http://www.conseil-etat.fr/fr/communiques-de-presse/ fichiers-informatiques.html. Consulté le 25 avril 2014.

- CONSEIL CONSTITUTIONNEL. *Libertés et ordre public* « *Les principaux critères de limitation des droits de l'homme dans la pratique de la justice Constitutionnelle* » [en ligne], 8ème séminaire des cours Constitutionnelles tenu. Erevan du 2 au 5 octobre 2003. Disponible sur : www.conseil-constitutionnel.fr/. Consulté le 27 janvier 2014.

- COPIN, Charles. *Où en est-on de l'identifiant santé ?* [en ligne], Idem magazine, avril 2011. Disponible sur : http://www.wmaker.net/menaces/idem-magazine/archives/2011/4. Consulté le 30 Août 2011.

- COULOMB, Alain. *Rapport au ministre de la santé sur les conditions et modalités de mise en œuvre du dossier médical personnel*. [en ligne], Roissy, du 14 au 16 octobre 2004. p. 12. Disponible sur : www.esante.gouv.fr. Consulté le 14 février 2014.

- CSSSPNQL. *Premières nations du Québec. Plan stratégique de télésanté 2007-2010.* [en ligne], Décembre 2007. p. 9 ISBN: 978-0-9784554-0-8. Disponible sur : http://www. cssspnql.com/docs/centre-de-documentation/plan-strat%C3%A9gique-t%C3%A9l%C3% A9sant%C3%A9-pn-2007-10-fr.pdf?sfvrsn=2. Consulté le 29 avril 2014.

- DE MORANT, Guillaume. *Europe : les archivistes en alerte* [en ligne], Le Mag Coulisse des archives. p. 16. rfg. n° 205 Avril- Mai 2013. Disponible sur : Http://www.cil.cnrs.fr/ CIL/IMG/pdf/coulisses_des_archives_rfg_205.pdf. Consulté le 9 avril 2014.

- DEGOULET, Patrice et FIESCHI, Marius. *Traitement de l'information médicale. Méthodes et applications hospitalières.* [en ligne], Paris, Masson, 1991. Chapitre 10 : informatisation des dossiers médicaux. 27 mars 2010 par USMCS. Disponible sur : http://www.lescentresdesante.com/article115.html. Consulté le 17 janvier 2012.

- DELIS. *Selon quelles modalités peut-on assurer la confidentialité du nouveau dossier médical informatisé ? Garantissez la confidentialité de vos données médicales informatisées.* [en ligne], Development Institut International Paris, les 20-21janvier 2000. Disponible sur : http://www.delis.sgdg.org/menu/sante/diidospat.htm. Consulté le 5 avril 2014.

- DGCIS SNITEM. *Elaboration d'une politique de normalisation en France pour l'interopérabilité des dispositifs médicaux*. [en ligne], 1er Novembre 2010. Disponible sur : http://www.industrie.gouv.fr/portail/chiffres/tic-et-sante/politique-de-normalisation-vf.pdf Consulté le 02 mars 2011.

- DIRECTION DE L'INFORMATION LEGALE ET ADMINISTRATIVE.

  - *Dossier médical personnel : vos avis sur son contenu*. [en ligne], 7 novembre 2006. Disponible sur : http://www.vie-publique.fr/actualite/alaune/dossier-medical-personnel-vos-avis-son-contenu.html. Consulté le 27 décembre 2013.

  - *Qu'est-ce que le principe de subsidiarité ?* [en ligne], Vie publique 14 janvier 2013. Disponible sur : http://www.vie-publique.fr/decouverte-institutions/Union-europeenne/fonctionnement/france-ue/qu-est-ce-que-principe-subsidiarite.html. Consulté le 21 mai 2014.

- DMP.gouv.fr. Espace patient. *Mon médecin ajoute des documents dans mon DMP*. [en ligne], Disponible sur:.http://dmp.gouv.fr/web/dmp/patient/mon-medecin-ajoute-des-documents-dans-mon-dmp. Consulté le 3 mars 2011.

- DROIT MEDICAL.COM. *Interopérabilité des systèmes informatiques de santé européens.* [en ligne], 10 décembre 2008. Disponible sur : http://droit-medical.com/actualites/4-evolution/322-interoperabilite-systemes-informatiques-sante-europeens#ixzz1OaO7KMqX Consulté le 15 février 2009.

- DUSSERRE, Liliane. *La sécurité des échanges électroniques d'informations médicales nominatives entre médecins.* [en ligne], Rapport adopté lors de la session du Conseil national de l'ordre des médecins avril 2001. Disponible sur : http://www.conseil-national.medecin.fr/sites/default/files/echangeselectroniques.pdf. Consulté le 12 mai 2014.

- EL KALAM, Anas Abou, DESWARTE, Y, TROUESSIN, G CORDONNIER, E. *Gestion des données médicales anonymisées : problèmes et solutions in 2ème Conférence Francophone en Gestion et Ingénierie des Systèmes Hospitaliers (GISEH'04), Mons, 9-11 septembre 2004.* [en ligne], 16 p. Disponible sur : http://irt.enseeiht.fr/anas/recherche.htm. Consulté le 5 avril 2014.

- E-PRACTICE EDITORIAL TEAM. *National patient summary users are satisfied, says survey.* [en ligne], 23 mars 2012. Disponible sur : www.epractice.eu/en/news/5347051. Consulté le 21 mai 2014.
- FRASLIN Jean-Jacques.
  - *Interopérabilité médicale : La France aux abonnés absents*. [en ligne], 13 janvier 2009. Disponible sur : http://www.i-med.fr/spip.php?article280. Consulté le 17 octobre 2011.
  - *11 millions d'euros pour le « web zinzin* ». [en ligne], 16 septembre 2008. Disponible sur : http://www.i-med.fr/spip.php?article221. Consulté le 21 mai 2013.
  - *Pas d'année zéro pour le DMP québécois ! Le dossier de santé du Québec (DSQ) patine dans une pharmacie en attendant sa généralisation en 2011*. [en ligne], 29 mars 2010. Disponible sur : http://www.i-med.fr/spip.php?article380 Consulté le 18 mai 2012.
  - *Le CNOM souhaite un néo-DMP sincère et construit par les médecins.* [en ligne], 9 février 2008. Disponible sur : www.i-med.fr. Consulté le 13 mai 2012.
- GENTOT, Michel. *La protection des données personnelles à la croisée des chemins, La protection de la vie privée dans la société d'information.* [en ligne], chapitre 1 du tome 3 23 p. Disponible sur : http://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr1.pdf. Consulté le 11 février 2014.
- GIP ASIP Santé. *L'essentiel sur le DMP au service de votre pratique professionnelle*. [en ligne], Disponible sur : www.dmp.gouv.fr. Consulté le 6 décembre 2011.

- GIP DMP *:*

  - *Cadre d'interopérabilité des systèmes d'information de santé*. [en ligne], 29 juin 2009. Disponible sur : http://www.i-med.fr/spip.php?article347. Consulté le 9 octobre 2011.
  - *DMP, Le dossier médical personnel. Dossier de presse du colloque national DMP : éthique et confiance*. [en ligne], 4 décembre 2006. p.21. Disponible sur : http://www.unrs.fr/doc/ACTUALITES/dossier_presse_colloqueDMP.pdf. Consulté le 20 décembre 2013.
- GIPSPSI. *Le livre de présentation du système de santé en France*. [en ligne], Chapitre 1. Décembre 2013. Disponible sur : www.gipspsi.org. Consulté le 20 février 2014.
- GROUPE DE TRAVAIL INTEROP. *Interopérabilité*. [en ligne], Bordeaux 13 février 2010. Disponible sur : http://aful.org/ressources/presentation/perspectives-interoperabilite/preview_html ? file=file&file_html=file_html&file_html_subfiles=file_html_subfiles. Consulté le 07 février 2011.
- GUGLIELMI, Gilles J : *Le passeport français n'est plus électronique mais biométrique*. [en ligne], 4 mai 2008. Disponible sur : http://www.guglielmi.fr/spip.php?article131. Consulté le 27 mars 2014.
- HAUTE AUTORITE DE SANTE. *Encadrer la téléprescription dans le cadre de la régulation médicale*. [en ligne], Lettre d'information n° 19 de novembre – décembre 2009. Disponible sur : http://www.has-sante.fr/portail/jcms/c_887837/encadrer-la-teleprescription-dans-le-cadre-de-la-regulation-medicale. Consulté le 15 novembre 2011.
- HOUSE OF COMMONS, Health committee. *The electronic Patient Record*, sixth report of session 2006-2007. Volume 1, ordered by the House of Commons to be printed 25 july 2007. p. 21. HC 422, published on the 13 September 2007. [en ligne], disponible sur: http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422.pdf. Consulté le 3 octobre 2013.
- INFIRMIERS.COM. *Une "société interprofessionnelle de soins ambulatoires" pour les professionnels de santé libéraux*. [en ligne], 18 décembre 2012. Disponible sur : http://www.infirmiers.com/votre-carriere/ide-liberale/une-societe-interprofessionnelle-de-soins-ambulatoires-pour-les-professionnels-de-sante-liberaux.html. Consulté le 28 avril 2014.

- INSTITUT NATIONAL DU CANCER. *Recommandations nationales pour la mise en œuvre du dispositif d'annonce du cancer dans les établissements de santé : Mesure 40 du plan cancer*. [en ligne], Novembre 2005. p.2. Disponible sur : www.e-cancer.fr

- IRCAD, France Telecom, Computer Motion. *« Opération LINDBERG » Une première mondiale en télé-chirurgie : le geste chirurgical a traversé l'atlantique*. [en ligne], Conférence de presse 19 septembre 2001. p. 3/13. Disponible sur : http://www.ircad.fr/event/lindbergh/lindbergh_presse_fr.pdf. Consulté le 2 mars 2012.

- KAUDER, Serge. *Les lois "Informatique et Libertés" en France, en Europe et dans le monde.* [en ligne], 16 décembre 2003. Disponible sur : http://www.net-iris.fr/blog-juridique/44-serge-kauder/8501/les-lois-informatiques-et-libertes-en-france-en-europe-et-dans-le-monde. Consulté le 11 août 2011.

- LA REVUE TELESANTE. *L'amélioration de l'accès aux soins passe par le déploiement de la télémédecine*. [en ligne], Interview accordée par la Présidente Ghislaine ALAJOUNINE. Disponible sur : http://www.jiqhs.fr/wp-content/uploads/2010/12/Résumé-télémédecine_Ghislaine-Alajouanine.docx. Consulté le 29 avril 2014.

- LAUSSON, Julien. *La CNIL favorable à l'inscription du droit à l'oubli numérique dans la Constitution.* [en ligne], Numerama magazine. 24 novembre 2009. Disponible sur : http://www.Numerama.com. Consulté le 29 mars 2014.

- LDH Toulon. *Il y a 30ans, G.A.M.I.N ou l'oubli de l'humain*. [en ligne], 20 juin 2009. Disponible sur : http://www.ldh-toulon.net/spip.php?article3353. Consulté le 29 mars 2014.
- LDH Toulon. *La doctrine de la CNIL concernant les identifiants.* [en ligne]. 9 avril 2009. Disponible sur http://ldh-toulon.net/la-doctrine-de-la-Cnil-concernant.html. Consulté les 18 mai 2014.
- Le monde. *Comprendre le programme "prism"*. [en ligne], 11 juin 2013. Disponible sur : www.lemonde.fr. Consulté le 2 mai 2014.

- LESSIS (Les entreprises des systèmes d'informations sanitaires et sociaux). *Données personnelles de santé, un masquage des données de santé au service de tous les acteurs*. [en ligne], LESSIS-janvier 2007. Disponible sur : www.lesiss.org. Consulté le 15 Août 2013

- MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX. *Bonne nouvelle ! Le dossier santé Québec bientôt partout au Québec !* [en ligne], Dépliant d'informations sur le dossier santé Québec. Mai 2013. P.2 ou site Internet : Disponible sur : http://www. dossierdesante.gouv.qc.ca. Consulté le 30 juillet 2013.

- MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX DU QUEBEC. *Dossier santé du Québec, rapport d'étape Septembre 2008*. [en ligne], 40 p. Disponible sur : http://collections.banq.qc.ca/ark:/52327/bs1811704. Consulté le 26 mai 2012.
- MINISTERE DE LA SANTE. *Présentation des opérations retenues au titre du plan hôpital 2012*. [en ligne], Dossier de presse, 10 février 2010. p.1. Disponible sur : http://www.sante.g du mercredi 10 févrierouv.fr/IMG/pdf/Dossier_de_presse_100210-Hopital2012.pdf. Consulté le 5 mars 2014.

- MINISTERE DES AFFAIRES ETRANGERES. *Les dossiers médicaux électroniques : plus de la moitié des médecins américains sont "high-tech"*. [en ligne], Bulletins-electroniques.com. 31 mai 2013. Disponible sur : http://www.bulletins-electroniques. com/actualites/73132.htm. Consulté le 21 avril 2014.

- MINISTERE DU TRAVAIL, DE L'EMPLOI ET DE LA SANTE. Plaquette HPST *Une ambition nécessaire pour préserver le système de santé*. [en ligne], 8 p. Disponible sur: http://www.sante.gouv.fr/IMG/pdf/Plaquette_HPST_grand_public-2.pdf. Consulté le 22 mai 2014.

- MINISTERIO DE SANIDAD, SERVICIO SOCIALES E IGUALIDAD. *La tarjeta Sanitad Individual tendrá un formato único y será interoperable en todas las Comunidades Autónomas*. [en ligne], Disponible sur http://msc.es/gabinete/notasPrensa.do?id=2993. Consulté le 22 avril 2014.

- OFFICE FEDERAL DE LA SANTE PUBLIQUE. *Cybersanté (e-health) questions-réponses*. [en ligne], 16 octobre 2007. P.4. Disponible sur : www.e-health-suisse.ch/faq/ 00052/index.html?lang=fr&download. Consulté le 16 septembre 2011.

- ONU en partenariat avec l'IUT (Union internationale des télécommunications). *Les télécommunications et la santé.* [en ligne], Les télécommunications en action, chapitre 2.

Disponible sur : http://www.regency.org/t_in_act/pdf/french/health.pdf. Consulté le 29 avril 2014.

- PAQUEL, Norbert. *Interopérabilité des systèmes, le syndrome de la tour de Babel*. [en ligne] TLM n° 31 avril 1998. Informatique de santé : enjeux, formation continue. Disponible sur : http://www.tlmfmc.com/site/dossiers_detail.tpl?sku=305082874372600 &sku2=305082906273448. Consulté le 22 mai 2014.

- PICOT, Jocelyne. *Plan opérationnel pour la télésanté au Québec*. [en ligne], Document de travail préparé par la Direction générale des services de santé et médecine universitaire du Ministère de la santé et des services sociaux et présenté à inforoute santé du Canada. 2 février 2006. Volume 1. P. 7-8. Disponible sur : http://www.medicine.mcgill.ca/ruis/docs/ telesante/plan_op_telesante.pdf. Consulté le 22 mai 2014.

- PRADEAU, F. *Le dossier du patient dans les établissements de santé : tenue, contenu, archivage et communication.* [en ligne], p.1. Disponible sur : http://membres.multimania .fr/pradeau/exposes/DosMed/dossier_medical_synthese_011015.pdf. Consulté le 2 janvier 2012.
- SALEM, Géraldine. *La qualité de vie des patients atteints de maladies chroniques : Aspects comparés des systèmes français, suédois, canadien et américain* [en ligne], in Rapport 2010. Disponible sur: www.fondationroche.org. Consulté le 04 juin 2012.

- SARRAMON, J.P. *Médecine : médecin – malade. World congress on telemedecine for the development of the global information society for health.* [en ligne], Toulouse. Du 30 Novembre au 1er Décembre 1995. in L'apport des nouvelles technologies de l'information et de la communication au service de la santé en Afrique dans le cadre du NEPAD. 21 février 2002. p. 24. Disponible sur : http://www.asmp.fr/travaux/gpw/nouveltecno/ rapport. pdf. Consulté le 30 avril 2014.

- SERVICE PUBLIC. *Contenu du dossier médical*. [en ligne], 11 juin 2012. Disponible sur: http://m.vosdroits.service-public.fr/particuliers/F12207.xhtml. Consulté le 22 mai 2014.

- SIMITIS, Spiros. *Les données sensibles revisitées. Examen des réponses au questionnaire du Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE)* [en ligne], Strasbourg, 24-

26 novembre 1999. Disponible sur : http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Simitis_1999_fr.pdf. Consulté le 9 mai 2014.

- TICSANTE.COM. *La DGOS prépare un plan national de déploiement de la télémédecine*. [en ligne], 1er décembre 2010. Disponible sur : http://www.ticsante.com/la-DGOS-prepare-un-plan-national-de-deploiement-de-la-telemedecine-NS_801.html. Consulté le 29 avril 2014.

- TRUDEL, Pierre. *Améliorer la protection de la vie privée dans l'administration électronique : pistes afin d'ajuster le droit aux réalités de l'État en réseau*. [en ligne], CRDP. Université de Montréal. 52 p. Mars 2003. Disponible sur : http://www.chaire lrwilson.ca/cours/drt6929d/egouvMRCI23-06.pdf. Consulté le 22 mars 2014.

- UNION DES CONSOMMATEURS. *Le dossier de santé électronique : le contrôle des données personnelles de santé dans un contexte d'informatisation des dossiers médicaux*. [en ligne], 31 mars 2010. p. 10. Disponible sur : http://Uniondesconsommateurs.ca/docu/vieprivee/100331UC_CVPC_DSE.pdf. Consulté le 26 mai 2012.

IV. TEXTES, DOCUMENTS ET PUBLICATIONS OFFICIELLES

TRAITÉS INTERNATIONAUX

- Déclaration universelle des droits de l'homme. [en ligne], Paris, 10 décembre 1948. Disponible sur : http://www.unesco.org/education/nfsunesco/doc/droits_homme.htm. Consulté le 22 mai 2014.

- Pacte international relatif aux droits civils et politiques. [en ligne]. New York, 16 novembre 1966. JORF du 1er février 1981, p. 398. Disponible sur : http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19810201&numTexte=&pageDebut=00398&pageFin=. Consulté le 31 mars 2014.

PUBLICATIONS DES ORGANISMES INTERNATIONAUX

OCDE

- *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*. [en ligne], 23 septembre 1980. Disponible sur : http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelavie priveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm. Consulté le 22 mai 2014.

- *Recommandation sur les biobanques et bases de données de recherche en génétique humaine*.[en ligne], 2009. 57 p. Disponible sur : www.oecd.org/dataoecd/41/1/44054924. pdf. Consulté le 22 mai 2014.

OMS

- *Cinquante huitième assemblée mondiale de la santé, neuvième séance plénière de la Commission sur la cybersanté.* [en ligne], Genève 16-25 mai 2005, WHA58/.2005/REC/1. 173 p. Disponible sur: http://apps.who.int/gb/ebwha/ pdf_files/WHA58/WHA58_28-fr.pdf. Consulté le 2 Septembre 2011.

- *Déclaration sur la promotion des droits des patients en Europe.*[en ligne] Amsterdam, 28-30 mars 1994. ICP/HLE 121, 28 juin 1994. 15 p. Disponible sur: http://www. who.int/genomics/public/eu_declaration1994.pdf. Consulté le 27 décembre 2013

- *Rapport de la Consultation internationale de* l'OMS du 11 au 17 décembre 1997. Genève. Publication WHO/DGO/98.1 1998. Document EB 101/INF. DOC/9.

- *Rapport du secrétariat. Cybersanté : terminologie normalisée*.[en ligne] 25 mai 2006. Document EB118/8. Disponible sur : http://apps.who.int/gb/ebwha/pdf_files/EB118/B118_ 8-fr.pdf. Consulté le 22 mai 2014.

CNUCID

- Loi type de la CNUCID sur le commerce électronique et guide pour son incorporation. 1996 avec l'article 5 bis tel qu'adopté en 1998. [en ligne], New York 1999, 91 p. ISBN : 92-1-233323-0. Disponible sur: http://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf. Consulté le 22 mai 2014.

AMM

- Déclaration d'Helsinki. *Principes éthiques applicables à la recherche médicale impliquant les êtres humains*. [en ligne], Helsinki, Juin 1964. Disponible sur : http://www.wma.net/fr/30publications/10policies/b3/index.html. Consulté le 05 octobre 2010.

LÉGISLATION EUROPÉENNE

- Charte européenne *des droits fondamentaux*.[en ligne], Nice, 7 décembre 2000. JOCE 18 décembre 2000, C 364/1. Disponible sur : http://www.europarl.europa.eu/ charter/pdf/text_fr.pdf. Consulté le 3 avril 2014.
- Convention pour *la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*. [en ligne], Strasbourg, 28 janvier 1981. Disponible sur : http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm. Consulté le 3 avril 2014
- Convention de Rome n° 80/934/CEE du 19 juin 1980 sur *la loi applicable aux obligations contractuelles*. JOCE n° C 027 du 26 janvier 1998, p. 0034-0046.
- Convention européenne de *sauvegarde des droits de l'homme et des libertés fondamentales.* [en ligne], Rome, 4 novembre 1950. Disponible sur : http://conventions.coe.int/Treaty/fr/Treaties/Html/005.htm. Consulté le 22 mai 2014.
- Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 *relative à l'application des droits des patients en matière de soins de santé transfrontaliers*. JOUE n° L 88 du 4 avril 2011. p. 45–65.

- Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 *relative aux services dans le marché intérieur*. JOUE L 376, p 36 -68.
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 *relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« directive sur le commerce électronique »). JOCE n° L 178 du 17 juillet 2000, p. 0001-0016.
- Directive 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*. JOCE n° L 204 du 21 juillet 1998, p. 0037–0048.
- Directive 98/48/CE du Parlement européen et du Conseil *portant modification de la directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques.* JOCE n° L 217 du 5 Août 1998, p. 0018-0026.
- 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*. JOCE n° L 281 du 23 novembre 1995, p. 0031–0050.
- Directive 91/250/CEE du Conseil des communautés européennes, du 14 mai 1991, *concernant la protection juridique des programmes d'ordinateur***.** JOCE n° L 122 du 17 mai 1991, p. 0042 – 0046.
- Proposition de règlement du parlement européen et du Conseil *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 (règlement général sur la protection de données)*. [en ligne], Bruxelles, 25 janvier 2012. Disponible sur : http://eurlex.europa.eu/LexUriServ/ LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Consulté le 22 mai 2014.
- Règlement (CE) n° 44/2001/ du Conseil du 22 décembre 2000 *concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale.* JOUE 16 janvier 2001, n° L 012, p. 0001-0023.
- Traité d'Amsterdam *modifiant le traité sur l'Union européenne, les traités instituant les communautés européennes et certains actes connexes*. [en ligne], Amsterdam, 2 octobre 1997, JOCE C/340/, 10 novembre 1997. Disponible sur http://www.ecb.europa.eu/ ecb/legal/pdf/amsterdam_fr.pdf. Consulté le 22 mai 2014.

- Traité de Lisbonne *modifiant le traité sur l'Union européenne et le traité instituant la communauté européenne*. Lisbonne, 13 décembre 2007. JOUE C 306 du 17 décembre 2007.
- Traité pour le *fonctionnement de l'Union européenne*. Version consolidée au JOUE n° C 326 du 26 octobre 2012. p.0001-0390.

PUBLICATIONS DU PARLEMENT EUROPEEN

- Résolution législative du Parlement européen sur la 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. [en ligne], 12 mars 2014. Disponible sur : http://www.europarl.europa.eu/sides/getDoc.do ?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR. Consulté le 11 septembre 2014.

PUBLICATIONS DU CONSEIL DE L'EUROPE

- Position commune n° 1/95 du 20 février 1995 *en vue de l'adoption de la directive relative à la protection des personnes physiques à l'égard des données à caractère personnel à la libre circulation des données.* JOCE n° C 93 du 13 avril 1995, p.1.

- Rapport *sur l'application de principes de protection des données aux réseaux mondiaux de télécommunications*.[en ligne], Strasbourg, 18 novembre 2004, T-PD (2004) 04. 64 p. Disponible sur : http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/T-PD(2004)04_Poullet_report.pdf. Consulté le 22 mai 2014.

- Recommandation 2008/594/CE du 2 juillet 2008 *sur l'interopérabilité transfrontalière des systèmes des dossiers informatisés de santé*.[en ligne], Notifié sous le n° C(2008) 3282. JOUE du 18 juillet 2008. p L 190/37-L 190/43. Disponible sur : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:190:0037:0043:FR:PDF. Consulté le 22 mai 2014.

- Recommandation R (97) 18 du 30 septembre 1997 *concernant la protection des données à caractère personnel, collectées et traitées à des fins statistiques.* [en ligne], 8 p. Disponible sur: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet

&InstranetImage=2001721&SecMode=1&DocId=578636&Usage=2. Consulté le 11 avril 2014.

- Recommandation R (97) 5 du 13 février 1997 *relative à la protection des données médicales.* [en ligne], 4 p. Disponible sur : https://wcd.coe.int/com.instranet.InstraServlet ? command=com.instranet.CmdBlobGet&InstranetImage=637549&SecMode=1&DocId=83 9736&Usage=2. Consulté le 11 avril 2014.

- Recommandation R (83) 10 du 23 septembre 1983 *relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques*. [en ligne]. 4 p. Disponible sur : https://wcd.coe.int/com.instranet.InstraServlet?command=com. instranet.CmdBlobGet&InstranetImage=602932&SecMode=1&DocId=680154&Usage=2. Consulté le 28 avril 2014.

- Recommandation R (81) 1 du 23 janvier 1981 *relative à la réglementation applicable aux banques de données médicales automatisées*. [en ligne], 4 p. Disponible sur : https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&Ins tranetImage=599533&SecMode=1&DocId=670462&Usage=2. Consulté le 28 avril 2014.

- Résolution n° 1165 (1998) du 26 juin 1998, *droit au respect de la vie privée* (24ème séance). [en ligne], disponible sur : http://www.assembly.coe.int//Main.asp?link=http:// www.assemblycoe.int/Documents/AdoptedText/ta98/fres1165.htm#1. Consulté le 22 mai 2014.

- Résolution n° 85/C136/01 du 7 mai 1985 *relative à une nouvelle approche en matière d'harmonisation technique et de normalisation*. JOCE n° C 136 du 4 juin 1985, p. 1-9.

PUBLICATIONS DE LA COMMISSION EUROPEENNE

- Groupe européen d'éthique. *Avis n° 13 du 30 juillet 1999 relatif aux aspects éthiques de l'utilisation des données personnelles de santé dans la société de l'information*. [en ligne], 14 p. Disponible sur : http://ec.europa.eu/bepa/european-group-ethics/docs/ avis13_fr.pdf. Consulté le 22 mai 2014.

- Groupe de travail de l'article 29.

- Avis n° 8/2010 *sur le droit applicable*. [en ligne], 16 décembre 2010, 0836-02/10/FR WP 179. Disponible sur : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_fr.pdf. Consulté le 22 mai 2014.
- Avis n° 3/2010 *sur le principe de la responsabilité*. [en ligne], 13 juillet 2010. 00062/10/FR WP 173. Disponible sur: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf. Consulté le 23 mai 2014.
- Communiqué de presse de *l'avis sur les techniques d'anonymisation*.[en ligne], 10 avril 2014. Disponible sur : http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140410_pr_9_10_april.pdf. Consulté le 19 avril 2014.
- Document de travail *sur le traitement des données à caractère personnel relatives à la santé contenue dans les dossiers médicaux électroniques (DME*). [en ligne]. 15 février 2007. n° 00323/07/FR WP 131. 25 p. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_fr.pdf. Consulté le 5 avril 2014.

LÉGISLATION FRANÇAISE

- Déclaration des droits de l'homme et du citoyen. [en ligne], Paris, 26 août 1789. Disponible sur : http://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789. Consulté le 22 mai 2011.

LOIS

- Loi n° 2014-201 du 24 février 2014 *portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la santé*. JORF n° 0047 du 25 février 2014. p. 3250, texte n° 4. NOR : AFSX1315898L.

- Loi n° 2011-267 du 14 mars *2011 d'orientation de programmation pour la performance de la sécurité intérieure*. JORF, n° 0062, 15 mars 2011, p. 4582. NOR : IOCX0903274L.

- 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, 22 juillet 2009, p. 12184. Texte n° 1. NOR : SASX0822640L.

- Loi n° 2008-125 du 13 février 2008 *autorisant la ratification du traité de Lisbonne modifiant le traité sur l'Union européenne, le traité instituant la communauté européenne et certains actes connexes.* JORF, n° 0038, 14 février 2008, p. 2712. Texte n°1. NOR : MAEX0802893L.

- Loi n° 2007-1786 du 19 décembre 2007 *de financement de la sécurité sociale pour 2008*. JORF, n° 0296, 21 décembre 2007, p. 20603. Texte n° 1. NOR : BCFX0766311L.
- 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, 6 mars 2007, p.4190. Texte n° 4. NOR : SOCX0600231L.

- 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 (1) (Titre résultant de la décision du Conseil Constitutionnel n° 2007-546 DC du 25 janvier 2007)*, JORF, n° 27, 1er février 2007, p. 1937-1941. NOR : SANX0500266L.

- Loi n° 2004-810 du 13 Août 2004 *relative à l'assurance maladie.* JORF, n° 190, 17 Août 2004, p 14598. Texte n° 2. NOR : SANX0400122L.

- Loi n° 2004-806 du 9 août 2004 *relative à la politique de santé publique*. JORF, n° 185, 11 Août 2004, p. 14277. NOR : SANX0300055L et rectificatif JORF, 12 août 2004. p. 14399. Texte n°3. NOR : SANX0300055Z.

- Loi n° 2004-801 du 6 août 2004 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. JORF, n° 182, 7 août 2004, p. 14063. Texte n°2. NOR : JUSX0100026L.

- Loi n° 2004-575 du 21 juin 2004 *pour la confiance dans l'économie numérique (LCEN)* JORF, n° 0143, 22 juin 2004, p. 11168. Texte 2. NOR : ECOX0200175L.

- Loi n° 2002-303 du 4 mars *2002 relative aux droits des malades et à la qualité du système de santé* (1). JORF, n° 54, 5 Mars 2002, p 4118 et suivants. Texte n°1. NOR : MESX0100092L.

- Loi n° 2000-719 du 1er août 2000 *modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.* JORF, n° 177, 2 août 2000, p. 11903. Texte n° 1. NOR : MCCX9800149L.

- Loi n° 2000-321 du 12 avril 2000 *relative aux droits des citoyens dans leurs relations avec les administrations*. JORF, n° 88, 13 avril 2000, p. 5646. Texte n° 1. NOR : FPPX9800029L

- Loi n° 99-641 du 27 juillet 1999 *portant création d'une couverture maladie universelle*. JORF, n° 172, 28 juillet 1999, p. 11229. NOR : MESX9900011L.

- 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 no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. JORF, n°152, 2 juillet 1994, p 9559. NOR : RESX9200045L.

- Loi n° 94-43 du 18 janvier 1994 *relative à la santé publique et à la protection sociale* (annexes 5). JORF, n° 15, 19 janvier 1994, p. 960. NOR : SPSX9300136L.

- Loi n° 93-23 du 8 janvier 1993 *modifiant le titre VI du livre III du code des communes et relative à la législation dans le domaine funéraire*. JORF, n°7, 9 janvier 1993, p.499. NOR : INTX9200170C.

- Loi n° 91-748 du 31 juillet 1991 *portant réforme hospitalière (1)* JORF, n°179, 2 août 1991, p. 10255. NOR: SPSX9000155L

- Loi n° 89-462 du 6 juillet 1989 *dite MALANDIN, MERMAZ tendant à améliorer les rapports locatifs et portant modification de la loi 861290 du 23-12-1986*. JORF du 8 juillet 1989, p. 8541. NOR : EQUX8910174L.

- Loi n° 88-1138 du 20 décembre 1988 *dite « Huriet-Sérusclat » relative à la protection des personnes qui se prêtent à des recherches biomédicales.* JORF du 22 décembre 1988, p. 16032. NOR : SPSX8810045L.

- Loi n° 86-1305 du 23 décembre 1986 *modifiant celle du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques* JORF du 26 décembre 1986, p. 15596.
- Loi n° 82-890 du 19 octobre 1982 *autorisant l'approbation d'une convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*. JORF du 20 octobre 1982, p. 3163.
- Loi n° 80-460 du 25 juin 1980 *autorisant l'adhésion de la République française au pacte international relatif aux droits civils et politiques, ouvert à la signature le 19 décembre 1966 à New-York.* [en ligne]. JORF du 26 juin 1980, p.1569. Disponible sur : http://www.legifrance.gouv.fr. Consulté le 31 mars 2014.
- Loi n° 79-18 du 3 janvier 1979 *sur les archives*. JORF du 5 janvier 1979, p. 43.
- 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.
- Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*. JORF du 7 janvier 1978. p. 227.
- Loi n° 73-1227 du 31 décembre 1973 *autorisant la ratification de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales signée à Rome le 4 novembre 1950, et de ses protocoles additionnels.*[en ligne] JORF du 3 janvier 1974, p. 67. Disponible sur : http://legifrance.gouv.fr/. Consulté le 31 mars 2014.
- Loi n° 70–1318 du 31 décembre 1970 *portant réforme hospitalière.* JORF du 3 janvier 1971, p. 00067. Cette loi a été abrogée le 4 janvier 1992.
- Loi n° 51-711 du 7 juin *1951 sur l'obligation, la coordination et le secret en matière de statistiques***.** JORF du 8 juin 1951, p. 6013.
- Loi n° 41-1987 du 24 mai 1941 *relative à la normalisation*. JORF du 28 mai 1941, p. 2219.

REGLEMENTS

➢ Ordonnances

- 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*. JORF, n° 199, 27 août 2005, p. 13923. Texte n° 46. NOR : SANX0500172R.

- Ordonnance du 4 septembre 2003 *portant simplification de l'organisation et du fonctionnement du système de santé ainsi que des procédures de création d'établissements ou de services sociaux ou médico-sociaux soumis à autorisation.* JORF, n° 206, 6 septembre 2003, p. 15391. Texte n° 26. NOR : SANX0300081R.

- Ordonnance n° 96-346 du 24 avril 1996 *portant réforme de l'hospitalisation publique et privée.* JORF, n° 98, 25 avril 1996, p. 6324. NOR : TASX9600043R.

- Ordonnance n° 96-345 du 24 avril 1996 *relative à la maîtrise médicalisée des dépenses de santé.* JORF n° 98 du 25 avril 1996. p. 6311. NOR : TASX9600042R

➢ Décrets

- Décret n° 2012-1249 du 9 novembre 2012 *autorisant la création de traitement de données à caractère personnel pour la mise en œuvre de programmes de prévention et d'accompagnement en santé des assurés sociaux*. JORF, n° 0263, 11 novembre 2012. p. 17878. Texte n° 1. NOR : AFSS1233684D.

- Décret n° 2012-694 du 7 mai 2012 *portant modification du code de déontologie médicale*. JORF, n° 0108, 8 mai 2012. p. 8479. Texte n° 97. NOR : ETSH1207448D.

- Décret n° 2012-652 du 4 mai 2012 *relatif au traitement d'antécédents judiciaires*. JORF, n° 0107, 6 mai 2012, p. 8047. Texte n° 14. NOR : IOCD1125123D

- Décret n° 2011-496 du 5 mai *2011 portant création d'une stratégie à la délégation des systèmes d'information de santé auprès des ministères chargés de la santé, de la sécurité*

sociale, de solidarité et de la cohésion sociale. JORF, n° 0105, 6 mai 2011. Texte n° 31.NOR : ETSG1106711D.

- Décret n° 2010 - 1229 du 19 octobre 2010 relatif à la télémédecine. JORF n°0245 du 21 octobre 2010. Texte n° 13. NOR : SASH1011044D.

- Décret n° 2009-1273 du 22 octobre 2009, *autorisant la création d'un traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1)*. JORF, n° 0246, 23 octobre 2009, p. 17726. Texte n° 19. NOR : SASS0922224D.

- Décret n° 2009-697 du 16 juin 2009 *relatif à la normalisation.* JORF, n°0138, 17 juin 2009, p 9860. Texte n° 6. NOR : ECEI0909907D.
- Décret n° 2008-1326 du 15 décembre 2008 *relatif au dossier pharmaceutique*. JORF n°0293, 17 décembre 2008, p.19237. Texte n° 26. NOR : SJSS0819822D.

- 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, 16 mai 2007, p. 9362 Texte 210. NOR : SANP0721653D.

- Décret n° 2007-663 du 2 mai 2007 *pris pour l'application des articles 30,31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie.* JORF n° 104, 4 mai 2007, p. 7865. Texte n°1. NOR : PRMD0751412D.

- Décret n° 2007-451 du 25 mars 2007 *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, modifiée par la loi n° 2004-801 du 6 août 2004*. JORF, n°74, 28 mars 2007, p. 5782. Texte n° 30. NOR : JUSC0720211D.

- Décret n° 2007-199 du 14 février 2007 *relatif à la carte d'assurance maladie et modifiant le code de la sécurité sociale (deuxième partie : Décrets en Conseil d'État)***.** JORF, n°39, 15 février 2007, p. 2799. Texte n° 26. NOR : SANS0720208D.

- Décret n° 2006-143 du 9 février 2006 *relatif aux modalités d'accès des médecins aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie et*

modifiant le code de la sécurité sociale (deuxième partie : décrets en Conseil d'État). JORF, n° 36, 11 février 2006. p. 2190. Texte n° 22. NOR: SANS0620002D.

- Décret n° 2006-119 du 6 février 2006 *relatif aux directives anticipées prévues par la loi n° 2005-370 du 22 avril 2005 relative aux droits des malades et à la fin de vie et modifiant le code de la santé publique (dispositions réglementaires).* JORF, n° 32, 7 février 2006, p. 1973. Texte n° 32. NOR : SANP0620219D.

- 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 (dispositions réglementaires)*. JORF, n° 4, 5 janvier 2006, p. 174. Texte n° 14. NOR : SANX0500308D.

- 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, 22 octobre 2005, p 16769. Texte n° 31. NOR : JUSC0520586D.

- Décret n° 2004-15 du 7 janvier 2004 *portant code des marchés publics*. JORF, n° 6, 8 janvier 2004, p. 37003. Texte n°2. NOR: ECOZ0300023D.

- Décret n° 2003-462 du 21 mai 2005 *relatif aux dispositions réglementaires des parties I, II et III du code de la santé publique.* JORF, n° 122, 27 mai 2003, p. 37006. Texte n° 3. NOR: SANP0321523D.

- Décret n° 2002-637 du 29 avril 2002 *relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 1111-7 et L. 1112-1 du code de la santé publique*. JORF, n°101, 30 avril 2002, p.7790. Texte n° 8. NOR : MESP0221143D.

- Décret n° 2000-1282 du 6 décembre 2000 *portant création de l'agence technique pour l'information sur l'hospitalisation et modifiant le code de la santé publique (deuxième partie: Décret en Conseil d'État).* JORF, n° 301, 29 décembre 2000, p. 20814. Texte n° 15. NOR : MESH0023447D.

- Décret n° 96-925 du 18 octobre 1996 *relatif au carnet de santé institué par l'article L. 162-1-1 du code de la sécurité sociale et modifiant ce code (deuxième partie : Décrets en Conseil d'État)***.** JORF, n° 246, 20 octobre 1996. p. 15429. NOR: TASS9623355D.

- Décret n° 95-1321 du 27 décembre 1995 *modifiant le décret n° 76. 1004 du 4 novembre 1976 fixant les conditions d'autorisation des laboratoires d'analyses de biologie médicale.* JORF, n° 302, 29 décembre 1995, p. 18856. NOR : TASP9523465D.

- Décret n° 95-234 du 1er mars 1995 *relatif au dossier de suivi médical et au carnet médical institué par l'article 77 de la loi numéro 94-43 du 18 janvier 1994 relatif à la santé publique et à la protection sociale*. JORF, n° 54, 4 mars 1995. p. 03448. NOR: SPSS9500441D.

- Décret n° 93-354 du 15 mars 1993 relatif *aux conditions d'autorisation des laboratoires d'analyses de biologie médicale et au contrôle de bonne exécution de ces analyses et modifiant les décrets numéro 76-1004 du 4 novembre 1976 et n° 83-104 du 15 février 1983.* JORF, n° 64, 17 mars 1993, p. 4155. NOR : SANP9300553D.

- Décret n° 92-329 du 30 mars 1992 *relatif au dossier médical et à l'information des personnes accueillies dans les établissements de santés publics et privés et modifiant le code de la santé publique (deuxième partie : décret en Conseil d'État).* JORF, n°78, 1er avril 1992, p. 4607. NOR : SANH9200522D.

- Décret n° 91-242 du 28 février 1991 *portant publication de la convention sur la loi applicable aux obligations contractuelles (ensemble un protocole et deux déclarations communes) signée à Rome les 19 juin 1980 (1).* JORF, n° 54, 3 mars 1991 p. 3072. NOR: MAEJ9130005D.
- Décret n° 87-1005 du 16 décembre 1987 *relatif aux missions et à l'organisation des unités participant au service d'aide médicale urgente appelées SAMU.* JORF, 17 décembre 1987, p. 14692. NOR : ASEP8701666D.

- Décret n° 85-1203 du 19 novembre 1985 *portant publication de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, fait à Strasbourg le 28 janvier 1981*. JORF du 20 novembre 1985. p. 13436.

- Décret n° 81-76 du 29 janvier 1981 *portant publication du pacte international relatif aux droits civils et politiques ouverts à la signature à New York le 19 décembre 1966*. JORF du 1er février 1981, p. 398

- Décret n° 74-360 du 3 mai 1974 *portant publication de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales signée à Rome le 4 novembre 1950 et de ses protocoles additionnels.* JORF du 4 mai 1974, p. 4750.

- Décret n° 74-230 du 7 mars 1974 *relatif à la communication du dossier des malades hospitalisés ou consultants des établissements hospitaliers publics*. JORF du 12 mars 1974, p. 02832. Ce décret a été abrogé le 1er Avril 1992.

- Décret n°74-27 du 14 janvier 1974 *relatif aux règles de fonctionnement des centres hospitaliers et des hôpitaux locau**x.*** JORF du 16 janvier 1974, p. 603.

- Décret n° 43-891 du 17 avril 1943 *portant règlement d'administration publique pour l'application de la loi du 21 décembre 1941 sur la réorganisation des hôpitaux et des hospices.* JORF du 27 avril 1943, p. 1156.

➢ Arrêtés

- Arrêté du 18 septembre 2013 *portant approbation de la convention constitutive du groupement d'intérêt public « agence nationale des systèmes d'information partagés de santé* ». JORF, n° 0243, 18 octobre 2013, p. 17153. Texte n°20. NOR : AFSZ1324608A.

- Arrêté du 19 juillet 2013 relatif à la mise en œuvre du système national d'information interrégimes de l'assurance maladie. JORF n° 0187 du 13 août 2013. p. 13791. Texte n° 3. NOR : AFSS1318985A.

- Arrêté du 28 novembre 2009 *portant approbation de modification de la convention constitutive du groupe d'intérêts publics dénommés « agence des systèmes d'information partagés de santé ».* JORF, n° 0277, 29 novembre 2009, p. 20626. Texte n° 16. NOR : SASG0925044A.

- Arrêté du 28 novembre 2009 *portant approbation de la dissolution du groupement d'intérêt public « Carte de professionnel de santé » et transfert des biens, droits et obligations à l'Agence des systèmes d'information partagés de santé*. JORF, n°0277 du 29 novembre 2009, p. 20627. Texte n° 17. NOR : SASG0925049A.

- Arrêté du 16 octobre 2009 *portant approbation de la convention constitutive du groupement d'intérêt public «Agence nationale d'appui à la performance des établissements de santé et médico-sociaux»***.** JORF, n° 0246, 23 Octobre 2009, p. 17737, Texte n° 26. NOR : SASH0923114A.

- Arrêté du 8 septembre 2009 *portant approbation de la modification de la convention constitutive d'un groupement d'intérêt public*. JORF, n° 0213, 15 Septembre 2009, p. 15096. Texte n°15. NOR : SASC0917305A.

- Arrêté du 14 mars 2007 *relatif aux spécifications physiques et logiques de la carte d'assurance maladie et aux données contenues dans cette carte***.** JORF, n° 65, 17 mars 2007, p. 4983. Texte n° 30. NOR : SANS0721152A.
- Arrêté du 3 janvier *2007 portant modification de l'arrêté du 5 mars 2004 portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès*. JORF, n° 13, 16 janvier 2007, p. 982. Texte n° 32. NOR : SANP0720101A.

- Arrêté du 3 février 2005 *portant approbation de la convention nationale des médecins généralistes et des médecins spécialistes.* JORF, n° 35, 11 février 2005, p. 2275. Texte n° 4. NOR : SANS0520354A.

- Arrêté du 5 mars 2004 *portant homologation des recommandations de bonnes pratiques relatives à l'accès aux informations concernant la santé d'une personne, et notamment l'accompagnement de cet accès.* JORF, n° 65, 17 mars 2004, p. 5206. Texte n° 16. NOR : SANP0420786A

- Arrêté du 20 septembre 1994 *relatif au recueil et au traitement de données d'activité médicale et de coût, visée 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 du 18 octobre 1994, p. 14761. NOR : SPSH9402990A (abrogé le 11 février 2004 par arrêté 2003-12-36, article 9).

- Arrêté du 25 novembre 1993 *portant approbation de la convention des médecins.* JORF du 26 novembre 1993, p. 16297. NOR : SPSX9301043A.

- Arrêté du 27 novembre 1991 *autorisant le traitement informatique des dossiers médicaux économiques et épidémiologiques de l'immunodéficience humaine dans les centres d'information et de soins de l'immunodéficience humaine et autres établissements hospitaliers*. JORF du 17 janvier 1992, p. 822.

➢ Circulaires

- Circulaire n° 275 du 6 janvier 1989 *relative à l'informatisation des hôpitaux publics.* [en ligne], NOR : SPSH8910005C (non parue au journal officiel). Disponible sur : http://www.atih.sante.fr/sites/default/files/public/content/990/Cir_6-1-89.pdf. Consulté le 26 mai 2014.

- Circulaire secrétariat n° 394 du 11 Août 1978. *relative à la communication des dossiers médicaux des malades ayant été hospitalisés à leur médecin traitant ou à un autre établissement hospitalier*. [en ligne], (non parue au journal officiel). Bulletin officiel du ministère de la santé et de la famille. SF 78/41, p. 15546. Disponible sur : http://www.ascodocpsy.org/wpcontent/uploads/2010/01/circulaire_dossiers_medicaux_malades_19780811.pdf. Consulté le 26 mai 2014.

- Circulaire ministérielle n° 1796 du 20 avril 1973 *relative au secret professionnel dans les établissements d'hospitalisation publics*.[en ligne] SP-SS 73/19, p 4.482. (non parue au journal officiel). Disponible sur http://portail-web.aphp.fr/daj/public/index/display/page/433/id_fiche/3401. Consulté le 26 mai 2014.

DECISIONS, RAPPORTS, AVIS ET AUTRES PUBLICATIONS OFFCIELLES DES ORGANISMES PUBLICS ET ORDRES PROFESSIONNELS FRANÇAIS

SENAT

- BRAUN, Gérard. *Rapport sur l'administration électronique au service du citoyen*. [en ligne], n° 402 (2003-2004). 6 juillet 2004. Disponible http://www.senat.fr/rap/r03-402/r03-402_mono.html. Consulté le 26 mai 2014.

- Commission des affaires sociales. *Comptes rendus des auditions de la Commission des affaires sociales*. [en ligne]. 16 octobre 2013. Disponible sur : http://www.senat.fr/compte-rendu-Commissions/20131014/soc.html#toc10. Consulté le 11 juin 2014.

- DETRAIGNE, Yves, ESCOFFIER, Anne-Marie. *Proposition de loi visant à mieux garantir la vie privée à l'heure du numérique.* [en ligne], n° 93. présenté le 6 novembre 2009. Disponible sur : http://www.senat.fr/leg/ppl09-093.html. Consulté le 26 mai 2014

- DIONIS DU SEJOUR, Jean, ÉTIENNE Jean-Claude. *Rapport sur les télécommunications à haut débit au service des systèmes de santé*. [en ligne], Tome I. n° 370. 23 juin 2004. Disponible sur : http://www.senat.fr/rap/r04-370-1/r04-370-11.pdf. Consulté le 2 mai 2014.

- GELARD, Patrice. *Amendement 205. Discussion des articles additionnels du financement de la sécurité sociale pour 2007*. [en ligne], 17 novembre 2006. Disponible sur : http://www.senat.fr/cra/s20061117/s20061117H1.html#toc2. Consulté le 26 mai 2014

- JEGOU, Jean-Jacques.

    - *Rapport sur les autorités administratives indépendantes : évaluation d'un objet juridique mal identifié (tome 1).* [en ligne], n° 404 (2005-2006). 15 juin 2006. Disponible sur:.http://www.senat.fr/rap/r05-404-1/r05-404-1.html. Consulté le 26 mai 2014

    - *Systèmes d'information de santé : le diagnostic est posé, le traitement s'impose.* [en ligne], Rapport d'information fait au nom de la Commission des finances, n° 35

(2007-2008) le 17 octobre 2007. http://www.senat.fr/notice-rapport/2007/r07-035-notice.html. Consulté le 26 mai 2014

- LARCHER, Gérard. *Proposition de loi visant à mieux garantir la vie privée à l'heure du numérique* [en ligne], adoptée le 23 mars 2010. n° 81. Disponible sur : http://www.senat.fr/leg/tas09-081.html. Consulté le 26 mai 2014

- MILON, Alain. *Rapport annuel de contrôle d'application des lois 2010*. [en ligne], 11 janvier 2011. Disponible sur : http://www.senat.fr/rap/apleg_10/apleg_1044.html. Consulté le 26 mai 2014.

- MUYARD, Monique. *Compte rendu des débats du Sénat de la séance du 15 novembre 2007 : Financement de la sécurité sociale pour 2008*. [en ligne], JORF n° 66 S (C.R) du 16 novembre 2007. p 4846-4883. Disponible sur: http://www.senat.fr/seances/ s200711/ s20071115/s2007 1115.pdf. Consulté le 26 mai 2014

- TÜRK, Alex. Rapport n° 209. (1993 - 1994) *Projet de loi relatif au traitement de données nominatives ayant pour fin la recherche en vue de la protection ou l'amélioration de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. [en ligne], 21 décembre 1993. p.8. Sommaire du rapport. Disponible sur : http://www.senat.fr/rap/l93-209/l93-209.html. Consulté le 26 mai 2014.

- VASSELLE, Alain. *Rapport relatif à l'assurance maladie.* [en ligne], n° 424 (2003-2004). 21 juillet 2004. Disponible sur : http://www.senat.fr/rap/l03-424-2/l03-424-2_mono.html#toc4. Consulté le 26 mai 2014

ASSEMBLEE NATIONALE

- DELATTE, Rémi. *Avis n° 1971, sur le projet de loi de finances pour 2010 (n° 1946),* Tome II [en ligne], 14 octobre 2009. Disponible sur: http://www.assemblee-nationale.fr/13/budget/plf2010/a1971-tii.asp#P338_62675. Consulté le 27 mai 2014.

- DELATTRE, Francis, *Rapport n° 1537 de l'Assemblée nationale sur le projet de loi, modifié par le sénat (n° 762), 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.[en ligne], le 14 Avril 2004.*

Disponible sur : http://www.assemblee-nationale.fr/12/rapports/r1537.asp. Consulté le 27 mai 2014.

- DIONIS DU SEJOUR, Jean, ETIENNE, Jean-Claude. *Rapport n° 1686, Nouvelles technologies de l'information et système de santé : « la nouvelle révolution médicale »*. [en ligne], Septembre 2004. Disponible sur : http://www.assemblee-nationale.fr/documents/ resume-rapport-ntic-sante.pdf. Consulté le 15 novembre 2011.

- DOOR, Jean-Pierre. *Rapport d'information n° 659 sur le dossier médical personnel*. [en ligne], 29 janvier 2008. Disponible sur http://www.assemblee-nationale.fr/13/rap-info/i0659.asp#p34_266743. Consulté le 27 juin 2010.

- DUBERNARD, Jean Michel. *Rapport n° 1703 sur le projet de loi relatif à l'assurance maladie.* [en ligne], 24 juin 2004. Disponible sur : http://www.assemblee-nationale.fr/12/rapports/r1703.asp#P278_28212. Consulté le 27 mai 2014.

- ESTROSI, Christian. *Question ministérielle n° 117101. Économie numérique- rapport-propositions*. [en ligne], JOAN, 30 août 2011, p. 9304. Réponse publiée au JOAN du 1er mai 2012. p. 3391. Disponible sur : http://questions.assemblee-nationale.fr/q13/13-117101QE.htm. Consulté le 26 mai 2014.

- GEORGE, François. *Compte rendu officiel analytique. Session ordinaire 2003-2004, 82ème jour de séance, 205ème séance*.[en ligne]. 29 avril 2004. Disponible sur : http : //www.assemblee-nationale.fr/12/cra/2003-2004/205.asp. Consulté le 26 mai 2014.

- GOUZES, Gérard. *Rapport n° 3526 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*. [en ligne], 22 janvier 2002. Disponible sur: http://www.assemblee-nationale.fr/11/ rapports/r3526.asp. Consulté le 28 avril 2014.

- JARDÉ, Olivier. *Rapport n° 2444 concernant la proposition de loi modifiée par le Sénat relative aux recherches cliniques ou non interventionnelles impliquant la personne humaine*. [en ligne], 7 avril 2010. Disponible sur : http://www.assemblee-nationale.fr/ 13/rapports/r2444.asp. Consulté le 26 mai 2014.

- LASBORDES, Pierre. *Rapport n° 1847 sur le dossier médical personnel (DMP): quel bilan d'étape pour quelles perspectives ? (Compte rendu de l'audition publique du 30 avril 2009)*. [en ligne], 20 juillet 2009. Disponible sur : http://www.assemblee-nationale.fr/13/rap-off/i1847.asp. Consulté le 8 mai 2014.

- LE DÉBAUT, BLOCHE et al. *Amendement n° 341. Droits d'auteur et droits voisins dans la société de l'information (n° 1206).* [en ligne] 7 mars 2006. Disponible sur : http : //www.assemblee-nationale.fr/12/amendements/1206/120600341.asp. Consulté le 26 mai 2014.
- MOREL-A-L' HUISSIER Pierre. *Question écrite n° 94963. Dossier médical personnel.* [en ligne], JOAN, 23 mai 2006, p. 5352. Réponse publiée au JOAN, 28 novembre 2006. p. 12551. Disponible sur : http://questions.assemblee-nationale.fr/q12/12-94963QE.htm. Consulté le 26 mai 2014.

- ROCHEBLOINE François. *Question n° 59945. Malades- Dossier médical- transferts*. [en ligne], JOAN, 16 avril 2001. P. 2224. Réponse publiée au JOAN du 6 Août 2001. P. 4601. http://questions.assemblee-nationale.fr/q11/11-59945QE.htm. Consulté le 26 mai 2014.

- ROGEMONT, Marcel. *Question n° 12931. Dossier médical personnel. [en ligne]*, JOAN du 18 décembre 2007. p. 7962. Réponse ministérielle publiée au JOAN du 20 mai 2008. p. 4261. Disponible sur : http://questions.assemblee-nationale.fr/q13/13-12931QE.htm. Consulté le 26 mai 2014.

DECISION DU GOUVERNEMNENT

- BACHELOT-NARQUIN Roselyne. *Décision du 10 novembre 2010 portant agrément du groupement constitué entre les sociétés* Santeos Atos Worldline Extelia en qualité d'hébergeur de données de santé à caractère personnel. [en ligne], NOR : SASX1030992S. Disponible sur http://www.sante.gouv.fr/fichiers/bo/2010/10-12/ste_20100012_0100_0081.pdf. Consulté le 10 juillet 2014.

CONSEIL ECONOMIQUE ET SOCIAL

- GROS Jeannette. Rapport. *Santé et nouvelles technologies de l'information et de la communication*. [en ligne], 10 avril 2002. 147 p. Disponible sur : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000462/0000.pdf. Consulté le 29 avril 2014.

COUR DES COMPTES

- *Communication à la Commission des finances de l'Assemblée nationale. Le coût du dossier médical personnel depuis sa mise en place.* [en ligne], Juillet 2012. 134 p. Disponible sur http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/134000136/0000.pdf. Consulté le 15 mai 2014.
- *Le partage des données entre les systèmes d'information de santé.* in rapport sur la sécurité sociale. [en ligne], Chapitre X, p. 307-327. Septembre 2007. Disponible sur: http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000560/0000.pdf. Consulté le 17 janvier 2011.
- *Rapport sur le financement de la sécurité sociale 2008*. [en ligne], Septembre 2008. 487 p. Disponible sur : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/084000597/0000.pdf. Consulté le 28 mai 2014.

CNIL

- **Rapports**

- *7ème rapport d'activité 1er janvier 1986 – 31 décembre 1986*. Paris : La documentation française 1986. ISBN : 2-11-001785-6.
- *13ème rapport d'activités* 1992. Paris : La documentation française. 1993. 412 p. ISBN : 2-11-002989-7.
- *14ème rapport d'activités 1993*. Paris : La documentation française 1994. 437p. ISBN : 2-11-003187-5.

- *17ème rapport d'activité 1996.* Paris : La documentation française. 1997. 532p. ISBN : 2-11-003757-1.
- *20ème rapport d'activité 1999.* Paris : La documentation française. 2000. 360p. ISSN : 2261-8619.
- *21ème rapport d'activité 2000.* Paris : La documentation française. 2001. 327p. ISBN : 2-11-004861-1 (br).
- *28ème rapport d'activité 2007*. Paris : La documentation française. 2008. 126p. ISBN : 978-2-11-007052-4.
- *30ème rapport d'activité 2009*. Paris : La documentation française. 2010. 112p. ISBN : 978-2-11-008039-4
- *32ème rapport d'activité 2011*. Paris : La documentation française. 2012. 104p. ISBN : 978-2-11-009075-1
- *Conclusions de la Commission nationale informatique et libertés sur l'utilisation du NIR comme identifiant de santé.* [en ligne], 20 février 2007. 4 p. Disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/NIR/Rapport%20NIR.pdf. Consulté le 28 mai 2014.
- COTTERET, Jean-Marie, GIQUEL, François. *Conclusions du contrôle du système de traitement des infractions constatées (STIC).* [en ligne], 20 janvier 2009. 32 p. http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000035/0000.pdf. Consulté le 3 avril 2014.
- DEBET, Anne. *Rapport sur la mesure de la diversité et protection des données personnelles*.[en ligne], 15 mai 2007. 41 p. Disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/diversite/RapportdiversiteVD.pdf. Consulté le 16 avril 2014.
- TRICOT, Bernard. *Rapport de la Commission informatique et libertés : (décret 74-938 du 8 novembre 1974).* Paris : La Documentation française, 1975. Volume 1. 341 p.

➢ Délibérations

- Délibération n° 2014-046 du 30 janvier 2014. (Autorisation unique n° AU-033) portant autorisation unique de traitement de données à caractère personnel mis en œuvre par les

prestataires de santé à domicile pour la téléobservance en application de l'arrêté du 22 octobre 2013 relatif aux dispositifs médicaux à pression positive continue. JORF n° 0034, 9 février 2014, texte n° 43. NOR : CNIX14003178X.

- Délibération n° 2014-015 du 23 janvier 2014 portant création d'une autorisation unique concernant le traitement de données à caractère personnel relatifs aux infractions, condamnations ou mesures de sûretés mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance, les intermédiaires d'assurance et par l'AGIRA. JORF n° 0032 du 7 février 2014, texte n° 75. NOR : CNIX1402984X.

- Décision n° 2014-001 du 15 janvier 2014 mettant en demeure la SAS HYPERCOSMOS qui exploite l'enseigne « E.LECLERC » à Saint Médard JALLES (N°MDM 131052). [en ligne], 8 p. Disponible sur : http://www.cnil.fr/fileadmin/documents/approfondir/D2014-001_ MED_hypercosmos.pdf/. Consulté le 31 mars 2014.

- Décision n° 2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo. (n° MDM 131040). [en ligne], 6 p. Disponible sur : http://www.cnil.fr/ fileadmin/documents/approfondir/deliberations/D2013037_MED_CH_ST_MALO.pdf. Consulté le 22 octobre 2013.

- Délibération n° 2012-261 du 19 juillet 2012 portant avis sur le projet de décret du ministère des affaires sociales et de la santé relatif à la mise en œuvre de services en santé par les organismes de gestion des régimes obligatoires de base d'assurance maladie (demande d'avis n° 1202167). JORF n° 0263 du 11 novembre 2012, texte n° 17. NOR : CNIX1239037X.

- Délibération n° 2011-316 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de procédure d'audit tendant à la protection des personnes à l'égard du traitement des données à caractère personnel. JORF n° 0255 du 3 novembre 2011, texte n° 63. NOR: CNIA1100014X.

- Délibération n° 2011-205 du 6 octobre 2011. portant avertissement à l'encontre de la société Foncia Groupe. [en ligne] 8 p. Disponible sur: http://www.cnil.fr/fileadmin/ documents/approfondir/deliberations/Formation_contentieuse/D2011205_Avertissement_FONCIA.pdf. Consulté le 28 mai 2014.

- Délibération n° 2010 460 du 9 décembre 2010 portant recommandation relative aux conditions de réutilisation des données à caractère personnel contenues dans des documents d'archives publiques. JORF n° 026 du 1er février 2011. Texte n° 72. NOR : CNIA1000016X.

- Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mises en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023308516. Consulté le 28 mai 2014.

- Délibération n° 2010-229 du 10 juin 2010 dispensant de déclaration les traitements automatisés de données à caractère personnel mis en œuvre par des organismes à but non lucratif abrogeant le remplaçant la délibération n° 2006-130 du 9 mai 2006 (décision de dispense de déclaration n° 8). JORF n° 0155 du 7 juillet 2010, texte 76 NOR : CNIA1000008X.

- Délibération n° 2010-116 du 6 mai 2010 autorisant à titre expérimental des pharmacies hospitalières à mettre en œuvre des traitements de données personnelles nécessaires au dossier pharmaceutique. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000022379205. Consulté le 28 mai 2014.

- Délibération n° 2009-569 du 1er octobre 2009 *portant avis sur un projet de décret en Conseil d'Etat relatif à la création d'un traitement de données relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1)* JORF n° 0246 du 23 octobre 2009, texte n° 72. NOR : CNIX0924897X.

- Délibération n° 2009-522 du 24 septembre 2009 portant autorisation de la mise en œuvre à titre expérimental par le Conseil général des Yvelines d'un traitement automatisé de données à caractère personnel ayant pour finalité la mise en place d'une plateforme de dossier médico-social partagé (DMSP) dans la région des Yvelines (autorisation n°1372117). [en ligne] disponible sur http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000021184075&fastReqId=1956948462&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 2009-476 du 10 septembre 2009 décidant la dispense de déclaration des traitements de données à caractère personnel mis en œuvre dans le cadre des plans de continuité d'activités relatifs à une pandémie grippale mis en œuvre par des employeurs publics et privés (Norme d'exonération n° 14). JORF n° 0222 du 25 septembre 2009, texte n° 55. NOR : CNIA0900022X.

- Délibération n° 2009-213 *sur la création par la Commission nationale de l'informatique et des libertés d'un site web dédié aux correspondants à la protection des données à caractère personnel* (demande d'avis n° 1358690). JORF n° 0142 du 21 juin 2009, texte n° 49. NOR : CNIA0900009X.

- Décision du 30 avril 2009 du président de la CNIL relative à la mise en œuvre par le service des correspondants informatique et libertés d'un site web dédié aux correspondants à la protection des données à caractère personnel. JORF n° 0142 du 21 juin 2009, texte n° 48. NOR : CNIA0900010S.

- Délibération n° 2008-487 du 2 décembre 2008 portant autorisation de traitement de données personnelles permettant la mise en œuvre généralisée du dossier pharmaceutique. [en ligne], disponible sur http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000020022185. Consulté le 28 mai 2014.

- Délibération n° 2008-422 du 6 novembre 2008 portant décision de la formation restreinte à l'égard de la société Cdiscount. [en ligne], disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/147/. Consulté le 28 mai 2014.

- Délibération n° 2008-005 du 10 janvier 2008 portant autorisation unique de mise en œuvre par les entreprises ou organismes exploitants de médicaments de traitements automatisés de données à caractère personnel relatifs à la gestion des données de santé recueillies dans le cadre de la pharmacovigilance des médicaments postérieurement à leur mise sur le marché. 10 Janvier 2008. JORF n° 0039 du 15 février 2008, texte n° 84. NOR : CNIA0800002X.

- Délibération n° 2007-194 du 10 juillet 2007 autorisant la mise en place généralisée par la Caisse nationale d'assurance maladie des travailleurs salariés d'un traitement permettant aux médecins d'accéder aux données relatives aux prestations servies aux bénéficiaires de l'assurance maladie. Historique des remboursements ou web médecin. [en ligne], disponible

sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017651846&fastReqId=1101993371&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 2007-106 du 15 mai 2007 portant autorisation des applications informatiques nécessaires à la mise en œuvre de la phase expérimentale du dossier pharmaceutique. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017652212. Consulté le 28 mai 2014.

- Délibération n° 2006-295 du 21 décembre 2006 portant adoption d'une norme simplifiée relative au traitement automatisé de données à caractère personnel mis en œuvre par les opticiens lunetiers pour la gestion d'une activité professionnelle. JORF n° 45 du 22 février 2007, texte n° 123. NOR : CNIA0600026X.

- Délibération n° 2006-162 du 8 juin 2006 portant adoption d'une norme simplifiée relative au traitement automatisé de données à caractère personnel mis en œuvre par les biologistes à des fins de gestion du laboratoire d'analyses de biologie médicale. (Norme simplifiée n° 53). JORF n° 160 du 12 juillet 2006 texte n° 72. NOR : CNIA0600015X.

- Délibération n° 2006-161 du 8 juin 2006 portant adoption d'une norme simplifiée relative au traitement automatisé de données à caractère personnel mis en œuvre par les pharmaciens à des fins de gestion de la pharmacie. (Norme simplifiée n° 52). JORF n° 154 du 5 juillet 2006. p. 10085, texte n° 91. NOR : CNIA0600014X.

- Délibération n° 2006-151 du 30 mai 2006 portant autorisation de mise en œuvre des applications informatiques nécessaires à l'expérimentation du dossier médical personnel. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017652120. Consulté le 28 mai 2014.

- Délibération n° 2006-082 du 21 mars 2006 portant avis sur la demande d'agrément présentée par le GIE Santeos, candidat à l'hébergement du dossier médical personnel dans le cadre de son expérimentation. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017651923&fastReqId=229741593&fastPos=13. Consulté le 28 mai 2014.

- Délibération n° 2006-081 du 21 mars 2006 portant avis sur la demande d'agrément présentée par la société inVita, candidate à l'hébergement du dossier médical personnel

dans le cadre de son expérimentation. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017651922&fastReqId=1051584247&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 2006-080 du 21 mars 2006 portant avis sur la demande d'agrément présentée par la société France Telecom candidate à l'hébergement du dossier médical personnel dans le cadre de son expérimentation. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017651921&fastReqId=1377763297&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 2006-056 du 2 mars 2006 décidant la dispense de déclaration des traitements mis en œuvre par les collectivités territoriales et les services du représentant de l'État dans le cadre de la dématérialisation du contrôle de légalité. (Norme d'exonération n° 05). JORF n° 102 du 30 avril 2006, texte n° 17. NOR : CNIA0600003X.

- Délibération n° 2005-296 du 22 novembre 2005 portant adoption de normes simplifiées relatives au traitement automatisé 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. (Norme simplifiée n° 50). JORF n° 7 du 8 janvier 2006, texte n° 19. NOR : CNIX0508937X

- Délibération n° 2004-097 du 9 décembre 2004 décidant la dispense de déclaration des traitements de gestion des rémunérations mises en œuvre par les personnes morales de droit privé autres que celles gérant un service public. (Norme d'exonération n° 02). JORF n° 4 du 6 janvier 2005, p. 287. Texte n° 54. NOR : CNIX0407889X.

- Délibération n° 2004-081 du 9 novembre 2004 autorisant une expérimentation présentée par la fédération nationale de la mutualité française ayant pour finalité d'accéder sous forme anonymisée aux données de santé, sur les feuilles de soins électroniques. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653182&fastReqId=906198484&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 2004-054 du 10 juin 2004 portant avis sur le projet de loi relatif à la réforme de l'assurance maladie. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653162. Consulté le 28 mai 2014.

- Délibération n° 04-018 du 8 avril 2004 relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653149&fastReqId=1458005962&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 04-017 du 8 avril 2004 relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en œuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy.[en ligne], disponible sur: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653148&fastReqId=1083531293&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 01-057 du 29 novembre 2001, portant recommandation sur la diffusion des données personnelles sur internet par les banques de données de jurisprudence. [en ligne], NOR : CNIX0105263X. Disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653503. Consulté le 28 mai 2014.

- Délibération n° 01-011 du 8 mars 2001 portant adoption d'une recommandation sur les sites de santé destinée au public. [en ligne], NOR : CNIX0104776X. Disponible sur: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653397&fastReqId=1787389670&fastPos=1. Consulté le 28 mai 2014.

- Délibération n° 00-064 du 19 décembre 2000 relative à un projet de décret en Conseil d'État portant création du « système de traitement des infractions constatées TIC » et application du troisième alinéa de l'article 31 de la loi du 6 janvier 1978. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653137&fastReqId=758927984&fastPos=1. Consulté le 16 avril 2014.

- Délibération n° 99-005 du 18 février 1999 portant avis sur un projet de loi présenté par le ministre de l'emploi et de la solidarité relatif à la couverture maladie universelle et sur deux articles additionnels concernant l'un, le volet de santé de la carte électronique d'assurance maladie et l'autre, la réalisation de traitements de données personnelles de santé à des fins d'évaluation ou d'analyse du système de santé. in 20ème rapport d'activités de la Cnil 1999.

p. 241-248. Disponible sur: http://www.ladocumentationfrancaise.fr/var/ storage/rapports-publics/004001043/0000.pdf. Consulté le 28 mai 2014.

- Délibération n° 97-008 du 4 février 1997 *portant adoption d'une recommandation sur le traitement des données de santé à caractère personne*l. [en ligne], NOR : CNIX9701968X. Disponible sur: http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000017653865. Consulté le 28 mai 2014.

- Délibération n° 83-058 du 29 novembre 1983 portant adoption d'une recommandation concernant la consultation du RNIP et l'utilisation du NIR. [en ligne], JORF du 21 janvier 1984. Disponible sur : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/35/. Consulté le 28 mai 2014.

- Délibération n° 82-205 du 7 décembre 1982 *portant avis conforme sur le projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi n° 78-17 du 6 janvier 1978 aux traitements automatisés d'informations nominatives mises en œuvre par les services des renseignements généraux*.[en ligne], disponible sur: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653966&fastReqId=1598837819&fastPos=1. Consulté le 16 avril 2014.

- Délibération n° 81-74 du 16 juin 1981 *portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile.* [en ligne], disponible sur: http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017654666&fastReqId=1988285836&fastPos=9. Consulté le 28 mai 2014.

ASIP SANTE

- *Premier rapport d'activité du Comité d'agrément des hébergeurs : 2006-2011 sous la présidence du Dr Philippe BICLET*. [en ligne], 7 Septembre 2011. 58 p. Disponible sur : http://esante.gouv.fr/sites/default/files/Rapport_CAH_4.08.11_VF.pdf. Consulté le 28 mai 2014.

- *Rapport d'activités 2010*. [en ligne], 84 p. Disponible sur : http://esante.gouv.fr/sites/default /files/ASIP_RA2010.pdf. Consulté le 13 février 2012

CONSEIL NATIONAL DE L'ORDRE DES MEDECINS (CNOM)

- DEAU, Xavier. *L'activité médicale auprès du médecin : peut-on admettre la prescription téléphonique et à quelles conditions ?* [en ligne], rapport adopté à la session du Conseil du 15 Octobre 2004. 4 p. Disponible sur : http://www.conseil-national.medecin.fr/sites/default /files/activitemedicaletelephonique.pdf. Consulté le 15 novembre 2011.

- *Les préconisations du Conseil national de l'ordre des médecins*. [en ligne], Télémédecine Janvier 2009. p. 5. Disponible sur: http://www.conseil-national.medecin.fr/sites/default/ files/telemedecine 2009.pdf. Consulté le 29 avril 2014.

- *L'interopérabilité médicale en Europe. Table ronde tenue au Conseil National dans le cadre de la présidence française de l'Union Européenne.*. [en ligne]. Compte rendu de la réUnion, 5 décembre 2008. 51 p. Disponible sur : http://www.medetic.com/docs/06/ interoperabilite-medicale-en-europe.pdf. Consulté le 28 mai 2014.

- MARCELLI, Aline.

  - *Le secret partagé*. [en ligne], rapport adopté lors de la session du Conseil national de l'ordre des médecins de mai 1998. 5 p. Disponible sur : http://www.conseil-national.medecin.fr/sites/default/files/secretpart.pdf. Consulté le 28 mai 2014.

  - *Relation entre le secret médical et les secrets professionnels*. [en ligne], *rapport adopté lors de la session du Conseil national de l'ordre des médecins du* 28 janvier 2000. 15 p. Disponible sur : http://www.conseil-national.medecin.fr/ sites/default/ files/ secretprofessionnel.pdf. Consulté le 19 mai 2014.

- *Sondage TNS Sofres sur l'informatisation de la santé* [en ligne]. 03 juin 2009. Disponible sur : http://www.conseil-national.medecin.fr/article/sondage-tns-sofres-pour-le-cnom-sur-l-informatisation-de-la-sante-656. Consulté le 29 avril 2104.

CONSEIL NATIONAL DE L'ORDRE DES PHARMACIENS (CNOP)

- *Charte du dossier pharmaceutique*. Direction de la communication du Conseil national de l'ordre des pharmaciens. 2009. (Non publiée).

ASSURANCE MALADIE

- *Rapport annuel 2009 du GIE SESAM-VITAL*. [en ligne], disponible sur : http://www.sesam-vitale.fr/nous-connaitre/docs/rapportannuel2009.pdf. Consulté le 3 mars 2012.

ASSOCIATION MEDICALE MONDIALE (AMM)

- *Déclaration d'Helsinki de Juin 1964*. [en ligne], The journal of the American Medical Association. 27 novembre 2013. Volume 310. n° 20. Disponible sur: http://www.wma.net/fr/30publications/10policies/b3/index.html. Consulté le 5 avril 2014.
- *Prise de position de l'AMM sur les principes directeurs pour l'utilisation de la télésanté dans les soins médicaux*.[en ligne], adoptée par la 60ème Assemblée Médicale Mondiale. Delhi, octobre 2009. Disponible sur : http://www.wma.net/fr/30publications/10policies/t5/index.html. Consulté le 28 mai 2014.

CLUB DES ACTEURS DE LA TELESANTE: (CATEL)

- *Rapport d'activités 2010-2011*.[en ligne], disponible sur: http://www.catel.pro/documents/Rapport-Activites-2010-2011-CATEL.pdf. Consulté le 29 avril 2014.

CONSEIL GENERAL DE L'INDUSTRIE, DE L'ENERGIE ET DES TECHNOLOGIES (CGIET)

- PICARD, Robert. PILLET, Didier. *Rapport n° 2010/42/CGIET/ SG : Caractérisation du secteur médico-social pour le développement d'offres TIC*.[en ligne], Décembre 2010. 53 p. Disponible sur: http://www.cgeiet.economie.gouv.fr/Rapports/Rapport_Caracterisation_

du_secteur_medico_social_pour_le_developpement_d_offres_TIC.pdf. Consulté le 15 Octobre 2011.

HAUTE AUTORITE DE LA SANTE: (HAS)

- *Recommandations professionnelles portant sur la prescription médicamenteuse par téléphone (ou téléprescription) dans le cas de la régulation médicale*. [en ligne], Février 2009. 31 p. Disponible sur : http://www.has-sante.fr/portail/upload/docs/application/pdf/2009-05/teleprescription_-_recommandations.pdf. Consulté le 27 octobre 2011.

COMMISSION D'ACCÈS AUX DOCUMENTS ADMINISTRATIFS: (CADA)

- *Centre hospitalier intercommunal Robert Ballanger*. [en ligne], Conseil n° 20130367. 20 juin 2013. Recueil des principaux avis et Conseils 1er semestre 2013. p. 9-10. Disponible sur : http://cada.data.gouv.fr/20130367/. Consulté le 12 décembre 2013.
- *Centre hospitalier universitaire (CHRU) de Montpellier*. [en ligne], Conseil n° 20131183. Séance du 28 mars 2013. Disponible sur : http://cada.data.gouv.fr/20131183/. Consulté le 28 mai 2014.
- *Directeur du centre hospitalier de Strasbourg*. [en ligne], Conseil n° 20053559. Séance du 6 Octobre 2005. Disponible sur : http://cada.data.gouv.fr/20053559/. Consulté le 28 mai 2014.
- *Directeur du centre hospitalier régional d'Orléans*. [en ligne], Avis n° 20100697. Séance du 25 février 2010. Recueil des principaux avis et conseils 1er semestre 2010. p. 9-10. Disponible sur : http://www.cada.fr/IMG/pdf/recueil2010_1.pdf. Consulté le 28 mai 2010.
- *Directeur du centre hospitalier René Dubos*. [en ligne], Conseil n° 20103989. Séance du 14 octobre 2010. Disponible sur : http://cada.data.gouv.fr/20103989/. Consulté le 28 mai 2014.

- *Directeur du centre hospitalier spécialisé de l'Yvonne*. [en ligne], Avis n° 20083853. Séance du 9 Octobre 2008. Disponible sur : http://cada.data.gouv.fr/20083853/. Consulté le 28 mai 2014.

- *Directeur général de l'Assistance Publique-hôpitaux de Paris (groupe hospitalier Cochin-Saint-Vincent-de-Paul/Maison de Solenn)*. [en ligne], Séance du 3 juillet 2008. Avis n° 20082236. Disponible sur : http://cada.data.gouv.fr/20082236/. Consulté le 28 mai 2014.

GROUPE D'ETUDES SOCIETE DE L'INFORMATION ET VIE PRIVEE

- CAMPANA Mireille. Groupe d'études société de l'information et vie privée. *La cryptographie in* La protection de la vie privée dans la société d'information. Chapitre 10. Tome 2. PUF, 2000. 62 p. http://www.asmp.fr/travaux/gpw/internetvieprivee/ rapport2/ chapitr10.pdf. Consulté le 28 mai 2014.

CONFERENCE NATIONALE DE LA SANTE

- *Avis sur les données de santé informatisées*. [en ligne], Assemblée plénière. 19 octobre 2010. 11 p. Disponible sur : http://www.sante.gouv.fr/IMG/pdf/Avis_donnees_sante_ 19102010.pdf. Consulté le 12 mai 2014.

RAPPORTS AU GOUVERNEMENT

- BRAIBANT, Guy. *Données personnelles et sociétés de l'information : Rapport au premier ministre sur la transposition en droit français de la directive n° 95-46*. Décembre 1998. La documentation française. Collection des rapports officiels. 292 p.

- COMITE CENTRAL D'ENQUETE SUR LE COÛT ET LE RENDEMENT DES SERVICES PUBLICS. *Conclusions sur Sesam-vitale. Sesam-vitale au-delà de l'informatique, un projet au service de la population*. [en ligne] 9 p. Disponible sur : http://www. ladocumentationfrancaise.fr/var/storage/rapports-publics/984000504/0000.pdf. Consulté le 27 mai 2014.

- FAGNIEZ, Pierre-Louis. *Le masquage d'informations par le patient dans son DMP*. [en ligne], 30 janvier 2007. 15p. Disponible sur : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000115/0000.pdf. Consulté le 2 mai 2014.

- GAGNEUX, Michel.

  - *Rapport sur la relance du DMP : pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé*. [en ligne], 23 avril 2008. 120 p. Disponible sur : http://www.sante.gouv.fr/IMG/pdf/Rapport_DMP_mission_Gagneux.pdf. Consulté le 27 mai 2014.

  - *Refonder la gouvernance du système d'information de santé.* [en ligne], Rapport. 3 mai 2009. 38 p. Disponible sur : http://www.sante.gouv.fr/IMG/pdf/Rapport_FINAL_.pdf. Consulté le 27 mai 2014.

- LASBORDES, Pierre. *La télésanté : un nouvel atout au service de notre bien-être : un plan quinquennal éco-responsable pour le déploiement de la télésanté en France*. [en ligne], Rapport. 15 octobre 2009. 247 p. Disponible sur : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/094000539/0000.pdf. Consulté le 27 mai 2014.

- MISSION INTERMINISTERIELLE de revue de projet sur le dossier médical personnel (DMP). *Rapport sur le dossier médical personnalisé (DMP)*. [en ligne], 8 Novembre 2007. 85 p. Disponible sur : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics//074000713/0000.pdf. Consulté le 12 décembre 2013.

- RAFFARIN, Jean-Pierre. *Discours du 12 novembre 2002 relatif au plan RE/SO 2007*. [en ligne], disponible sur : http://archives.internet.gouv.fr. Consulté le 20 février 2014.

- SIMON, Pierre et ACKER, Dominique. Rapport *La place de la télémédecine dans l'organisation des soins.* [en ligne], Novembre 2008. Ministère de la santé et des sports. 160 p. Disponible sur : http://www.sante.gouv.fr/IMG/pdf/Rapport_final_Telemedecine.pdf. Consulté le 28 mai 2014.

- TRUCHE, Pierre, FAUGERE Jean-Paul, FLICHY Patrice. *Administration électronique et protection des données personnelles-livre blanc*. Rapport. Février 2002. La documentation française. Collection des rapports officiels. 129 p.

LEGISLATIONS ETRANGERES

CANADA

- *Loi concernant le partage de certains renseignements de santé*. [en ligne], Projet de loi n° 59 (2012, chapitre 23). Assemblée nationale. Édition officielle du Québec 2012. Disponible sur : Http://www.dossierdesante.gouv.qc.ca/fichier/Loi-concernant-le-part age-de-certains-renseignements-de-sante.pdf. Consulté le 19 novembre 2013.

- *Loi modifiant la loi sur les services de santé et les services sociaux et de dispositions législatives.* [en ligne], Projet de loi n° 83 (2005, chapitre 32). Assemblée nationale. Édition officielle du Québec 2005. Disponible sur : http://www2.publicationsduquebec. gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2005C32F.PDF. Consulté le 6 décembre 2013.

- *Loi uniforme canadienne sur le commerce électronique*. [en ligne] Août 1999. Disponible sur : http://www.ulcc.ca/fr/us/index.cfm?sec=1&sub=lul. Consulté le 9 mars 2014.

- Décret n° 323-2013, du 27 mars 2013 *sur la loi concernant le partage de certains renseignements de santé* (2012, chapitre 23). Gazette officielle du Québec, 10 avril 2013, 145e année, n° 15. p. 1415.

- Décret 788-2012, 4 juillet 2012. Loi concernant le partage de certains renseignements de santé (2012, c.23). Gazette officielle du Québec. 18 juillet 2012, 144eme année, n° 29. p. 3669.
- Décret n° 566-2010 du 23 juin 2010 *concernant la poursuite du projet du Dossier santé du Québec.* (*Modification du décret du 18 juin 2009).* [en ligne], Gazette officielle du Québec, 14 juillet 2010, 142e année, n° 28. p. 3111. Disponible sur : Http://www.dossierdesante. gouv.qc.ca/fichier/Decret-566-2010.pdf. Consulté le 8 mars 2012.
- Décret n° 757-2009 du 18 juin 2009, *portant conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec*. [en ligne], Gazette officielle du Québec, 8 juillet 2009, 141eme année, n° 27. p.3162. Disponible sur : http://www. dossierdesante.gouv.qc.ca/fichier/Decret-757-2009.pdf**.** Consulté le 8 mars 2012.

- Décret n° 404-2008 23 avril 2008 *définissant les conditions de mise en œuvre du projet expérimental du dossier de santé du Québec*. [en ligne], Gazette officielle du Québec, 7 mai 2008, 140ème année, n° 19. p. 1979. Disponible sur : http://www.dossierdesante.gouv.qc.ca/fichier/Decret-404-2008.pdf. Consulté le 28 mai 2014.
- *Conditions de mise en œuvre de la deuxième phase du projet expérimental du Dossier de santé du Québec*. [en ligne], 2009. 39 p. Disponible sur : http://www.dossierdesante.gouv.qc.ca/fichier/conditions-mise-en-oeuvre-deuxieme-phase-experimental.pdf. Consulté le 28 mai 2014.

- *Document d'information concernant la mise en œuvre de la deuxième phase d'expérimentation du dossier de santé du Québec*. [en ligne], Mise à jour le 10 juin 2010. Ministère de la santé et des services sociaux. Disponible sur : http://www.dossier desante.gouv.qc.ca/download.php?f=df11f15de2c7fbb8788186012489e4c7. Consulté le 28 mai 2012.

- *Lignes directives relatives aux activités de télésanté RUIS UL*. [en ligne], Version-3.1. Août 2013. Ministère de la santé et des services sociaux. 23 p. Disponible sur : http://www.csssalphonsedesjardins.ca/fileadmin/CSSSAD/PDF/Centres_d_expertises_et_services_r%C3%A9gionaux/Lignes_directrices_RUIS-UL_V_3_1_finale.pdf. Consulté le 21 avril 2014.

ESPAGNE

- Loi 16/2010 du 3 juin 2010 *modifiant la loi 21/2000 du 29 décembre 2000* sur *le droit à l'information médicale et l'autonomie du patient ainsi que la documentation clinique* [en ligne], disponible sur: http://noticias.juridicas.com/base_datos/CCAA/ca-l16-2010.html. Consulté le 10 février 2014

- Loi 11/2007 du 22 juin *relative à l'accès des citoyens aux services publics par voie électronique.* [en ligne], Bulletin officiel de l'Etat "Boletín oficial del estado" n° 150, du 23 juin 2007, p. 27150-27166. Disponible sur : https://www.boe.es/buscar/doc.php?id=BOE-A-2007-12352. Consulté le 10 février 2014

- Loi 3/2005 du 17 mars 2005 *modifiant la loi 3/2001 du 28 mai 2001 régissant le recueil du consentement du patient dans le cadre de l'élaboration de son dossier médical*. [en ligne], disponible sur : http://noticias.juridicas.com/base_datos/CCAA/ga-l3-2005.html. Consulté le 10 février 2014

- Loi 16/2003 du 28 mai 2003 *portant sur la cohésion et la qualité du système national de santé.* [en ligne], disponible sur : http://noticias.juridicas. com/base_datos/Admin/l16-2003.html. Consulté le 10 février 2014.

- Loi 41/2002 du 14 novembre 2002 *portant sur les règles fondamentales relatives à l'autonomie du patient ainsi que ses droits et obligations en matière d'information et de documentation clinique*. [en ligne], Bulletin officiel de l'Etat "Boletín oficial del estado" n° 274 du 15 novembre 2002, pp. 40126-40132. Disponible sur : http://www.boe.es/diario _boe/txt.php?id=BOE-A-2002-22188. Consulté le 10 février 2014

- Loi organique 15/1999 du 13 décembre 1999 *relative à la protection des données à caractère personnel.* [en ligne], Bulletin officiel de l'Etat "Boletín oficial del estado" n° 298 du 14 Décembre 1999. Disponible sur : http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750. Consulté le 10 février 2014.

- Décret 38/2012 du 13 mars 2012 *portant sur le dossier médical et les droits et obligations des patients et des professionnels de santé en matière de documentation clinique*. [en ligne], disponible sur : http://noticias.juridicas.com/base_datos/CCAA/pv-d38-2012.html. Consulté le 10 février 2014

- Décret royal 1093/2010 *portant approbation de la liste minimale de données que doit contenir un dossier médica*l. [en ligne], Bulletin officiel de l'Etat" Boletín oficial del estado" n° 225 du 16 septembre 2010, p. 78742-78767. Disponible sur : http://www.boe.es/ buscar/doc.php?id=BOE-A-2010-14199. Consulté le 10 février 2014

- Décret royal 4/2010, du 8 janvier 2010 *de régulation du programme national d'interopérabilité dans le domaine de l'administration électronique*. [en ligne], disponible sur : http://noticias.juridicas.com/base_datos/Admin/rd4-2010.html. Consulté le 10 février 2014

- Décret royal 1720/2007, du 21 décembre, *portant approbation du règlement d'application de la loi organique 15/1999, du 13 de décembre, de protection des données personnelles*. [en ligne], disponible sur : http://noticias.juridicas.com/base_datos/Admin/rd1720-2007.html. Consulté le 10 février 2014
- Décret royal 183/2004 *relatif à la carte individuelle de santé*. [en ligne], disponible sur: http://noticias.juridicas.com/base_datos/Admin/rd183-2004.html. Consulté le 10 février 2014
- Arrêté du 26 octobre 2011 *sur les critères techniques et/ou scientifiques d'accès aux dossiers médicaux à des fins épidémiologiques ou de santé publique*. Diario oficial de Galicia" (DOG) n° 219 du mercredi 16 novembre 2011. p. 33555.

ALLEMAGNE

- Loi fédérale *sur la protection des données (BDBS) du 27 janvier 1977 modifiée en août 2009 est entrée en vigueur en septembre 2009 et en avril 2010*. [en ligne], Federal Data Protection Act. Federal law. Gazette I, p. 2814. Disponible sur: Http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile. Consulté le 28 mars 2014.

PAYS BAS

- Loi *sur la protection des données personnelles, "Wet Bescherming personsgegevens"* du 6 juillet 2000. [en ligne], disponible sur : http://maxius.nl/wet-bescherming-persoonsgegevens. Consulté le 11 août 2013.

SUÈDE

- Loi *sur les données des patients, "Patientdatalag (SFS 2008 : 355)"* du 1er juillet 2008. [en ligne], disponible sur: http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Patientdatalag-2008355_sfs-2008355/?bet=2008:355. Consulté le 29 mai 2014.
- Loi *sur les biobanques dans les soins de santé : medical care act, (SFS 2002 : 297)* du 23 mai 2002. [en ligne], disponible sur : http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/

Svenskforfattningssamling/Lag-2002297-om-biobanker-i-_sfs-2002-297/. Consulté le 29 mai 2014.

- Loi *sur le registre des soins de santé (1998: 543, lagen om hälsodataregister)* du 11 juin 1998. [en ligne], disponible sur : http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/sfs_sfs-1998-543/. Consulté le 29 mai 2014.

- Loi *sur la protection des données, "personuppgiftslag (1998:204)"* du 29 avril 1998. [en ligne], disponible sur : http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/?bet=1998:204. Consulté le 23 janvier 2013.

- Loi *sur la prévention médicale, la recherche et le traitement des maladies et des blessures (SFS 1982 :763, halso-och sjukvårdslagen)* du 30 juin 1982. [en ligne], disponible sur : http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Halso--och-sjukvardslag-1982_sfs-1982-763/. Consulté le 29 mai 2014.

- Ordonnance *sur les données patient (SFS 2008 : 360, patientdataförordningen)* du 29 mai 2008 [en ligne], mise à jour par l'ordonnance 2013:124 entrée en vigueur le 1er Avril 2013. Disponible sur : http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Patientdataforordning-200836_sfs-2008-360/?bet=2008:360. Consulté le 03 Avril 2013.

LUXEMBOURG

- Loi du 2 août 2002 *relative à la protection des personnes à l'égard du traitement des données à caractère personnel modifiée*. [en ligne], Mémorial Journal officiel du grand-duché de Luxembourg. A - n° 91 du 13 août 2002. p. 1836. Disponible sur : http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf#zoom=125,0,0& page mode=none. Consulté le 7 mars 2014.

- Règlement grand-ducal du 27 novembre 2004 *concernant le chargé de la protection des données et portant exécution de l'article 40, paragraphe (10) de la loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel*. [en ligne], Mémorial Journal officiel du grand-duché. A - n° 200 du 20 décembre 2004. p.

2956. Disponible sur : http://www.legilux.public.lu/leg/a/archives/2004/0200/a200.pdf. Consulté le 28 mars 2014.

V. JURISPRUDENCE

COUR EUROPÉENNE DES DROITS DE L'HOMME (CEDH)

- CEDH 6 octobre 2009, *C. C. c. Espagne*, n° 1425/06. in Conseil de l'Europe 2010. *Note d'information sur la jurisprudence de la Cour* n° 123, Octobre 2009. p. 18. ISSN 1814-6511.

- CEDH 4 décembre 2008, *S. et Marper c. Royaume-Uni,* n° 30562/04 et n° 30566/04. [en ligne], disponible sur: http://www.echr.coe.int et la vidéo sur: http://www.echr.coe.int/ Pages/home.aspx?p=hearings&w=3056204_27022008&language=lang. Consulté le 29 mai 2014.

- CEDH 2 décembre 2008, *K.U. c. Finlande,* no 2872/02, [en ligne], disponible sur: http://hudoc.echr.coe.int/sites/fra/Pages/search.aspx?i=001-90015#{"itemid":["001-90015"]}. Consulté le 29 mai 2014.

- CEDH 24 juillet 2008, *Me André c. France*, n° 18603/03, Gazette du palais, 13 janvier 2009, Commentaire PANNIER, Jean.

- CEDH 10 octobre 2006, *L.L. c. France*, n° 7508/02, [en ligne], disponible sur: http://www.courdecassation.fr/IMG/File/pdf_2007/observatoire_droit_europeen/veille_cedh_2006%20_internet.pdf. Consulté le 1 juin 2014.

- CEDH 20 octobre 2005, *Gunnarsson c. Islande*, n°. 4591/04, [en ligne], Note d'information n° 79 sur la jurisprudence de la Cour, octobre 2005, p. 19-20. Disponible sur : http://www.echr.coe.int/Documents/CLIN_2005_10_79_FRA_824904.pdf. Consulté le 29 mai 2014.

- CEDH 9 mars 2004, *Glass c. Royaume-Uni*, no. 61827/00, Recueil 2004 II p. 52-81.
- CEDH 9 juin 1998 *McGinley et Egan c. Royaume-Uni*, Recueil 1998-III, p. 1362, § 97.
- CEDH 25 février 1997, *Z. c. La Finlande*, R.D.P.C, 1998, p. 311-345.
- CEDH, 21 septembre 1994, *Fayed c. Royaume-Uni*, n° 17101/90, Série A no. 294-B, p. 50-51, § 67.
- CEDH 26 mars 1987 *Leander c. Suède* n° 9248/81, [en ligne], disponible sur : http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-62077#{"itemid":["001-62077"]}. Consulté le 29 mai 2014.
- CEDH, 26 mars 1985, *X et Y c. Pays-Bas*. n° 8978/80, RSC 1985, p. 629. Obs. PETTITI, L. E.

COUR DE JUSTICE DE L'UNION EUROPÉENNE (CJUE)

- CJUE, grande chambre 12 juillet 2011, l'Oréal *SA contre eBay international AG*, n° C-324/09. [en ligne], disponible sur : http://curia.europa.eu/juris/document/document.jsf?docid=107261&doclang=FR. Consulté le 30 mai 2014.
- CJUE 7 décembre 2010, grande chambre, , *Peter Pammer*. n° C-585/08 et C-144/09. [en ligne], Document n° 62008CJ0585. Disponible sur : http://curia.europa.eu/juris/celex.jsf?celex=62008CJ0585&lang1=en&lang2=MT&type=NOT&ancre=. Consulté le 30 avril 2014.
- CJUE, grande chambre 23 mars 2010, *Google France et Google*, n° C-236/08 à C-238/08. [en ligne], disponible sur : http://curia.europa.eu/juris/celex.jsf?celex=62008CJ0236&lang1=fr&type=TXT&ancre=. Consulté le 30 mai 2014.
- CJCE. 19 avril 2007, *Stamatelaki*, n° C-444/05. JOCE 96/14 du 28 avril 2007.
- CJCE 16 mai 2006, *Watts*, n° C-372/04, Recueil. p. I-4325

- CJCE 6 novembre 2003, *Götta Hovrätt c. Bodil Linqvist*, n° C- 101/01. [en ligne], disponible sur : http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIn dex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=205847. Consulté le 30 mai 2014.

- CJCE 28 avril 1998, *Kohll*, n° C-158/96, Recueil. p. I-1931.

CONSEIL CONSTITUTIONNEL

- Décision n° 2009-580 du 10 juin 2009 *portant sur la loi favorisant la diffusion et la protection de la création sur Internet.* JORF du 13 juin 2009, p. 9675. Recueil, p. 107.

- Décision n° 2008-562 DC du 21 février 2008. *Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental*. JORF du 26 février 2008, p. 3272. Recueil, p. 89.

- Décision n° 2007-557 DC du 15 novembre 2007. *Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile.* JORF du 21 novembre 2007, p. 19001. Recueil, p. 360.

- Décision n° 2006-544 DC du 14 décembre 2006. *Loi de financement de la sécurité sociale pour 2007.* JORF du 22 décembre 2006, p. 19356. Recueil, p. 129.

- Décision n° 2005-532 DC du 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, JORF du 24 janvier 2006, p. 1138. Recueil, p. 31.

- Décision n° 2004-504 DC du 12 août 2004 *relative à la loi sur l'assurance maladie*. JORF du 17 août 2004, p. 14657. Recueil, p. 153.

- Décision n° 2004-499 DC du 29 juillet 2004, *Loi 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.14087. Recueil, p. 126.

- Décision n° 2004-492 DC du 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, JORF du 10 mars 2004, p. 4637. Recueil, p. 66.

- Décision n° 2003-484 DC du 20 novembre 2003. *Loi relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité*. JORF du 27 novembre 2003, p. 20154. Recueil, p. 438.
- Décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, JORF du 13 mars 2003, p. 4789. Recueil, p. 211.
- Décision n° 2000-433 DC du 27 juillet 2000. *Loi modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication*. JORF n° 177 du 2 août 2000. p. 11922, texte n° 2. NOR : CSCL0004281S. Recueil, p. 121.
- Décision n° 99-419 DC, 9 novembre 1999. *Loi relative au pacte civil de solidarité.* JORF du 16 novembre 1999. p. 16962, texte n° 2. NOR : CSCL9903826S.
- Décision n° 99-416 DC du 23 juillet 1999. *Loi portant création d'une couverture maladie universelle*. JORF du 28 juillet 1999, p. 11250. Recueil, p. 100.
- Décision n° 98-405 DC du 29 décembre 1998. *Loi de finances pour 1999*. JORF du 31 décembre 1998, p. 20138. Recueil, p. 326.
- Décision n° 94-352 DC du 18 janvier 1995. *Loi d'orientation et de programmation relative à la sécurité*. JORF du 21 janvier 1995. p.1154. Recueil, p. Recueil, p. 170.
- Décisions n° 93-325 DC du 13 août 1993. *Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France.* JORF du 18 août 1993, p. 11722. NOR : CSCX9310124S.
- Décision n° 80-127 DC du 20 janvier 1981. *Loi renforçant la sécurité et protégeant la liberté des personnes*. JORF du 22 janvier 1981, p. 308. Recueil, p. 15.

COUR DES COMPTES

- REFERE n° 46485 délibéré le 15 septembre 2006. [en ligne], Annexe I du rapport JEGOU. Disponible sur : http://www.senat.fr/rap/r07-035/r07-035_mono.html#toc44. Consulté le 5 avril 2014.

CONSEIL D'ÉTAT

- 10EME ET 9EME SOUS-SECTIONS REUNIES, 11 avril 2014. *Ligue des droits de l'homme*, n° 360759. Disponible sur : http://www.conseil-etat.fr/fr/selection-de-decisions-du-conseil-d-etat/ce-11-avril-2014-ligue-des-droits-de-l-homme-.html. Consulté le 30 mai 2014.

- 10EME ET 9EME SOUS-SECTIONS REUNIES, 12 mars 2014, *Société Foncia groupe c/ CNIL*, n° 354629. [en ligne], JurisData n° 2014-004450. Disponible sur : http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000028717845. Consulté le 3 avril 2014.

- 10EME ET 9EME SOUS-SECTIONS REUNIES, 26 mars 2012, *Sociétés pages jaunes groupe c/ Commission national de l'informatique et des libertés.* [en ligne] n° 353193. Tables du recueil Lebon 2014. Disponible sur : http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000025580456&fastReqId=95055113&fastPos=1. Consulté le 30 mai 2014.

- 8EME ET 3EME SOUS-SECTIONS REUNIES, 13 janvier 2010, *M. et Mme Philippe A*, [en ligne], n° 321416, disponible sur : http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000021697573&fastReqId=1428592503&fastPos=1. Consulté le 30 mai 2014.

- 10EME ET 9EME SOUS-SECTION REUNIES, 17 novembre 2006, *Mme A.* [en ligne], n° 270863. Inédit au Recueil Lebon. Disponible sur : http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000008238833&fastReqId=148504015&fastPos=1. Consulté le 1 juin 2014.

- 1ERE ET 6EME SOUS-SECTIONS REUNIES, 26 septembre 2005, n° 270234 *Conseil national de l'ordre des médecins*. Recueil Lebon. RDSS 2006, p. 53. Note CRISTOL, Danièle.

- 4EME ET 6EME SOUS-SECTIONS REUNIES, 28 avril 2003, *M. André X*. n° 238181. [en ligne], Tables du Recueil Lebon. Revue Gestions Hospitalières 2004, n° 435, p. 284-285. ISSN : 0016-9218.

- SECTION DU CONTENTIEUX, 18 décembre 2002, *Mme Duvignères*, n° 233618, Recueil Lebon. [en ligne], disponible sur: http://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000008124026. Consulté le 30 mai 2014.

- SECTION DU CONTENTIEUX, 28 juillet 2000, *Association France nature environnement*, n° 204024. Recueil Lebon, p. 323. AJDA 2000, p. 959, Obs. ONDOUA, A.

- 10EME ET 7EME SOUS-SECTIONS REUNIES, 28 juillet 1995 *Confédération générale du travail*. [en ligne], n° 132453. Recueil Lebon 1995. Disponible sur: http://www.legifrance.gouv.fr/affichJuriAdmin.do?idTexte=CETATEXT000007899367&dateTexte=. Consulté le 30 mai 2014.

- 4EME ET 1ERE SOUS SECTIONS REUNIES, 28 juin 1995 M. Guy X c. Conseil national de l'ordre des médecins. [en ligne], n° 154253 inédit au recueil Lebon. Disponible sur: http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte= CETATEXT000007881812&fastReqId=755892474&fastPos=2. Consulté le 4 avril 2013.
- ASSEMBLEE, 10 avril 1992. *Époux V.,* n° 79027. Recueil Lebon 1992. RFDA 11 mai 1992, p. 571, AJDA, 20 mai 1992, p. 355, note LEGAL, Hubert.

- 1ERE ET 4EME SOUS SECTIONS REUNIES, 8 février 1989, n° 54494. *Conseil national de l'ordre des médecins.* Table du Recueil Lebon 1989. RDSS 1990, p. 308. Note DUBOIS, Louis.

- SECTION DU CONTENTIEUX, 5 juin 1987, *M. Kaberseli*, n° 59674. Recueil Lebon 1987. p. 205. AJDA, 1987. p. 606.

- SECTION DU CONTENTIEUX, 11 février 1972 *Sieur Crochette,* n° 76799. Recueil Lebon 1972, p. 138. JCPG 1973, II, n° 17363.
- ASSEMBLEE, du 12 avril 1957 *Deve*. Dalloz 1957, p. 336.

- SECTION SOCIALE, 2 juin 1953 *Ministre du Travail et de la Sécurité sociale*. Bulletin de l'ordre des médecins 1952-1954. p. 194.

- SECTION SOCIALE, 6 février 1951 *Ministre du Travail et de la Sécurité sociale.* [en ligne], disponible sur : http://www.legislation.cnav.fr/jur/JUR-CE_06021951.htm. Consulté le 1er juin 2014.

COUR DE CASSATION

- Cass. crim. 30 octobre 2013, *M. Jean-Jacques X.*, n° 12-84.784. Bull. crim. 2013, n° 210, p. 404. JurisData n° 2013-023970. www.lexisnexis.com. Consulté le 10 Décembre 2013.
- Cass. civ. 2ème, 10 mai 2012, *Caisse primaire d'assurance maladie de Vaucluse*, n° 10-28.767. [en ligne], arrêt inédit. Disponible sur : http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000025862593&fastReqId=281814186&fastPos=8. Consulté le 3 juin 2014.
- Cass. civ. 1ère, 17 février 2011. 3 arrêts : respectivement n°s 09-13.202, 09-67.896, 09-15.857. [en ligne], n° 164, 165, 166, Bulletin numérique. Disponible sur : http://www.courdecassation.fr. Consulté le 2 juin 2014.
- Cass. com., 19 Octobre 2010, *Société JFA chantier naval c/ société Kerstholt teakdecksystems BV*, n° 09-69.246. Bull. 2010, IV, n° 154.
- Cass. crim. 9 mars 2010, *X. Philippe*, n° 09-81.778. [en ligne], disponible sur : http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000022136495&fastReqId=505705257&fastPos=1. Consulté le 3 juin 2014.
- Cass. civ., 1ère 24 Septembre 2009. *Société Jacky Boy Music c. M Salvado*r. n° 08-11.112. Bull 2009, VII, n° 184, p. 166. JurisData: 2009-049655.
- Cass, Crim., 14 mars 2006, *Fabrice H. / Ministère public*, n° 05-83.423. Gazette du Palais, 20 juillet 2006 n° 201, p. 41. Note BENSOUSSAN-BRULE, Virginie.
- Cass. civ. 1ère, 7 février 2006 *M. Jean Fx.*, n° 04-10941. Bull. civ. 2006, I, n° 59, p. 59.
- Cass.Crim., 28 septembre 2004 *Marc X.*, n° 03-86.604. Gazette du Palais, 9 avril 2005 n° 99, p. 38. Note A.C.

- Cass. civ. 1ère, 12 juillet 2001 *Société X*, n° 98-21.337 Bull. civ. 2001, I, n° 222. Dalloz, n° 17, 25 avril 2002, p. 1380-1383. Note BIGOT, Christophe.
- Cass. civ. 1ère, 29 novembre 1994, *Le GAEC de Perros*, n° 92-15.783. Bull. civ. 1994. I. n° 353. p. 254.
- Cass. crim. 6 juin 1972, *Demoiselle Aubert*, n° 70-90.271. Bull. crim. n° 190, Gazette du palais 1972, II, p. 668.
- Cass. civ. 1ère, 25 mai 1971, *Dame Y*, n° 69-14.266. Bull. civ. I, n°. 171. p. 144. JCPG, 1971, II, 16859.
- Cass. civ. 1ère, 21 février 1961. Bull. civ. 1961, I, n° 112. P. 90.
- Cass. civ. 1ère ,8 Novembre 1955, JCP 1955, II, 9014. Observation de SAVATIER, René.
- Cass. civ. 2ème, 17 décembre 1954, *Centre national de transfusion sanguine et autres*, JCPG 1954, II. 8490.
- Cass. civ. 21 juin 1950, *Messageries Maritimes*. Revue. Critique. 1950. P.609, note BATIFFOL. Dalloz 1951. P. 749, note HAMEL, Joseph. JCP 1950. II. 5812, note LEVY, Jean Philippe.
- Cass. crim., 8 mai 1947, *Degraene*, Bull. crim. 1947, n° 126. Dalloz 1948- p. 109. Note GULPHE.
- Cass. civ. 20 mai 1936, *Mercier*. Droit pénal 1936, I, p. 88. Conclusions MATTER.
- Cass. crim., 19 décembre 1885, *Watelet*. Bull. crim. 1885, n° 363. Droit pénal 1986-I. p.347.
- Cass. crim. 26 juillet 1845, Almir-Charles Saint Pair. Bull. crim. 1845, n° 245. Droit Pénal 1845, I, p. 340.
- Req., 18 juin 1835, *Thouret-Noroy*, S. 1835, I, 26, p. 401. Droit pénal 1835,I, p. 300, Conclusions DUPIN.

COUR D'APPEL

- C.A Paris, 1ère chambre, section F. 27 janvier 2005. *M. Y. L...c. Ordre des avocats*. Gazette du palais n° 33 du 2 février 2005. p. 4-14.
- C.A Lyon, 17 novembre 1952, JCP 1953, II, p. 7541. Note SAVATIER.
- C.A Paris, 14 Avril 2010. *Omar S. Fred T et a. c. Société Daily Motion*. RLDI 2010/62, n° 2034. p. 47. Note HAR-DOUIN.
- C.A Paris, 11 décembre 2013, *Google Ireland, Google France / Olivier Martinez.* Note Legalnews. [en ligne], 21 janvier 2014. Disponible sur: http://www.legalnews.fr.doc-distant.univ-lille2.fr/index.php?option=com_content&view=article&id=294713:le-statut-dhebergeur-est-confere-a-google-pour-son-service-adwords&catid=71:technologies-de-linformation& Itemid=150. Consulté le 3 juin 2014.

TRIBUNAL DE GRANDE INSTANCE

- TGI Paris, 1ère chambre 4 avril 2006 *Syndicat Sud Télécom Paris c/ S.A. France Télécom, Monsieur Patrick C. et Monsieur Bertrand G*. n° RG : 05/18400. RJS 12/06, n° 1242. p. 929 et suiv.
- TGI Paris, 3ème chambre, 2ème section 25 avril 2003, *Sonacotra / Syndicat Sud Sonacotra*. [en ligne], n° RG : 02/02978. Disponible sur http://www.legalis.net/ spip.php?page= jurisprudence-decision&id_article=120. Consulté le 3 juin 2014.
- TGI Paris, 1ère chambre, section sociale, 19 avril 2005, *Comité d'entreprise d'Effia Services, Syndicat Sud Rail / Effia Services*. [en ligne], n° RG : 05/003282. Disponible sur : http://www.juripole.fr/J20050419.php. Consulté le 3 juin 2014.
- TGI Brest, Chambre correctionnelle, 11 juin 2013. RLDI 2013/97, n° 3226. Observations L.C.

TRIBUNAL DES CONFLITS

- T. confl., 14 février 2000, n° 02929, LPA 2000, n° 196, p. 8, note. WELSCH S. RFDA 2000, p. 1232 note POUYAUD, D.

COUR SUPREME DU CANADA

- Cour suprême du Canada. 11 juin 1992. *McInerney c. MacDonald*, [en ligne], 2 R.C.S. 138. Dossier 21899. Disponible sur : http://csc.lexum.org/fr/1992/1992rcs2-138/1992rcs2-138.html. Consulté le 5 novembre 2011.

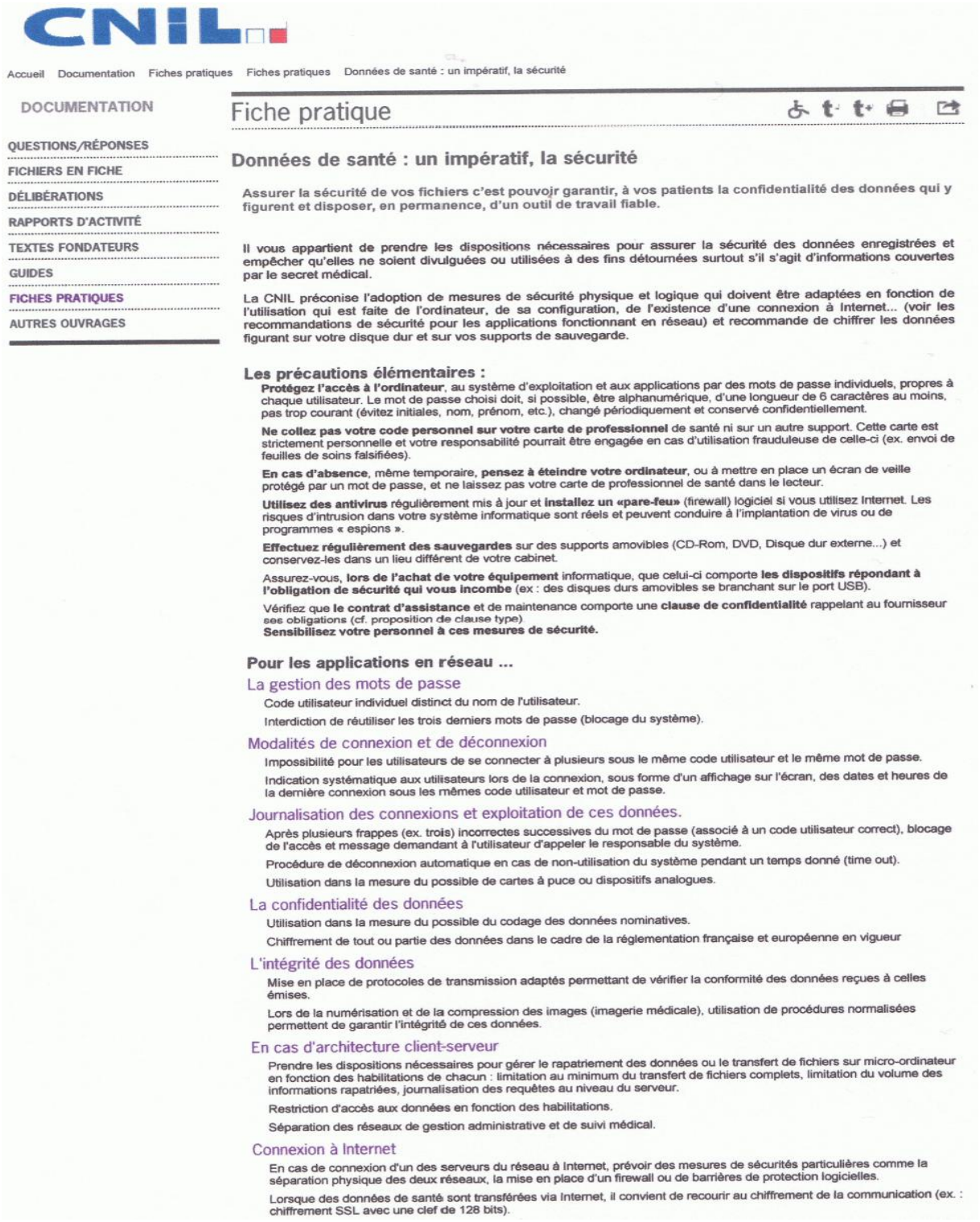
VI. SITES WEB

- AFNOR boutique : http://www.boutique.afnor.org/
- Asip santé: http://esante.gouv.fr/
- Association francophone des utilisateurs de logiciels libres: http://aful.org/association/
- Assurance maladie: http://www.ameli.fr
- CATEL: http://www.catel.pro/
- CNIL : http://www.cnil.fr/
- Commission européenne: http://ec.europa.eu/
- Conseil d'État: http://www.conseil-etat.fr/
- Conseil national de l'ordre national des médecins : http://www.conseil-national.medecin.fr/
- Cour de Cassation: http://www.courdecassation.fr/
- Cour européenne des droits de l'homme: http://www.echr.coe.int/
- Direction générale de la compétitivité, de l'industrie et des services: http://www.industrie.gouv.fr/
- Dossier santé Québec: www.dossierdesante.gouv.qc.ca
- E-Health interop: http://www.ehealth-interop.nen.nl/
- EPSOS: http://www.epsos.eu/france/le-projet-epsos.html
- Groupe de la de travail «article 29» : http://ec.europa.eu/justice/data-protection/article-29
- Health Level Seven International: http://www.hl7.org/.
- Journal du net: www.journaldunet.com/
- Journal officiel de la république française: http://www.journal-officiel.gouv.fr/
- Légifrance : http://www.legifrance.gouv.fr

- Ministère de la santé : http://www.sante.gouv.fr
- Portail DMP: www.dmp.gouv.fr
- Régie de l'assurance maladie du Québec : http://www.ramq.gouv.qc.ca/
- Sésame Vitale : http://www.sesam-vitale.fr

TABLE DES ANNEXES

ANNEXE I: DONNÉES DE SANTÉ: UN IMPÉRATIF, LA SÉCURITÉ



CNIL

Accueil Documentation Fiches pratiques Fiches pratiques Données de santé : un impératif, la sécurité

DOCUMENTATION

QUESTIONS/RÉPONSES
FICHIERS EN FICHE
DÉLIBÉRATIONS
RAPPORTS D'ACTIVITÉ
TEXTES FONDATEURS
GUIDES
FICHES PRATIQUES
AUTRES OUVRAGES

Fiche pratique

Données de santé : un impératif, la sécurité

Assurer la sécurité de vos fichiers c'est pouvoir garantir, à vos patients la confidentialité des données qui y figurent et disposer, en permanence, d'un outil de travail fiable.

Il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées surtout s'il s'agit d'informations couvertes par le secret médical.

La CNIL préconise l'adoption de mesures de sécurité physique et logique qui doivent être adaptées en fonction de l'utilisation qui est faite de l'ordinateur, de sa configuration, de l'existence d'une connexion à Internet... (voir les recommandations de sécurité pour les applications fonctionnant en réseau) et recommande de chiffrer les données figurant sur votre disque dur et sur vos supports de sauvegarde.

Les précautions élémentaires :

Protégez l'accès à l'ordinateur, au système d'exploitation et aux applications par des mots de passe individuels, propres à chaque utilisateur. Le mot de passe choisi doit, si possible, être alphanumérique, d'une longueur de 6 caractères au moins, pas trop courant (évitez initiales, nom, prénom, etc.), changé périodiquement et conservé confidentiellement.

Ne collez pas votre code personnel sur votre carte de professionnel de santé ni sur un autre support. Cette carte est strictement personnelle et votre responsabilité pourrait être engagée en cas d'utilisation frauduleuse de celle-ci (ex. envoi de feuilles de soins falsifiées).

En cas d'absence, même temporaire, **pensez à éteindre votre ordinateur**, ou à mettre en place un écran de veille protégé par un mot de passe, et ne laissez pas votre carte de professionnel de santé dans le lecteur.

Utilisez des antivirus régulièrement mis à jour et **installez un «pare-feu»** (firewall) logiciel si vous utilisez Internet. Les risques d'intrusion dans votre système informatique sont réels et peuvent conduire à l'implantation de virus ou de programmes « espions ».

Effectuez régulièrement des sauvegardes sur des supports amovibles (CD-Rom, DVD, Disque dur externe...) et conservez-les dans un lieu différent de votre cabinet.

Assurez-vous, **lors de l'achat de votre équipement** informatique, que celui-ci comporte **les dispositifs répondant à l'obligation de sécurité qui vous incombe** (ex : des disques durs amovibles se branchant sur le port USB).

Vérifiez que **le contrat d'assistance** et de maintenance comporte une **clause de confidentialité** rappelant au fournisseur ses obligations (cf. proposition de clause type)
Sensibilisez votre personnel à ces mesures de sécurité.

Pour les applications en réseau ...

La gestion des mots de passe

Code utilisateur individuel distinct du nom de l'utilisateur.

Interdiction de réutiliser les trois derniers mots de passe (blocage du système).

Modalités de connexion et de déconnexion

Impossibilité pour les utilisateurs de se connecter à plusieurs sous le même code utilisateur et le même mot de passe.

Indication systématique aux utilisateurs lors de la connexion, sous forme d'un affichage sur l'écran, des dates et heures de la dernière connexion sous les mêmes code utilisateur et mot de passe.

Journalisation des connexions et exploitation de ces données.

Après plusieurs frappes (ex. trois) incorrectes successives du mot de passe (associé à un code utilisateur correct), blocage de l'accès et message demandant à l'utilisateur d'appeler le responsable du système.

Procédure de déconnexion automatique en cas de non-utilisation du système pendant un temps donné (time out).

Utilisation dans la mesure du possible de cartes à puce ou dispositifs analogues.

La confidentialité des données

Utilisation dans la mesure du possible du codage des données nominatives.

Chiffrement de tout ou partie des données dans le cadre de la réglementation française et européenne en vigueur

L'intégrité des données

Mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises.

Lors de la numérisation et de la compression des images (imagerie médicale), utilisation de procédures normalisées permettent de garantir l'intégrité de ces données.

En cas d'architecture client-serveur

Prendre les dispositions nécessaires pour gérer le rapatriement des données ou le transfert de fichiers sur micro-ordinateur en fonction des habilitations de chacun : limitation au minimum du transfert de fichiers complets, limitation du volume des informations rapatriées, journalisation des requêtes au niveau du serveur.

Restriction d'accès aux données en fonction des habilitations.

Séparation des réseaux de gestion administrative et de suivi médical.

Connexion à Internet

En cas de connexion d'un des serveurs du réseau à Internet, prévoir des mesures de sécurités particulières comme la séparation physique des deux réseaux, la mise en place d'un firewall ou de barrières de protection logicielles.

Lorsque des données de santé sont transférées via Internet, il convient de recourir au chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits).

Source: CNIL . *Données de santé un impératif, la sécurité*. Disponible sur http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/un-imperatif-la-securite/.

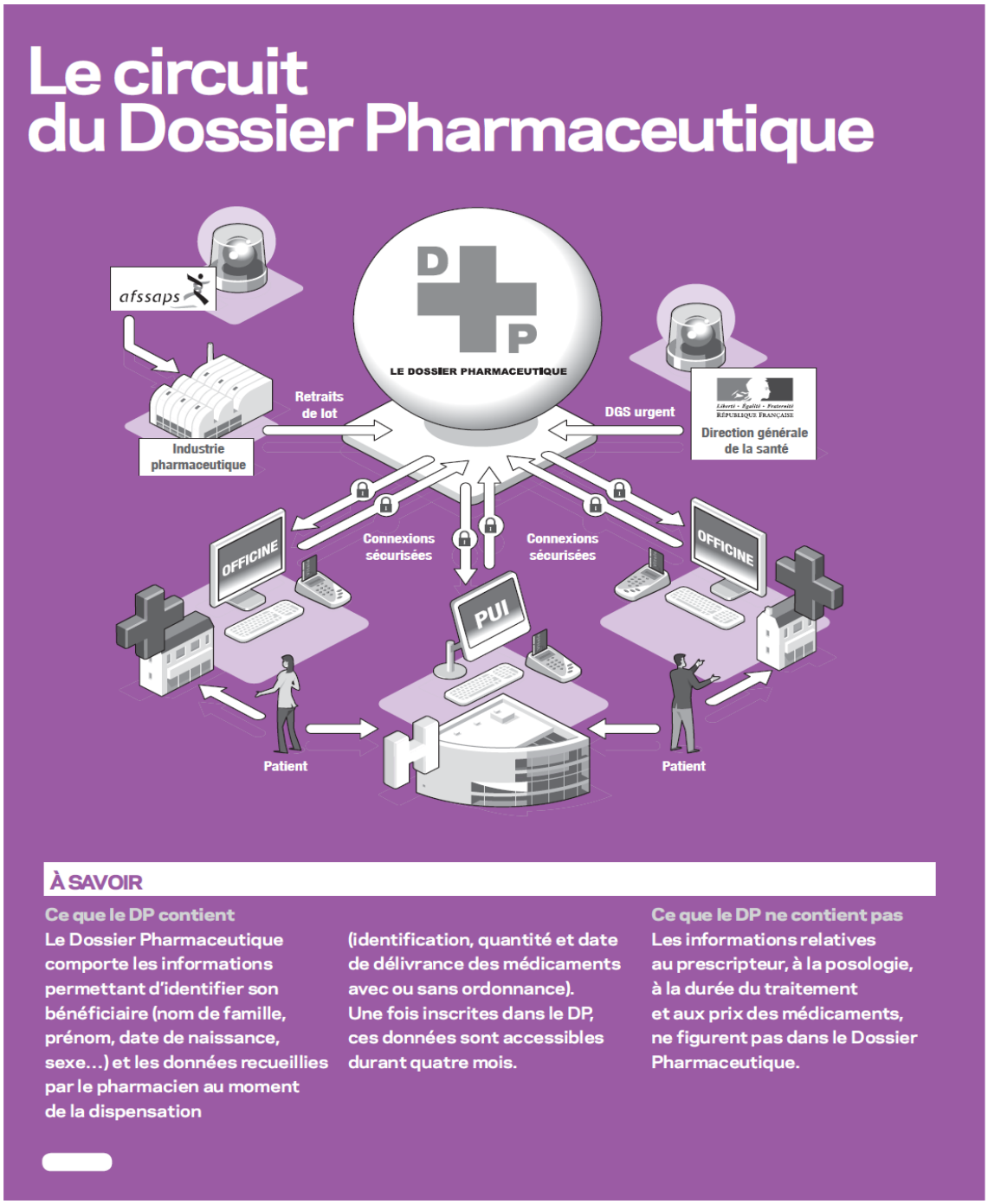
Evaluez le niveau de sécurité des données personnelles dans votre organisme

Avez-vous pensé à ?

Fiche		Mesure	
1	Analyser les risques	**Recensez** les fichiers et données à caractère personnel et les traitements	❑
		Déterminez les menaces et leurs impacts sur la vie privée des personnes	❑
		Mettez en œuvre des **mesures de sécurité adaptées** aux menaces	❑
2	Authentifier les utilisateurs	Définissez un identifiant ***(login)*** unique à chaque utilisateur	❑
		Adoptez une **politique de mot de passe utilisateur rigoureuse**	❑
		Obligez l'utilisateur à **changer son mot de passe après réinitialisation**	❑
3	Gérer les habilitations & sensibiliser les utilisateurs	**Définissez des profils d'habilitation**	❑
		Supprimez les permissions d'accès obsolètes	❑
		Documentez les procédures d'exploitation	❑
		Rédigez une **charte informatique** et annexez-la au **règlement intérieur**	❑
4	Sécuriser les postes de travail	**Limitez le nombre de tentatives d'accès** à un compte	❑
		Installez un «**pare-feu**» *(firewall)* logiciel	❑
		Utilisez des **antivirus régulièrement mis à jour**	❑
		Prévoyez une procédure de **verrouillage automatique de session**	❑
5	Sécuriser l'informatique mobile	Prévoyez des **moyens de chiffrement** pour les **ordinateurs portables** et les unités de stockage amovibles (**clés USB**, CD, DVD…)	❑
6	Sauvegarder et prévoir la continuité d'activité	Effectuez des **sauvegardes régulières**	❑
		Stockez les supports de sauvegarde dans un endroit sûr	❑
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	❑
		Prévoyez et testez régulièrement la **continuité d'activité**	❑
7	Encadrer la maintenance	**Enregistrez les interventions** de maintenance dans une **main courante**	❑
		Effacez les données de tout matériel avant sa **mise au rebut**	❑
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	❑
8	Tracer les accès et gérer les incidents	Prévoyez un **système de journalisation**	❑
		Informez les utilisateurs de la mise en place du système de journalisation	❑
		Protégez les équipements de journalisation et les informations journalisées	❑
		Notifiez les personnes concernées des accès frauduleux à leurs données	❑
9	Protéger les locaux	**Restreignez les accès** aux locaux au moyen de **portes verrouillées**	❑
		Installez des **alarmes anti-intrusion** et vérifiez-les périodiquement	❑
10	Protéger le réseau informatique interne	**Limitez les flux réseau au strict nécessaire**	❑
		Sécurisez les accès distants des appareils informatiques nomades par **VPN**	❑
		Utilisez le protocole SSL avec une clé de 128 bits pour les **services web**	❑
		Mettez en œuvre le protocole WPA - AES/CCMP pour les réseaux WiFi	❑
11	Sécuriser les serveurs et les applications	Adoptez une **politique de mot de passe administrateur rigoureuse**	❑
		Installez sans délai les **mises à jour critiques**	❑
		Assurez une **disponibilité** des données	❑
12	Gérer la sous-traitance	Prévoyez une **clause spécifique** dans les contrats des sous-traitants	❑
		Assurez-vous de l'**effectivité des garanties** prévues (audits de sécurité, visites...)	❑
		Prévoyez les **conditions de restitution** et de destruction des données	❑
13	Archiver	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	❑
		Détruisez les archives obsolètes de manière sécurisée	❑
14	Sécuriser les échanges avec d'autres organismes	**Chiffrez** les données avant leur envoi	❑
		Assurez-vous qu'il s'agit du **bon destinataire**	❑
		Transmettez le **secret** lors d'un envoi distinct et via un canal différent	❑

Source: CNIL. *Les guides de la cnil* Guide 2010. Disponible sur: http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf

ANNEXE III: LE CIRCUIT DU DOSSIER PHARMACEUTIQUE



Source: CNOP. *Le dossier pharmaceutique* in Les cahiers de l'ordre des pharmaciens. n° 1. p. 12. Disponible sur: http://www.ordre.pharmacien.fr/Communications/Publications-ordinales/Le-Dossier-Pharmaceutique.

ANNEXE IV: DÉCRET CONFIDENTIALITÉ

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA SANTÉ ET DES SOLIDARITÉS

Décret nº 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)

NOR : *SANP0721653D*

Le Premier ministre,

Sur le rapport du ministre de la santé et des solidarités,

Vu le code de la santé publique, notamment son article L. 1110-4 ;

Vu le code de la sécurité sociale, notamment ses articles L. 161-33, L. 161-36 (A) et R. 161-54 ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret nº 2005-1309 du 20 octobre 2005 pris pour l'application de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi nº 2004-801 du 6 août 2004 ;

Vu les avis de la Commission nationale de l'informatique et des libertés en date du 11 octobre 2005 et du 21 décembre 2006 ;

Le Conseil d'Etat (section sociale) entendu,

Décrète :

Art. 1er. – Le chapitre préliminaire du titre Ier du livre Ier de la première partie du code de la santé publique (dispositions réglementaires) est ainsi modifié :

I. – La section unique devient la section 2, intitulée « Section 2 : Associations de bénévoles », et son article R. 1110-1 devient l'article R. 1110-4.

II. – Avant la section 2, il est inséré une section 1 ainsi rédigée :

« Section 1

« Confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique

« *Art. R. 1110-1.* – La conservation sur support informatique des informations médicales mentionnées aux trois premiers alinéas de l'article L. 1110-4 par tout professionnel, tout établissements et tout réseau de santé ou tout autre organisme intervenant dans le système de santé est soumise au respect de référentiels définis par arrêtés du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. Ces référentiels s'imposent également à la transmission de ces informations par voie électronique entre professionnels.

« Les référentiels déterminent les fonctions de sécurité nécessaires à la conservation ou à la transmission des informations médicales en cause et fixant le niveau de sécurité requis pour ces fonctions.

« Ils décrivent notamment :

« 1º Les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers ;

« 2º Les modalités d'accès aux traitements, dont les mesures d'identification et de vérification de la qualité des utilisateurs, et de recours à des dispositifs d'accès sécurisés ;

« 3º Les dispositifs de contrôle des identifications et habilitations et les procédures de traçabilité des accès aux informations médicales, ainsi que l'histoire des connexions ;

« 4º En cas de transmission par voie électronique entre professionnels, les mesures mises en œuvre pour garantir la confidentialité des informations échangées, le cas échéant, par le recours à un chiffrement en tout ou partie de ces informations.

« *Art. R. 1110-2.* – Pour chaque traitement mis en œuvre par les personnes et les organismes mentionnés à l'article R. 1110-1 et comportant des informations médicales à caractère personnel, le dossier de déclaration ou de demande d'autorisation auprès de la Commission nationale de l'informatique et des libertés décrit les moyens retenus afin d'assurer la mise en conformité de ce traitement avec le référentiel le concernant.

« Le responsable du traitement, au sens de l'article 3 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, est chargé de veiller au respect du référentiel. Il lui appartient notamment de :

« 1° Gérer la liste nominative des professionnels habilités à accéder aux informations médicales relevant de ce traitement et la tenir à la disposition des personnes concernées par ces informations ;

« 2° Mettre en œuvre les procédés assurant l'identification et la vérification de la qualité des professionnels de santé dans les conditions garantissant la cohérence entre les données d'identification gérées localement et celles recensées par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale ;

« 3° Porter à la connaissance de toute personne concernée par les informations médicales relevant du traitement les principales dispositions prises pour garantir la conformité au référentiel correspondant.

« *Art. R. 1110-3.* – 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. »

Art. 2. – A compter de la date de publication des arrêtés mentionnés à l'article R. 1110-1 du code de la santé publique, dans sa rédaction issue du présent décret, les professionnels de santé, établissements, réseaux ou organismes mentionnés à cet article disposent d'un délai d'un an pour se mettre en conformité avec les dispositions des articles R. 1110-1 à R. 1110-2 du même code.

Les dispositions de l'article R. 1110-3 du code de la santé publique ne sont applicables aux établissements de santé que dans un délai de trois ans à compter de la publication du présent décret.

Art. 3. – Le ministre de la santé et des solidarités est chargé de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 15 mai 2007.

DOMINIQUE DE VILLEPIN

Par le Premier ministre :

Le ministre de la santé et des solidarités,
PHILIPPE BAS

Source: www.legifrance.fr

ANNEXE V: DÉCRET HÉBERGEMENT

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA SANTÉ ET DES SOLIDARITÉS

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 (dispositions réglementaires)

NOR : *SANX0500308D*

Le Président de la République,

Sur le rapport du Premier ministre et du ministre de la santé et des solidarités,

Vu le code du patrimoine, notamment le titre Ier du livre II ;

Vu le code de la santé publique, notamment ses articles L. 1111-7, L. 1111-8 et L. 1112-1 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, notamment ses articles 21 et 24 ;

Vu 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 ;

Vu le décret n° 97-34 du 15 janvier 1997 modifié relatif à la déconcentration des décisions administratives individuelles, notamment son article 2 ;

Vu le décret n° 97-1185 du 19 décembre 1997 modifié pris pour l'application à la ministre de l'emploi et de la solidarité du 1° de l'article 2 du décret du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu l'avis du Conseil national de l'ordre des médecins en date du 1er avril 2004 ;

Vu l'avis du Conseil national de l'ordre des chirurgiens-dentistes en date du 8 avril 2004 ;

Vu l'avis du Conseil national de l'ordre des pharmaciens en date du 11 mai 2004 ;

Vu l'avis du Conseil national de l'ordre des sages-femmes en date du 26 mai 2004 ;

Vu les avis de la Commission nationale de l'informatique et des libertés en date des 27 mai 2004 et 15 mars 2005 ;

Le Conseil d'Etat (section sociale) entendu ;

Le conseil des ministres entendu,

Décrète :

Art. 1er. – Le chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique (dispositions réglementaires) est ainsi modifié :

I. – La section unique devient la sous-section 1, intitulée « Sous-section 1 : Accès aux informations de santé à caractère personnel », au sein d'une section 1 dont le titre est ainsi rédigé :

« Section 1

« Principes généraux »

II. – Après l'article R. 1111-8, il est ajouté une sous-section 2 ainsi rédigée :

« Sous-section 2

« Hébergement des données de santé à caractère personnel

« *Art. R. 1111-9.* – Toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel, mentionné à l'article L. 1111-8, et bénéficier d'un agrément à ce titre doit remplir les conditions suivantes :

« 1° Offrir toutes les garanties pour l'exercice de cette activité, notamment par le recours à des personnels qualifiés en matière de sécurité et d'archivage des données et par la mise en œuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données confiées, ainsi qu'un usage conforme à la loi ;

« 2° Définir et mettre en œuvre une politique de confidentialité et de sécurité, destinée notamment à assurer le respect des exigences de confidentialité et de secret prévues par les articles L. 1110-4 et L. 1111-7, la protection contre les accès non autorisés ainsi que la pérennité des données, et dont la description doit être jointe au dossier d'agrément dans les conditions fixées par l'article R. 1111-14 ;

« 3° Le cas échéant, identifier son représentant sur le territoire national au sens de l'article 5 de la loi du 6 janvier 1978 ;

« 4° Individualiser dans son organisation l'activité d'hébergement et les moyens qui lui sont dédiés, ainsi que la gestion des stocks et des flux de données ;

« 5° Définir et mettre en place des dispositifs d'information sur l'activité d'hébergement à destination des personnes à l'origine du dépôt, notamment en cas de modification substantielle des conditions de réalisation de cette activité ;

« 6° Identifier les personnes en charge de l'activité d'hébergement, dont un médecin, en précisant le lien contractuel qui les lie à l'hébergeur.

« *Art. R.* 1111-10.* – L'agrément nécessaire à l'activité d'hébergement de données de santé à caractère personnel est délivré par le ministre chargé de la santé, qui se prononce après avis de la Commission nationale de l'informatique et des libertés et d'un comité d'agrément placé auprès de lui.

« A cet effet, la personne intéressée adresse au ministre chargé de la santé un dossier de demande d'agrément comprenant les éléments mentionnés à l'article R. 1111-12. Le ministre transmet le dossier à la Commission nationale de l'informatique et des libertés, qui apprécie les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données. La commission rend son avis dans un délai de deux mois à compter de la réception du dossier, délai pouvant être renouvelé une fois sur décision motivée de son président.

« Dès que la commission s'est prononcée ou à l'expiration du délai qui lui était imparti, elle transmet la demande d'agrément, accompagnée, le cas échéant, de son avis, au comité d'agrément mentionné au premier alinéa. Ce comité se prononce sur tous les aspects du dossier, en particulier sur les garanties d'ordre éthique, déontologique, technique, financier et économique qu'offre le candidat. Il émet son avis dans le mois qui suit la réception du dossier transmis par la Commission nationale de l'informatique et des libertés. Il peut toutefois demander un délai supplémentaire d'un mois.

« Le ministre chargé de la santé dispose, pour prendre sa décision, d'un délai de deux mois suivant l'avis du comité d'agrément. A l'issue de ce délai, son silence vaut décision de rejet.

« *Art. R. 1111-11.* – I. – Le comité d'agrément mentionné à l'article R. 1111-10 comprend :

« 1° Un membre de l'inspection générale des affaires sociales nommé sur proposition du chef de l'inspection générale des affaires sociales ;

« 2° Deux représentants des associations compétentes en matière de santé, agréées au niveau national dans les conditions prévues à l'article L. 1114-1 ;

« 3° Deux représentants des professions de santé, l'un nommé sur proposition du Conseil national de l'ordre des médecins et l'autre sur proposition de l'Union nationale des professions de santé ;

« 4° Trois personnalités qualifiées :

« *a)* Une personne choisie en raison de ses compétences dans les domaines de l'éthique et du droit ;

« *b)* Une personne choisie en raison de ses compétences en matière de sécurité des systèmes d'information et de nouvelles technologies ;

« *c)* Une personne choisie en raison de ses compétences dans le domaine économique et financier.

« Le directeur général de la santé, le directeur de l'hospitalisation et de l'organisation des soins, le directeur des Archives de France, le directeur général des entreprises et le directeur général de la concurrence, de la consommation et de la répression des fraudes, ou leurs représentants, assistent aux séances du comité avec voix consultative.

« II. – Les membres du comité d'agrément, dont celui qui, parmi eux, exercera la présidence du comité, sont nommés pour cinq ans par arrêté du ministre chargé de la santé. Leur mandat est renouvelable une fois.

« Lors de leur entrée en fonction, les membres du comité adressent au président une déclaration mentionnant toute activité personnelle ou professionnelle en rapport direct ou indirect avec les missions du comité, ainsi que les liens directs ou indirects qu'ils peuvent avoir avec tout organisme hébergeant ou susceptible d'héberger des données de santé à caractère personnel ou avec les organismes professionnels et les sociétés de conseil intervenant dans le domaine de compétence du comité. Ils s'engagent à signaler toute modification concernant cette situation.

« Ils ne peuvent siéger lorsque est examinée une affaire relative à un organisme au sein duquel ils détiennent un intérêt, exercent des fonctions ou détiennent un mandat, ou au sein duquel ils ont, au cours des dix-huit mois précédant la séance, détenu un intérêt, exercé des fonctions ou détenu un mandat.

« Des suppléants en nombre égal au nombre de titulaires sont désignés dans les mêmes conditions que ceux-ci. Un membre titulaire empêché ou intéressé par une affaire est remplacé par son suppléant.

« Le remplacement d'un membre du comité en cas de cessation de fonction en cours de mandat est réalisé dans les mêmes conditions que sa nomination et pour la durée du mandat restant à courir.

« Les fonctions de membre du comité ouvrent droit à des indemnités pour frais de déplacement et de séjour dans les conditions prévues par les dispositions législatives et réglementaires applicables aux fonctionnaires civils de l'Etat.

« III. – Le comité d'agrément ne peut délibérer que si deux tiers au moins de ses membres sont présents. Dans le cas contraire, une nouvelle séance peut se tenir sans obligation de quorum après un délai de quinze jours.

« Les avis rendus par le comité sont motivés. Ils sont pris à la majorité des voix exprimées des membres présents. En cas de partage égal des voix, celle du président est prépondérante.

« IV. – Le comité d'agrément peut être saisi par le ministre chargé de la santé de tout sujet entrant dans son domaine de compétence.

« *Art. R. 1111-12.* – Le dossier de demande d'agrément comprend les éléments suivants :

« 1° L'identité et l'adresse du responsable du service d'hébergement et, le cas échéant, de son représentant ; pour les personnes morales, les statuts sont produits ;

« 2° Les noms, fonctions et qualifications des opérateurs chargés de mettre en œuvre le service, ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont accès aux données hébergées ;

« 3° L'indication des lieux dans lesquels sera réalisé l'hébergement ;

« 4° Une description du service proposé ;

« 5° Les modèles de contrats devant être conclus, en application du deuxième alinéa de l'article L. 1111-8, entre l'hébergeur de données de santé et les personnes physiques ou morales qui sont à l'origine du dépôt des données de santé à caractère personnel ; ces modèles sont établis conformément aux dispositions de l'article R. 1111-13 ;

« 6° Les dispositions prises pour assurer la sécurité des données et la garantie des secrets protégés par la loi, notamment la présentation de la politique de confidentialité et de sécurité prévue au 2° de l'article R. 1111-9 ;

« 7° Le cas échéant, l'indication du recours à des prestataires techniques externes et les contrats conclus avec eux ;

« 8° 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.

« L'hébergeur déjà agréé informe sans délai le ministre chargé de la santé de tout changement affectant les informations mentionnées ci-dessus et de toute interruption, temporaire ou définitive, de son activité.

« *Art. R. 1111-13.* – Les modèles de contrats devant être joints à la demande d'agrément, mentionnés au 5° de l'article R. 1111-12, contiennent obligatoirement au moins les clauses suivantes :

« 1° La description des prestations réalisées : contenu des services et résultats attendus ;

« 2° Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels de santé et les établissements de santé les prenant en charge et désignés par eux peuvent être autorisés à accéder à ces données ou en demander la transmission et l'indication des conditions de mise à disposition de ces données ;

« 3° Lorsque le contrat est souscrit par un professionnel de santé ou un établissement de santé, la description des modalités selon lesquelles les données hébergées sont mises à leur disposition, ainsi que les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et de transmission ;

« 4° La description des moyens mis en œuvre par l'hébergeur pour la fourniture des services ;

« 5° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure ;

« 6° Les obligations de l'hébergeur à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ;

« 7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement ;

« 8° Une information sur les garanties permettant de couvrir toute défaillance éventuelle de l'hébergeur ;

« 9° Une présentation des prestations à la fin de l'hébergement.

« *Art. R. 1111-14.* – Une présentation de la politique de confidentialité et de sécurité, prévue au 2° de l'article R. 1111-9, doit être fournie à l'appui de la demande d'agrément conformément au 6° de l'article R. 1111-12. Elle comporte notamment les précisions suivantes :

« 1° En matière de respect des droits des personnes concernées par les données hébergées :

« *a)* Les modalités permettant de s'assurer de l'existence du consentement de l'intéressé à l'hébergement des données le concernant ;

« *b)* Les modalités retenues pour que l'accès aux données de santé à caractère personnel et leur transmission éventuelle n'aient lieu qu'avec l'accord des personnes concernées et par les personnes désignées par elles ;

« *c)* Les conditions dans lesquelles sont présentées et prises en compte les éventuelles demandes de rectification des données de santé à caractère personnel hébergées ;

« *d)* Les moyens mis en œuvre pour assurer le respect des dispositions de l'article L. 1111-7 relatif à l'accès des personnes à leurs informations de santé, notamment en termes de délais et de modalités de consultation ;

« *e)* Les procédures de signalement des incidents graves, dont l'altération des données ou la divulgation non autorisée des données personnelles de santé ;

« *f)* La fourniture à la personne concernée par les données hébergées, à sa demande, de l'historique des accès aux données et des consultations ainsi que du contenu des informations consultées et des traitements éventuellement opérés.

« 2° En matière de sécurité de l'accès aux informations :

« *a)* Les dispositions prises pour garantir la sécurité des accès et des transmissions des données de santé à caractère personnel vis-à-vis des établissements ou des professionnels de santé à l'origine du dépôt et des personnes concernées par ces données ;

« *b)* Les mesures prises en matière de contrôle des droits d'accès et de traçabilité des accès et des traitements ;

« *c)* Les conditions de vérification du contenu des traces des accès et des traitements afin de détecter les tentatives d'effraction ou d'accès non autorisés ;

« *d)* Les modalités de vérification du registre des personnes habilitées à accéder aux données hébergées tenant compte des éventuelles mises à jour ;

« *e)* Les procédés techniques retenus en matière d'identification et d'authentification ; en ce qui concerne les professionnels de santé, ces procédés techniques doivent avoir été agréés par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale.

« 3° En matière de pérennité des données hébergées :

« *a)* Les procédures visant à assurer, au moment du transfert des données vers l'hébergeur, la réception sécurisée des données et l'intégrité de celles-ci, leur prise en compte dans le système d'information de l'hébergeur et le suivi de cette prise en charge ;

« *b)* Les modalités de prise en compte et d'enrichissement tout au long de la durée de l'hébergement, de l'ensemble des informations concernant les données depuis leur création, telles que les données permettant de les identifier et de les décrire, de les gérer, de déterminer leurs propriétés techniques et d'en assurer la traçabilité ;

« *c)* Les modalités de surveillance des supports en vue d'anticiper les changements technologiques et, le cas échéant, d'opérer des migrations de supports dans des conditions en garantissant la traçabilité ;

« *d)* Les procédures liées à la réplication des données sur différents supports informatiques en des lieux distincts ;

« *e)* Les conditions de mise en œuvre d'une alerte concernant les formats d'encodage des données, destinée à avertir la personne à l'origine du dépôt en cas d'obsolescence de ce format et, éventuellement, les procédures visant à réaliser, avec l'autorisation de la personne à l'origine du dépôt, des migrations de formats des données, si ces derniers ne permettent plus d'assurer la lisibilité des informations et à assurer la traçabilité de ces migrations.

« 4° En matière d'organisation et de procédures de contrôle interne en vue d'assurer la sécurité des traitements et des données :

« *a)* La désignation d'un responsable sécurité et d'un responsable qualité ;

« *b)* La définition des missions, des pouvoirs et des obligations des personnels de l'hébergeur et de ses éventuels sous-traitants, habilités à traiter les données de santé à caractère personnel ;

« *c)* Les spécifications techniques des logiciels et des mécanismes de sécurité propres à garantir la confidentialité des transmissions, notamment en ce qui concerne le mode de chiffrement des flux d'information ;

« *d)* Les modalités retenues pour l'évaluation périodique des risques et l'audit des mesures de protection mises en place afin de garantir la sécurité des données et en vue d'apporter les modifications nécessaires en cas de détection de défaillances ;

« *e)* Les dispositifs de simulation régulière de défauts de fonctionnement pour vérifier l'efficacité des mécanismes destinés à garantir la continuité des services ;

« *f)* Les moyens mis en œuvre pour sensibiliser et former le personnel aux mesures de protection mises en place et à leurs obligations en matière de confidentialité et de respect du secret professionnel ;

« *g)* Les conditions de mise en œuvre de la sécurité physique des sites informatiques, des mesures de protection de l'infrastructure technique, notamment en termes de sécurité des réseaux, des serveurs et des postes de travail ;

« *h)* Les dispositions prises en ce qui concerne l'exploitation de l'infrastructure technique ;

« *i)* Les conditions de mise en œuvre du plan de secours informatique comportant notamment les dispositions prises pour informer du déclenchement de ce plan les personnes physiques ou morales à l'origine du dépôt des données de santé à caractère personnel ainsi que les dispositions prises pour la reprise des activités.

« *Art. R. 1111-15.* – L'agrément est délivré aux hébergeurs de données de santé à caractère personnel pour une durée de trois ans.

« La demande de renouvellement doit être déposée au plus tard six mois avant le terme de la période d'agrément. Elle comprend les documents mentionnés au 8° de l'article R. 1111-12 et un récapitulatif des modifications intervenues depuis la dernière demande d'agrément en ce qui concerne les autres documents mentionnés à cet article, ainsi qu'un audit externe réalisé aux frais de l'hébergeur, attestant de la mise en œuvre de la politique de confidentialité et de sécurité mentionnée à l'article R. 1111-14. Elle est instruite selon la même procédure que celle applicable à la demande initiale.

« Les décisions d'agrément, ainsi que le renouvellement de cet agrément, sont publiées au *Bulletin officiel* du ministère de la santé.

« *Art. R. 1111-16.* – Le ministre chargé de la santé, lorsqu'il envisage de procéder au retrait d'un agrément en application du quatrième alinéa de l'article L. 1111-8, communique à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception, les motifs de ce projet de retrait et l'appelle à formuler ses observations, écrites ou, à sa demande, orales, dans un délai de deux mois.

« En cas de divulgation non autorisée de données de santé à caractère personnel ou de manquements graves de l'hébergeur à ses obligations mettant notamment en cause l'intégrité, la sécurité et la pérennité des données hébergées, le ministre chargé de la santé peut, à titre conservatoire, dans l'attente qu'il soit statué définitivement sur le projet de retrait d'agrément, prononcer la suspension de l'activité d'hébergement.

« La décision de retrait est notifiée à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception. Elle met fin de plein droit à l'hébergement des données confiées à l'hébergeur et entraîne la restitution de ces données aux personnes ayant contracté avec l'hébergeur.

« Les décisions de suspension et de retrait font l'objet de la mesure de publicité prévue à l'article R. 1111-15. Elles sont transmises pour information au comité d'agrément mentionné à l'article R. 1111-10 ainsi qu'à la Commission nationale de l'informatique et des libertés. »

Art. 2. – I. – Après le premier alinéa de l'article R. 1111-2 du code de la santé publique, il est inséré un alinéa ainsi rédigé :

« Dans le cas où les informations demandées sont détenues par un établissement de santé et si les dispositifs techniques de l'établissement le permettent, le demandeur peut également consulter par voie électronique tout ou partie des informations en cause. »

II. – L'article R. 1112-7 du même code est remplacé par les dispositions suivantes :

« *Art. R. 1112-7.* – Les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur agréé en application des dispositions à l'article L. 1111-8.

« Le directeur de l'établissement veille à ce que toutes dispositions soient prises pour assurer la garde et la confidentialité des informations ainsi conservées ou hébergées.

« Le dossier médical mentionné à l'article R. 1112-2 est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein. Lorsqu'en application des dispositions qui précèdent, la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. Dans tous les cas, si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de dix ans à compter de la date du décès. Ces délais sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité médicale de l'établissement de santé ou de professionnels de santé à raison de leurs interventions au sein de l'établissement.

« A l'issue du délai de conservation mentionné à l'alinéa précédent et après, le cas échéant, restitution à l'établissement de santé des données ayant fait l'objet d'un hébergement en application de l'article L. 1111-8, le dossier médical peut être éliminé. 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. »

III. – Le délai de conservation des dossiers médicaux fixé à l'article R. 1112-7 du code de la santé publique s'appliquera à l'issue d'un délai de douze mois suivant la publication du présent décret.

Art. 3. – Au 2 du titre II de l'annexe au décret n° 97-1185 du 19 décembre 1997, le tableau intitulé « code de la santé publique » est ainsi complété :

26	Agrément nécessaire à l'activité d'hébergement de données de santé à caractère personnel.	Art. R.* 1111-10

Art. 4. – Les dispositions du présent décret peuvent être modifiées par décret en Conseil d'Etat, à l'exception de celles qui déterminent la compétence du ministre chargé de la santé figurant à l'article R.* 1111-10 du code de la santé publique et de celles de l'article 3 du présent décret dont la modification ne peut intervenir que dans les conditions prévues à l'article 2 du décret du 15 janvier 1997.

Art. 5. – Le Premier ministre, le ministre de la santé et des solidarités et le ministre de la culture et de la communication sont responsables, chacun en ce qui le concerne, de l'application du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 4 janvier 2006.

JACQUES CHIRAC

Par le Président de la République :

Le Premier ministre,
DOMINIQUE DE VILLEPIN

Le ministre de la santé et des solidarités,
XAVIER BERTRAND

Le ministre de la culture et de la communication,
RENAUD DONNEDIEU DE VABRES

Source: www.legifrance.fr

ANNEXE VI: DÉCRET TÉLÉMÉDECINE

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA SANTÉ ET DES SPORTS

Décret nº 2010-1229 du 19 octobre 2010
relatif à la télémédecine

NOR : *SASH1011044D*

Le Premier ministre,

Sur le rapport de la ministre de la santé et des sports,

Vu le code de l'action sociale et des familles ;

Vu le code de la santé publique, notamment son article L. 6316-1 ;

Vu le code de la sécurité sociale ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi nº 85-772 du 25 juillet 1985 portant diverses dispositions d'ordre social, notamment son article 44 ;

Vu l'avis du Haut Conseil des professions paramédicales en date du 28 avril 2010 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 3 mai 2010 ;

Vu l'avis de la Caisse centrale de la mutualité sociale agricole en date du 11 mai 2010 ;

Vu l'avis de la commission des accidents du travail et des maladies professionnelles en date du 12 mai 2010 ;

Vu l'avis de la Caisse nationale de l'assurance maladie des travailleurs salariés en date du 25 mai 2010 ;

Vu l'avis de la Haute Autorité de santé en date du 23 juin 2010 ;

Vu l'avis de l'Union nationale des caisses d'assurance maladie en date du 1er juillet 2010 ;

Le Conseil d'Etat (section sociale) entendu,

Décrète :

Art. 1er. – Après le chapitre V du titre Ier du livre III de la sixième partie du code de la santé publique est ajouté un chapitre VI ainsi rédigé :

« CHAPITRE VI

« Télémédecine

« Section 1

« Définition

« *Art. R. 6316-1.* – Relèvent de la télémédecine définie à l'article L. 6316-1 les actes médicaux, réalisés à distance, au moyen d'un dispositif utilisant les technologies de l'information et de la communication. Constituent des actes de télémédecine :

« 1º La téléconsultation, qui a pour objet de permettre à un professionnel médical de donner une consultation à distance à un patient. Un professionnel de santé peut être présent auprès du patient et, le cas échéant, assister le professionnel médical au cours de la téléconsultation. Les psychologues mentionnés à l'article 44 de la loi nº 85-772 du 25 juillet 1985 portant diverses dispositions d'ordre social peuvent également être présents auprès du patient ;

« 2º La téléexpertise, qui a pour objet de permettre à un professionnel médical de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux en raison de leurs formations ou de leurs compétences particulières, sur la base des informations médicales liées à la prise en charge d'un patient ;

« 3º La télésurveillance médicale, qui a pour objet de permettre à un professionnel médical d'interpréter à distance les données nécessaires au suivi médical d'un patient et, le cas échéant, de prendre des décisions relatives à la prise en charge de ce patient. L'enregistrement et la transmission des données peuvent être automatisés ou réalisés par le patient lui-même ou par un professionnel de santé ;

« 4º La téléassistance médicale, qui a pour objet de permettre à un professionnel médical d'assister à distance un autre professionnel de santé au cours de la réalisation d'un acte ;

« 5° La réponse médicale qui est apportée dans le cadre de la régulation médicale mentionnée à l'article L. 6311-2 et au troisième alinéa de l'article L. 6314-1.

« Section 2

« Conditions de mise en œuvre

« *Art. R. 6316-2.* – 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.

« 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 technologies de l'information et de la communication.

« *Art. R. 6316-3.* – Chaque acte de télémédecine est réalisé dans des conditions garantissant :

« 1° *a)* L'authentification des professionnels de santé intervenant dans l'acte ;

« *b)* L'identification du patient ;

« *c)* L'accès des professionnels de santé aux données médicales du patient nécessaires à la réalisation de l'acte ;

« 2° Lorsque la situation l'impose, la formation ou la préparation du patient à l'utilisation du dispositif de télémédecine.

« *Art. R. 6316-4.* – Sont inscrits dans le dossier du patient tenu par chaque professionnel médical intervenant dans l'acte de télémédecine et dans la fiche d'observation mentionnée à l'article R. 4127-45 :

« 1° Le compte rendu de la réalisation de l'acte ;

« 2° Les actes et les prescriptions médicamenteuses effectués dans le cadre de l'acte de télémédecine ;

« 3° L'identité des professionnels de santé participant à l'acte ;

« 4° La date et l'heure de l'acte ;

« 5° Le cas échéant, les incidents techniques survenus au cours de l'acte.

« *Art. R. 6316-5.* – Les actes de télémédecine sont pris en charge dans les conditions prévues aux articles L. 162-1-7, L. 162-14-1, L. 162-22-1, L. 162-22-6, L. 162-32-1 et L. 165-1 du code de la sécurité sociale.

« Section 3

« Organisation

« *Art. R. 6316-6.* – L'activité de télémédecine et son organisation font l'objet :

« 1° Soit d'un programme national défini par arrêté des ministres chargés de la santé, des personnes âgées, des personnes handicapées et de l'assurance maladie ;

« 2° Soit d'une inscription dans l'un des contrats pluriannuels d'objectifs et de moyens ou l'un des contrats ayant pour objet d'améliorer la qualité et la coordination des soins, tels qu'ils sont respectivement mentionnés aux articles L. 6114-1, L. 1435-3 et L. 1435-4 du code de la santé publique et aux articles L. 313-11 et L. 313-12 du code de l'action sociale et des familles ;

« 3° Soit d'un contrat particulier signé par le directeur général de l'agence régionale de santé et le professionnel de santé libéral ou, le cas échéant, tout organisme concourant à cette activité.

« Les contrats mentionnés aux 2° et 3° du présent article doivent respecter les prescriptions du programme relatif au développement de la télémédecine mentionné à l'article L. 1434-2 du code de la santé publique.

« *Art. R. 6316-7.* – Les programmes et les contrats mentionnés à l'article R. 6316-6 précisent les conditions dans lesquelles s'exerce l'activité de télémédecine, en tenant compte notamment des spécificités de l'offre de soins dans le territoire considéré.

« Ils précisent en particulier les modalités retenues afin de s'assurer que le professionnel médical participant à un acte de télémédecine respecte les conditions d'exercice fixées à l'article L. 4111-1 ou à l'article L. 4112-7 ou qu'il est titulaire d'une autorisation d'exercice délivrée par le ministre chargé de la santé et qu'il satisfait à l'obligation d'assurance prévue à l'article L. 1142-2.

« *Art. R. 6316-8.* – Les organismes et les professionnels de santé qui organisent une activité de télémédecine, à l'exception de la réponse médicale donnée dans le cadre de la régulation médicale, concluent entre eux une convention respectant les dispositions inscrites dans les contrats ou programmes mentionnés à l'article R. 6316-6. Cette convention organise leurs relations et les conditions dans lesquelles ils mettent en œuvre les exigences mentionnées dans le présent chapitre.

« *Art. R. 6316-9.* – 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 correspondants.

« *Art. R. 6316-10.* – 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.

« Le consentement exprès de la personne, prévu au premier alinéa de ce même article L. 1111-8, peut être exprimé par voie électronique.

« *Art. R. 6316-11.* – L'activité de télémédecine peut bénéficier des financements prévus aux articles L. 221-1-1 et L. 162-22-13 du code de la sécurité sociale ainsi que dans les conditions prévues aux articles L. 314-1 et L. 314-2 du code de l'action sociale et des familles. »

Art. 2. – Les organismes et les professionnels de santé mentionnés à l'article R. 6316-8 qui organisent ou exercent une activité de télémédecine disposent d'un délai de dix-huit mois à compter de la date de publication du présent décret pour se mettre en conformité avec ces dispositions.

Art. 3. – Le ministre du travail, de la solidarité et de la fonction publique, la ministre de la santé et des sports et le ministre du budget, des comptes publics et de la réforme de l'Etat sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 19 octobre 2010.

FRANÇOIS FILLON

Par le Premier ministre :

La ministre de la santé et des sports,
ROSELYNE BACHELOT-NARQUIN

Le ministre du travail, de la solidarité et de la fonction publique,
ERIC WOERTH

Le ministre du budget, des comptes publics et de la réforme de l'Etat,
FRANÇOIS BAROIN

Source: www.legifrance.fr

ANNEXES VII: EXTRAITS DE LA LOI INFORMATIQUE ET LIBERTÉS

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

Version consolidée au 9 juin 2014

L'Assemblée nationale et le Sénat ont adopté.
Le Président de la République promulgue la loi dont la teneur suit :

Chapitre Ier : Principes et définitions

Article 1

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 individuelles ou publiques.

Article 2
- Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

Constitue une donnée à caractère personnel 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Article 3
- Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004

I. - Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.

II. - Le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données. Toutefois, les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel ne constituent pas des destinataires.

Article 4
- Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004

Les dispositions de la présente loi ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

Article 5
- Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004

I. - Sont soumis à la présente loi les traitements de données à caractère personnel :

1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;
2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne.

II. - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.

Chapitre II : Conditions de licéité des traitements de données à caractère personnel

Section 1 : Dispositions générales

Article 6
- Modifié par Loi n°2004-801 du 6 août 2004 - art. 2 JORF 7 août 2004

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :
1° Les données sont collectées et traitées de manière loyale et licite ;
2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;
3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;
5° 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.

Article 7

· Modifié par Loi n°2004-801 du 6 août 2004 - art. 2 JORF 7 août 2004

Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :
1° Le respect d'une obligation légale incombant au responsable du traitement ;
2° La sauvegarde de la vie de la personne concernée ;
3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
4° L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
5° La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Section 2 : Dispositions propres à certaines catégories de données

Article 8

· Modifié par Loi n°2004-801 du 6 août 2004 - art. 2 JORF 7 août 2004

I.-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.

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

III.-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 traitements selon les modalités prévues à l'article 25. Les dispositions des chapitres IX et X ne sont pas applicables.

IV.-De même, ne sont pas soumis à l'interdiction 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.

Article 25

· Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004

I. - Sont mis en œuvre après autorisation de la Commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 et 27 :
1° Les traitements, automatisés ou non, mentionnés au 7° du II, au III et au IV de l'article 8 ;
2° Les 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 ;
3° Les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées ;
4° Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, 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 ;
5° Les 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 ;
6° 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 ;
7° Les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;
8° Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

II. - Pour l'application du présent article, les traitements qui

répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

III. - La Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

Source: www.legifrance.fr

ANNEXE VIII: CRÉATION DU DMP

Publié le *21-09-2012* (http://esante.gouv.fr)

La création d'un DMP en images

Image as link group

Show image as link:
Show as link

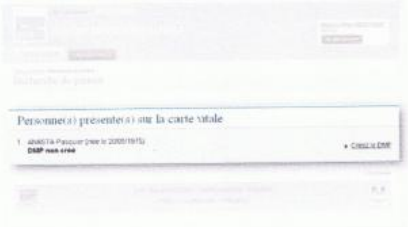
1. Lorsque vous arrivez dans l'établissement de santé, demandez l'ouverture de votre DMP au service des admissions ou rendez-vous dans l'espace spécialement prévu pour la création de DMP s'il en existe un.

2. La personne en charge des admissions vous reçoit et vous explique ce qu'est le DMP, ce que cela implique et vos droits quant à la consultation, le masquage et la destruction de vos données de santé personnelles qui seront stockées dedans. A cette occasion, elle vous remet une brochure qui récapitule toutes ces informations. Lisez là attentivement.

3. Le ou la chargée d'accueil va alors vous demander votre consentement oral à l'ouverture de votre DMP. Cette étape est dématérialisée : vous ne signez aucun papier. Tout est porté dans votre DMP, y compris le lieu de création et l'identité de la personne ou de la structure qui l'a créé. La chargée d'accueil peut apposer le tampon de l'établissement au dos de la brochure, attestant que vous avez été bien informé avant de créer votre DMP.

4. La chargée d'accueil va ensuite vous demander votre carte vitale et l'insérer dans son lecteur afin de créer votre DMP.

5. Elle vérifie alors que vous n'avez pas déjà un DMP :



6. Puis coche les actions que vous autorisez sur votre DMP :

(Le nom et les données personnelles sont factices)

7. C'est fait : votre DMP est créé ! La chargée d'accueil vous remet alors votre « document des secrets », qui atteste de cette création et liste les codes qui vous serons nécessaires pour consulter votre DMP à tout moment, de chez vous.

8. Les professionnels de santé pourront désormais consulter votre DMP et y ajouter des documents, avec votre autorisation. Pour leur signifier que vous avez un DMP, même en cas d'urgence, la chargée d'accueil appose sur votre Carte vitale un autocollant DMP :

Crédits photo : Jean Chiscano

Source URL: http://esante.gouv.fr/the-mag-issue-4/la-creation-d-un-dmp-en-images

ANNEXE IX: MODÈLE DE CONTRAT D'HÉBERGEMENT

2 Modèle de contrat

Ce formulaire correspond au recueil des informations exigées par les dispositions des articles *R. 1111-12 alinéa 5°* et *R. 1111-13* du décret n°2006-6 du 4 janvier 2006.

Référence du modèle de contrat :

Le modèle de contrat devant être joint à la demande d'agrément contient obligatoirement au moins les clauses suivantes telles quelles sont exigées par l'article *R. 1111-13*.
Pour chacune des clauses demandées, le candidat renverra à la référence précise du document décrivant la clause en indiquant la page et/ou le paragraphe ou article concerné.

Article	Énoncé de l'article	page et/ou paragraphe ou article concerné
[R. 1111-13 1°]	La description des prestations réalisées : contenu des services et résultats attendus :	
[R. 1111-13 2°]	Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels de santé et les établissements de santé les prenant en charge et désignés par eux peuvent être autorisés à accéder à ces données ou en demander la transmission et l'indication des conditions de mise à disposition de ces données :	
[R. 1111-13 3°]	Lorsque le contrat est souscrit par un professionnel de santé ou un établissement de santé, la description des modalités selon lesquelles les données hébergées sont mises à leur disposition, ainsi que les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et de transmission :	
[R. 1111-13 4°]	La description des moyens mis en œuvre par l'hébergeur pour la fourniture des services :	
[R. 1111-13 5°]	La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure :	
[R. 1111-13 6°]	Les obligations de l'hébergeur à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui :	
[R. 1111-13 7°]	Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement :	
[R. 1111-13 8°]	*Une information sur les garanties permettant de couvrir* toute défaillance éventuelle de l'hébergeur :	
[R. 1111-13 9°]	Une présentation des prestations à la fin de l'hébergement.	

Source: Asip santé. *Formulaire du référentiel de constitution des demandes de dossiers d'agrément*. Disponible sur: http://esante.gouv.fr/services/referentiels/securite/formulaires-du-referentiel-de-constitution-des-dossiers-de-demande-d-. Consulté le 9 juin 2014.

INDEX ALPHABETIQUE

Les chiffes renvoient aux numéros de page

TABLE DES MATIERES

L'encadrement juridique de la gestion électronique des données médicales

Résumé

La gestion électronique des données médicales consiste autant dans le simple traitement automatisé des données personnelles que dans le partage et l'échange de données relatives à la santé. Son encadrement juridique est assuré, à la fois, par les règles communes au traitement automatisé de toutes les données personnelles et par celles spécifiques au traitement des données médicales. Cette gestion, même si elle constitue une source d'économie, engendre des problèmes de protection de la vie privée auxquels le gouvernement français tente de faire face en créant l'un des meilleurs cadres juridiques au monde, en la matière. Mais, de grands chantiers comme celui du dossier médical personnel attendent toujours d'être réalisés et le droit de la santé se voit devancer et entraîner par les progrès technologiques. Le développement de la télésanté bouleverse les relations au sein du colloque singulier entre le soignant et le soigné. L'extension des droits des patients, le partage de responsabilité, l'augmentation du nombre d'intervenants, le secret médical partagé constituent de nouveaux enjeux avec lesquels il faut, désormais compter. Une autre question cruciale est celle posée par le manque d'harmonisation des législations augmentant les risques en cas de partage transfrontalier de données médicales.

Mots clefs: Données personnelles, données médicales, vie privée, traitement automatisé, dossier médical personnel, e-santé, télésanté, télémédecine, hébergeur, déclaration, agrément, consentement, secret médical, sécurité, confidentialité, interopérabilité, référentiels, masquage, responsabilité médicale.

Legal framework for the electronic management of medical data

Abstract

The electronic management of medical data is as much in the simple automated processing of personal data in the sharing and exchange of health data . Its legal framework is provided both by the common rules to the automated processing of all personal data and those specific to the processing of medical data . This management , even if it is a source of economy, creates protection issues of privacy which the French government tries to cope by creating one of the best legal framework in the world in this field. However , major projects such as the personal health record still waiting to be made and the right to health is seen ahead and lead by technological advances . The development of e-health disrupts relationships within one dialogue between the caregiver and the patient . The extension of the rights of patients , sharing responsibility , increasing the number of players , the shared medical confidentiality pose new challenges with which we must now count. Another crucial question is posed by the lack of harmonization of legislation increasing the risks in cross-border sharing of medical.

Keywords: Personal data, medical data, privacy, automated processing, personal health records, e-health, telehealth, telemedicine, hosting, reporting, approval, consent, confidentiality, security, interoperability, standards, masking, medical liability.

Unité de recherche/ Research unit: CERAPS, 1 place Déliot, 59000 Lille, ceraps(at)univ-lille2.fr, http://ceraps.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-lill2.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 .