UNIVERSITE DE LORRAINE

2018

FACULTE DE PHARMACIE

THESE

Présentée et soutenue publiquement

le 5 juin 2018, sur un sujet dédié à :

Le cadre juridique des données personnelles et le système de santé en France

pour obtenir

le Diplôme d'Etat de Docteur en Pharmacie

par Paul BOLOT

né le 27 septembre 1994

Membres du Jury

Président :	Madame Francine PAULUS, Maître de conférences
Juge :	Madame Alexandrine LAMBERT, Maître de conférences
	Madame Julie LEONHARD, Maître de conférences
	Monsieur René PAULUS, Pharmacien

UNIVERSITÉ DE LORRAINE
FACULTÉ DE PHARMACIE
Année universitaire 2017-2018

DOYEN
Francine PAULUS
Vice-Doyen/Directrice des études
Virginie PICHON
Conseil de la Pédagogie
Présidente, Brigitte LEININGER-MULLER
Vice-Présidente, Alexandrine LAMBERT
Collège d'Enseignement Pharmaceutique Hospitalier
Présidente, Béatrice DEMORE
Commission Prospective Facultaire
Président, Christophe GANTZER
Vice-Président, Jean-Louis MERLIN
Commission de la Recherche
Président, Raphaël DUVAL

Responsables de la filière Officine	Caroline PERRIN-SARRADO Julien GRAFOULET
Responsables de la filière Industrie	Isabelle LARTAUD, Jean-Bernard REGNOUF de VAINS
Responsables de la filière Hôpital	Béatrice DEMORE Marie SOCHA
Responsable Pharma Plus ENSIC	Jean-Bernard REGNOUF de VAINS
Responsable Pharma Plus ENSAIA	Raphaël DUVAL
Responsable Pharma Plus ENSGSI	Igor CLAROT
Responsable de la Communication	Marie-Paule SAUDER
Responsable de la Cellule de Formation Continue et individuelle	Béatrice FAIVRE
Responsable de la Commission d'agrément des maîtres de stage	François DUPUIS
Responsable ERASMUS	Mihayl VARBANOV

DOYENS HONORAIRES

Chantal FINANCE
Claude VIGNERON

PROFESSEURS EMERITES

Jeffrey ATKINSON
Jean-Claude BLOCK
Max HENRY
Alain MARSURA
Claude VIGNERON

PROFESSEURS HONORAIRES

Pierre DIXNEUF
Marie-Madeleine GALTEAU
Thérèse GIRARD
Michel JACQUE
Pierre LABRUDE
Vincent LOPPINET
Alain NICOLAS

MAITRES DE CONFERENCES HONORAIRES

Monique ALBERT
Mariette BEAUD
Gérald CATAU
Jean-Claude CHEVIN
Jocelyne COLLOMB
Bernard DANGIEN
Marie-Claude FUZELLIER

Janine SCHWARTZBROD
Louis SCHWARTZBROD

Françoise HINZELIN
Marie-Hélène LIVERTOUX
Bernard MIGNOT
Jean-Louis MONAL
Blandine MOREAU
Dominique NOTTER
Christine PERDICAKIS
Marie-France POCHON
Anne ROVEL
Gabriel TROCKLE
Maria WELLMAN-ROUSSEAU
Colette ZINUTTI

ASSISTANTS HONORAIRES

Marie-Catherine BERTHE
Annie PAVIS

ENSEIGNANTS	*Section CNU**	*Discipline d'enseignement*
PROFESSEURS DES UNIVERSITES - PRATICIENS HOSPITALIERS		
Danièle BENSOUSSAN-LEJZEROWICZ	*82*	*Thérapie cellulaire*
Jean-Louis MERLIN	*82*	*Biologie cellulaire*
Jean-Michel SIMON	*81*	*Economie de la santé, Législation pharmaceutique*
Nathalie THILLY	*81*	*Santé publique et Epidémiologie*
PROFESSEURS DES UNIVERSITES		
Christine CAPDEVILLE-ATKINSON	*86*	*Pharmacologie*
Igor CLAROT	*85*	*Chimie analytique*
Joël DUCOURNEAU	*85*	*Biophysique, Acoustique, Audioprothèse*
Raphaël DUVAL	*87*	*Microbiologie clinique*
Béatrice FAIVRE	*87*	*Hématologie, Biologie cellulaire*
Luc FERRARI	*86*	*Toxicologie*
Pascale FRIANT-MICHEL	*85*	*Mathématiques, Physique*
Christophe GANTZER	*87*	*Microbiologie*
Frédéric JORAND	*87*	*Eau, Santé, Environnement*
Isabelle LARTAUD	*86*	*Pharmacologie*
Dominique LAURAIN-MATTAR	*86*	*Pharmacognosie*
Brigitte LEININGER-MULLER	*87*	*Biochimie*
Pierre LEROY	*85*	*Chimie physique*
Philippe MAINCENT	*85*	*Pharmacie galénique*
Patrick MENU	*86*	*Physiologie*
Jean-Bernard REGNOUF de VAINS	*86*	*Chimie thérapeutique*
Bertrand RIHN	*87*	*Biochimie, Biologie moléculaire*
MAITRES DE CONFÉRENCES DES UNIVERSITÉS - PRATICIENS HOSPITALIERS		
Béatrice DEMORE	*81*	*Pharmacie clinique*
Alexandre HARLE	*82*	*Biologie cellulaire oncologique*
Julien PERRIN	*82*	*Hématologie biologique*
Loïc REPPEL	*82*	*Biothérapie*
Marie SOCHA	*81*	*Pharmacie clinique, thérapeutique et biotechnique*
MAITRES DE CONFÉRENCES		
Sandrine BANAS	*87*	*Parasitologie*
Xavier BELLANGER	*87*	*Parasitologie, Mycologie médicale*

Emmanuelle BENOIT	*86*	*Communication et Santé*
Isabelle BERTRAND	*87*	*Microbiologie*
Michel BOISBRUN	*86*	*Chimie thérapeutique*
François BONNEAUX	*86*	*Chimie thérapeutique*
Ariane BOUDIER	*85*	*Chimie Physique*
Cédric BOURA	*86*	*Physiologie*
Joël COULON	*87*	*Biochimie*
Sébastien DADE	*85*	*Bio-informatique*
Dominique DECOLIN	*85*	*Chimie analytique*
Roudayna DIAB	*85*	*Pharmacie galénique*
Natacha DREUMONT	*87*	*Biochimie générale, Biochimie clinique*
Florence DUMARCAY	*86*	*Chimie thérapeutique*
François DUPUIS	*86*	*Pharmacologie*
Reine EL OMAR	*86*	*Physiologie*
Adil FAIZ	*85*	*Biophysique, Acoustique*
Anthony GANDIN	*87*	*Mycologie, Botanique*
Caroline GAUCHER	*86*	*Chimie physique, Pharmacologie*
Stéphane GIBAUD	*86*	*Pharmacie clinique*
Thierry HUMBERT	*86*	*Chimie organique*
Olivier JOUBERT	*86*	*Toxicologie, Sécurité sanitaire*
Alexandrine LAMBERT	*85*	*Informatique, Biostatistiques*
Julie LEONHARD	*86/01*	*Droit en Santé*
Christophe MERLIN	*87*	*Microbiologie environnementale*
Maxime MOURER	*86*	*Chimie organique*
Coumba NDIAYE	*86*	*Epidémiologie et Santé publique*
Marianne PARENT	*85*	*Pharmacie galénique*
Francine PAULUS	*85*	*Informatique*
Caroline PERRIN-SARRADO	*86*	*Pharmacologie*
Virginie PICHON	*85*	*Biophysique*
Sophie PINEL	*85*	*Informatique en Santé (e-santé)*
Anne SAPIN-MINET	*85*	*Pharmacie galénique*
Marie-Paule SAUDER	*87*	*Mycologie, Botanique*
Guillaume SAUTREY	*85*	*Chimie analytique*
Rosella SPINA	*86*	*Pharmacognosie*
Sabrina TOUCHET	*86*	*Pharmacochimie*
Mihayl VARBANOV	*87*	*Immuno-Virologie*
Marie-Noëlle VAULTIER	*87*	*Mycologie, Botanique*
Emilie VELOT	*86*	*Physiologie-Physiopathologie humaines*
Mohamed ZAIOU	*87*	*Biochimie et Biologie moléculaire*

PROFESSEUR ASSOCIE

Julien GRAVOULET	*86*	*Pharmacie clinique*
Anne MAHEUT-BOSSER	*86*	*Sémiologie*

PROFESSEUR AGREGE

Christophe COCHAUD	*11*	*Anglais*

**Disciplines du Conseil National des Universités :*

80 : Personnels enseignants et hospitaliers de pharmacie en sciences physico-chimiques et ingénierie appliquée à la santé

81 : Personnels enseignants et hospitaliers de pharmacie en sciences du médicament et des autres produits de santé

82 : Personnels enseignants et hospitaliers de pharmacie en sciences biologiques, fondamentales et cliniques

85 ; Personnels enseignants-chercheurs de pharmacie en sciences physico-chimiques et ingénierie appliquée à la santé

86 : Personnels enseignants-chercheurs de pharmacie en sciences du médicament et des autres produits de santé

87 : Personnels enseignants-chercheurs de pharmacie en sciences biologiques, fondamentales et cliniques

11 : Professeur agrégé de lettres et sciences humaines en langues et littératures anglaises et anglo-saxonnes

SERMENT DES APOTHICAIRES

Je jure, en présence des maîtres de la Faculté, des conseillers de l'ordre des pharmaciens et de mes condisciples :

Ð' honorer ceux qui m'ont instruit dans les préceptes de mon art et de leur témoigner ma reconnaissance en restant fidèle à leur enseignement.

Ð'exercer, dans l'intérêt de la santé publique, ma profession avec conscience et de respecter non seulement la législation en vigueur, mais aussi les règles de l'honneur, de la probité et du désintéressement.

Ðe ne jamais oublier ma responsabilité et mes devoirs envers le malade et sa dignité humaine ; en aucun cas, je ne consentirai à utiliser mes connaissances et mon état pour corrompre les mœurs et favoriser des actes criminels.

Que les hommes m'accordent leur estime si je suis fidèle à mes promesses.

Que je sois couvert d'opprobre et méprisé de mes confrères si j'y manque.

« LA FACULTE N'ENTEND DONNER AUCUNE APPROBATION, NI IMPROBATION AUX OPINIONS EMISES DANS LES THESES, CES OPINIONS DOIVENT ETRE CONSIDEREES COMME PROPRES A LEUR AUTEUR ».

« L’ignorance mène à la peur, la peur mène à la haine et
la haine conduit à la violence. Voilà l’équation. »

Averroès

Remerciements

À Mmes Alexandrine Lambert et Julie Léonhard, pour leurs conseils, leur bienveillance et leur supervision dans la direction de cette thèse et pour participer à mon jury.

À Mme Francine Paulus pour me faire l'honneur de présider le jury de cette thèse.

À M. René Paulus pour accepter de prendre part au jury de cette thèse et d'ainsi contribuer à l'évaluation de ces travaux.

À l'ensemble des professeurs de la faculté de Pharmacie de Nancy, qui, par leurs enseignements, m'ont permis de devenir pharmacien.

À mes parents, mes sœurs, Valentine et Juliette, et toute ma famille, pour leur confiance et leur soutien constants.

À mes amis, de Nancy, de Finlande ou du New Jersey, pour leurs encouragements et leur camaraderie.

Sommaire

Liste des figures

Liste des tableaux

Liste des abréviations

AAI	Autorité Administrative Indépendante
ANSM	Autorité Nationale de Sécurité du Médicament et des produits de santé
ANSP	Agence Nationale de Santé Publique
ARS	Agence Régionale de Santé
ASIP Santé	Agence des Systèmes d'Informations Partagés de Santé
CEDH	Cour Européenne des Droits de l'Homme
CEPD	Contrôleur Européen de la Protection des Données
CIL	Correspondant Informatique et Libertés
CJUE	Cour de Justice de l'Union Européenne
CNIL	Commission Nationale de l'Informatique et des Libertés
CNOP	Conseil National de l'Ordre des Pharmaciens
CPS	Carte de Professionnel de Santé
C. santé publ.	Code de la santé publique
C. séc. soc.	Code de la sécurité sociale
DGOS	Direction Générale de l'Offre de Soins
DGS	Direction Générale de la Santé
DMP	Dossier Médical Partagé
DP	Dossier Pharmaceutique
DPO	*Data Protection Officer*
DSSIS	Délégation à la Stratégie des Systèmes d'Information de Santé
GDPR	*General Data Protection Regulation*
GIP	Groupement d'Intérêt Public
InVS	Institut national de Veille Sanitaire
NDP	Numéro Dossier Pharmaceutique
OCDE	Organisation de Coopération et de Développement Economiques
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PUI	Pharmacie à Usage Intérieur
RGPD	Règlement Général sur la Protection des Données

Introduction

Qui n'a jamais partagé ses données personnelles pour accéder à un service ? Nous l'avons tous déjà fait et nous le faisons de plus en plus. Adresse email, numéro de téléphone, nom, date de naissance, numéro de sécurité sociale, mais aussi adresse IP, INE[1], empreinte digitale sont autant d'exemples de données personnelles. En effet, une donnée personnelle est entendue, selon la CNIL[2], comme « *toute information relative à une personne physique susceptible d'être identifiée* » (1).

Avec l'essor des technologies de l'information et de la communication et un numérique désormais ubiquitaire, la protection des données personnelles est devenue une question impossible à ignorer. Au carrefour entre informatique, sécurité, économie et libertés, la protection des données personnelles est donc l'un des enjeux de nos sociétés contemporaines.

La révolution numérique et toutes ses évolutions technologiques démultiplient l'utilisation de nos données, avec la miniaturisation des outils, la diminution des coûts de stockage et des capacités d'analyses toujours plus grandes. Entre 1990 et 2015, le volume mondial de transfert de données a explosé, multiplié par 16 000. La valeur créée par les données personnelles pourrait ainsi atteindre près de 1 000 milliards d'euros en 2020 en Europe, soit 8% du PIB[3] de l'Union Européenne (2). Nos données personnelles sont ainsi de plus en plus nombreuses, de plus en plus précieuses, mais aussi de plus en plus nécessaires, conditionnant l'accès à de plus en plus de services. Cette expansion sans précédent de l'utilisation de nos données, portée par les avancées technologiques, s'est néanmoins réalisée dans un cadre légal, en perpétuelle construction et évolution depuis plus de quarante ans.

Les premières lois en matière de protection des données personnelles ont vu le jour dans les années 1970. À la suite du Land de Hesse en Allemagne, la Suède a ainsi été l'un des premiers États européens à se doter d'une réglementation en la matière, en 1973. Cinq ans plus tard la France s'équipe à son tour, avec la loi n° 78-17 du 6 janvier 1978, dite loi « Informatique et Libertés ». Ces premiers cadres légaux ont ensuite permis, quelques années plus tard, la rédaction de la Convention du 28 janvier 1981 du Conseil de l'Europe.

Initialement pensées pour répondre aux craintes d'un État totipotent, ces premières réponses législatives ont également permis de faire face à un phénomène alors naissant : la « marchandisation des données personnelles ». En effet, alors que les données personnelles étaient auparavant l'apanage des pouvoirs publics, la société de consommation y a vu son intérêt. Avec les données personnelles, le marketing devient ainsi plus personnalisé (3). Et c'est d'ailleurs grâce à ce statut de « marchandises » que l'Union Européenne a pu s'emparer du sujet dans les années 1990, avec l'adoption de la directive 95/46/CE, première volonté d'harmonisation des cadres légaux en matière de protection des données personnelles.

---

[1] INE : Identifiant National Etudiant
[2] CNIL : Commission National de l'Informatique et des Libertés
[3] PIB : Produit Intérieur Brut

Dans les années 2000, la France s'est dotée d'une nouvelle loi, la loi n° 2004-801 du 6 août 2004, transposant la directive européenne de 1995 et modifiant la loi de 1978. Enfin, en 2016, le Parlement Européen a adopté un nouveau règlement, le Règlement Général sur la Protection des Données personnelles, RGPD, ou *GDPR* pour *General Data Protection Regulation*, afin de répondre aux évolutions technologiques et sociétales. Depuis quarante ans, les Parlements, français et européen, légifèrent, pour réguler et protéger l'utilisation des données personnelles. La protection des données personnelles s'est construite comme le compromis entre le droit au respect de la vie privée et les « *intérêts légitimes des organisations publiques ou privées* » de traiter ces données (4).

Toutefois, au sein même des données personnelles, une catégorie particulière de données se distingue, par son caractère intime et les risques accrus qu'elle représente pour le respect de la vie privée : les données de santé. Récemment définies de façon explicite par le législateur[4], les données de santé sont particulièrement sensibles. Leur protection et utilisation relèvent donc tant de l'éthique que du droit, avec des lois différentes et complémentaires.

Dans un tel environnement juridique, légitimement et particulièrement dense, nous pouvons alors nous interroger quant à la protection des données personnelles au sein du système de santé en France. Le système de santé, du simple professionnel de santé aux plus compliqués établissements de santé, doit en effet collecter et traiter moult données personnelles, dont bon nombre de données de santé. Alors, quels sont les acteurs de la protection des données personnelles au sein du système de santé ? Quelle est la responsabilité des professionnels de santé ? Quels sont les droits des patients face au traitement de leurs données ? Autant de questions auxquelles nous allons tenter d'apporter des réponses. L'intérêt de cette problématique est donc sa complexité, puisque se mêlent des données différentes, encadrées par des systèmes juridiques pluriels et traités par des entités d'une grande variété.

Afin de répondre à cette question, nous nous attacherons tout d'abord à dépeindre le cadre légal de la protection des données personnelles. Comme nous le verrons, ce cadre juridique s'est construit au fil des ans, à toutes les échelles, internationale, européenne et nationale, la dernière pierre apportée à cet édifice législatif étant le récent Règlement Général sur la Protection des Données (RGPD). De ce cadre légal, découlent plusieurs grands principes fondamentaux de la protection des données personnelles et sur lesquels reposent trois piliers : la personne concernée, le responsable du traitement et l'autorité de contrôle.

Une fois cet environnement décrit, nous pourrons nous intéresser au cœur de notre sujet, à savoir la protection des données personnelles au sein du système de santé. Nous nous attarderons dans un premier temps au cadre particulier qui protège les données de santé. Nous nous intéresserons ensuite à la responsabilité du traitement de ces données, en termes de types de responsables et d'obligations à respecter. Puis nous détaillerons d'autres parties prenantes, avant d'aborder la question du partage de données de santé.

Enfin, nous terminerons nos travaux par une étude de cas, afin d'observer la mise en œuvre concrète et pratique des éléments théoriques décrits précédemment. Pour ce faire, nous

[4] cf. 2.1.1 Définition des données de santé

nous intéresserons au dossier Pharmaceutique. Après une présentation de cet outil visant à améliorer la coordination des soins et à lutter contre la iatrogénie, nous étudierons la mise en œuvre de ce dossier partagé, sous l'angle de la protection des données personnelles.

PARTIE 1. Cadre légal de la protection des données personnelles

La protection des données personnelles s'inscrit dans un environnement législatif récent et toujours en évolution, qui fournit un cadre juridique précis qui cherche en permanence à s'adapter aux nouvelles fonctionnalités et pratiques du numérique.

1.1 Des sources multiples et variées

Année après année, le cadre juridique de la protection des données personnelles s'est étoffé, enrichi, précisé, des années 1970 jusqu'aux années 2000. Mais récemment, un nouveau texte législatif est venu modifier et mettre à jour ce cadre, le Règlement Général sur la Protection des Données (RGPD).

1.1.1 Principaux textes

Depuis les années 1970, plusieurs lois ont vu le jour, avec cette même ambition de donner un cadre juridique à la protection des données personnelles. Mais avant de nous attacher à décrire quels en sont les principes clés, il convient de présenter les principaux textes en la matière. En effet, plusieurs textes existent, à différentes échelles, internationale, européenne et française, qui participent tous à définir ce cadre légal de la protection des données personnelles.

1.1.1.1 Textes internationaux

À l'échelle internationale, plusieurs textes existent, chacun émanant d'institutions internationales différentes. Cependant, tous les textes internationaux n'ont pas la même valeur juridique. En effet, tandis que certains textes ne bénéficient d'aucune valeur juridique et ne sont que des « recommandations internationales », d'autres sont juridiquement contraignants en s'inscrivent directement dans la hiérarchie des normes (à condition toutefois d'être ratifiés). S'agissant de la protection des données personnelles *stricto sensu*, un seul texte est considéré comme juridique contraignant : la convention 108 du Conseil de l'Europe. Les autres textes, dont notamment les recommandations de l'Organisation de Coopération et de Développement Economique (OCDE), ne sont que la traduction d'une volonté internationale d'harmonisation, sans être juridiquement opposables.

Par ailleurs, outre cette dichotomie en termes de valeur juridique, nous pouvons également noter des différences d'approches. Ainsi, tandis que le texte de l'OCDE vise essentiellement à offrir un « *niveau de protection commun* », afin de favoriser les échanges économiques mondiaux, le Conseil de l'Europe propose, quant à lui, un texte avec l'ambition de protéger les droits individuels, offrant un « *haut niveau de protection* » (4).

1.1.1.1.1 Textes internationaux non juridiquement contraignants

❖ **Recommandations de l'OCDE**

L'Organisation de Coopération et de Développement Economique, ou OCDE, est une institution internationale fondée en 1961 et qui rassemble aujourd'hui 35 pays. Sa mission est de « *promouvoir les politiques qui amélioreront le bien-être économique et social* » (5) et outre l'analyse de données, l'OCDE rédige également un certain nombre de recommandations et de lignes directrices.

Le 23 septembre 1980 fut ainsi adoptée la Recommandation du conseil concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (6), ainsi que les lignes directrices afférentes. Ce premier texte international définit les notions de « maître du fichier », « données de caractère personnel » et de « flux transfrontière de données de caractère personnel » et liste plusieurs principes clés, comme la limitation en matière de collecte, la qualité des données, les garanties de sécurité, la responsabilité. Enfin, ces lignes directrices invitent les États membres à « *adopter une législation nationale appropriée* », à « *favoriser et soutenir des systèmes d'auto-réglementation* », tout en permettant aux individus de « *disposer de moyens raisonnables pour exercer leurs droits* » (6).

❖ **Autres textes internationaux non juridiquement contraignants**

Outre l'OCDE, l'Organisation des Nations Unies a également produit un texte, non juridiquement contraignant, relatif aux données personnelles. En effet, la Résolution de l'Assemblée Générale des Nations Unies n°45/95, du 14 décembre 1990, aborde la question des « *fichiers de données personnelles informatisées du secteur public et privé et des organisations internationales* » (7).

1.1.1.1.2 Textes internationaux juridiquement contraignants

❖ **Convention 108 du Conseil de l'Europe**

Quelques mois après l'adoption des recommandations de l'OCDE, le Conseil de l'Europe présente sa Convention 108, autre texte international s'intéressant à la protection des données personnelles.

Le Conseil de l'Europe, est une institution supranationale, à ne pas confondre avec le Conseil Européen ou le Conseil de l'Union européenne. Fondé en 1949, le Conseil de

l'Europe comprend aujourd'hui 47 États membres, dont les 28 membres de l'Union européenne. En tant qu'organisation intergouvernementale, le Conseil de l'Europe s'intéresse à des sujets universels comme les droits de l'Homme, la démocratie et l'État de droit. Le Conseil de l'Europe veille ainsi à la protection des droits des enfants, à l'égalité entre les femmes et les hommes ou encore à la protection de la liberté d'expression.

Dès le début des années 1970, le Comité des Ministres du Conseil de l'Europe se pencha sur la question de la protection des données personnelles, à travers deux résolutions ((73) 22 et (74) 29), relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques, dans les secteurs privés et publics (8)(9). Mais c'est le 28 janvier 1981, que le Conseil de l'Europe ouvre à la signature sa Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (10), dite Convention 108. Ce texte est aujourd'hui ratifié par 51 États : les membres du Conseil de l'Europe mais aussi des États extérieurs, comme le Sénégal, la Tunisie ou encore l'Uruguay (Figure 1).

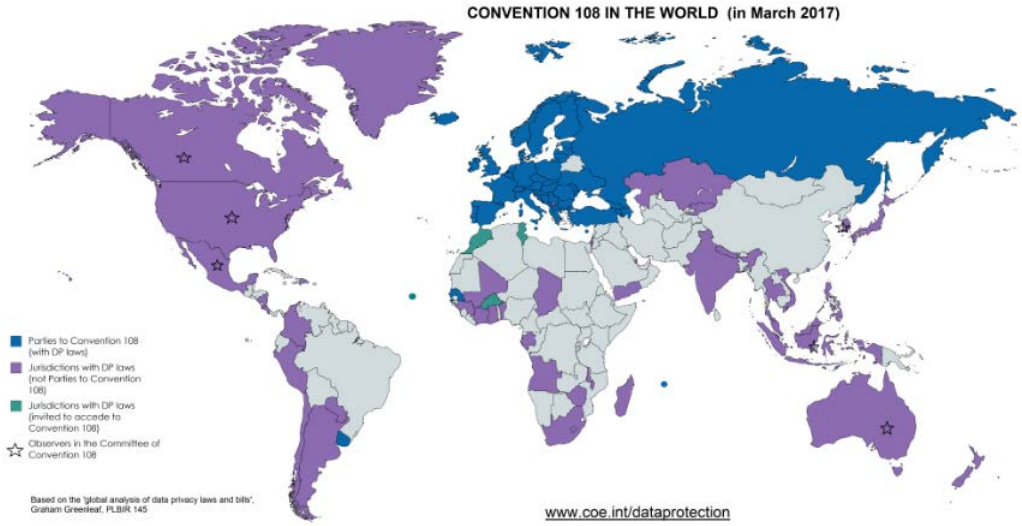


Figure 1. Carte des signataires de la Convention 108 du Conseil de l'Europe (11)

En France, la Convention 108 du Conseil de l'Europe est entrée en application en 1985, après son approbation par la loi du 10 octobre 1982 (12).

La Convention décrit tout d'abord les notions centrales de « données à caractère personnel », de « fichier automatisé », de « traitement automatisé » et de « maître du fichier ». Elle introduit également la notion de « catégories particulières de données » et reconnaît un certain nombre de droits que doit pouvoir exercer une personne concernée par le traitement de ses données personnelles (10). En somme, la Convention 108 du Conseil de l'Europe crée un socle légal commun à ses signataires, en définissant les données personnelles, en avançant des

principes clés (*e.g.* finalité, loyauté, proportionnalité, etc.) et en déclarant les droits que toute personne doit pouvoir exercer.

À ce jour, la Convention 108 du Conseil de l'Europe demeure le « *seul traité international contraignant* » en matière de protection des données personnelles. Par ailleurs, afin de répondre aux défis des nouvelles technologies apparues depuis sa création, la Convention est entrée dans un processus de modernisation. Initié en 2014, ce processus devrait notamment porter sur le principe de « *proportionnalité* », l'« *obligation de rendre des comptes* », le « *respect délibéré de la vie privée* », l'« *obligation de déclarer les violations de données* », la « *transparence du traitement des données* ». (13)

❖ **Autres textes internationaux juridiquement contraignants**

Sur un autre plan, la Convention de sauvegarde des droits de l'homme et libertés fondamentales, ou Convention européenne des droits de l'homme, joue également un rôle dans la définition du cadre légal de la protection des données personnelles. En effet, c'est en s'appuyant sur cette convention, et plus particulièrement son article 8 consacrée au « Droit au respect de la vie privée et familiale », que la Cour Européennes des Droits de l'Homme (CEDH) a rendu plusieurs arrêts en matière de protection des données personnelles (14). Cette jurisprudence a toute son importance puisqu'elle a, comme nous le verrons ultérieurement, participé à définir la notion de données de santé et les protections qui doivent s'appliquer à cette catégorie particulière de données personnelles[5].

Comme les premiers États dans les années 1970, les institutions internationales se sont, à leur tour, emparées du sujet de la protection des données personnelles. Néanmoins, ces tentatives d'harmonisation légale à l'échelle mondiale s'avèrent limitées. En effet, les recommandations de l'OCDE, en n'étant que de simples « recommandations, n'ont pas de valeur juridique. Quant à la Convention 108 du Conseil de l'Europe, s'il s'agit bien d'un texte contraignant, elle ne s'applique qu'à ses signataires, et une fois ratifiée.

1.1.1.2 Textes européens

Alors que les premiers États à légiférer sur la question des données personnelles étaient Européens, la machine communautaire a eu besoin de temps avant de délivrer son premier texte, avec la directive 95/46, en 1995. En effet, si aujourd'hui la légitimité de Bruxelles à intervenir sur ce sujet est pleinement acquise, la question de la compétence n'était pas évidente dans les années 1990. Heureusement, l'Union européenne joue désormais un rôle moteur dans l'évolution du cadre légal de la protection des données personnelles et a

[5] cf. 2.1.1 Définition des données de santé

récemment adopté un nouveau règlement, le règlement 2016/679, ou Règlement Général sur la Protection des Données, et sur lequel nous nous attarderons d'ailleurs dans une partie ultérieure[6].

1.1.1.2.1 Directive 95/46

À la suite de plusieurs lois nationales, dont celle de la France en 1978 (15), et d'un traité international, la Convention 108 du Conseil de l'Europe (10), l'Union européenne s'est emparée à son tour du sujet de la protection des données personnelles, au milieu des années 1990. De cette volonté politique résulte le premier cadre légal européen en la matière, à travers la directive 95/46 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 (16). Si l'Union européenne s'est considérée compétente et légiférer sur le sujet des données personnelles, c'est que ces dernières ont été considérées comme des marchandises et, qu'en vertu de l'article 100A du traité de Maastricht, les marchandises, comme les services et les capitaux, bénéficient d'une liberté de circulation (4).

Ainsi, dans ses premiers considérants, la directive déclare que, au nom du marché intérieur, les données à caractère personnel, doivent pouvoir « *circuler librement d'un État membre à l'autre* », mais aussi que « *les droits fondamentaux des personnes » doivent être « sauvegardés* » (16). Le considérant 8 ajoute que « *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 du traitement de ces données doit être équivalent dans tous les États membres* ». L'objet de cette directive est donc de fournir un cadre légal et harmonisé à la protection des données personnelles, afin de répondre à deux objectifs : d'une part assurer la libre circulation des données au nom du marché intérieur, et d'autre part garantir un niveau minimal de protection des personnes et de leurs droits.

Pour cela, la directive 95/46 définit tout d'abord plusieurs termes centraux : « données à caractère personnel », « traitement de données à caractère personnel », « fichier de données à caractère personnel », « responsable du traitement », « sous-traitement », « tiers », « destinataire », « consentement de la personne concernée ». La directive distingue également des catégories particulières de données, dans son article 8. En termes de champ d'application, la directive concerne « *le traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* » (16). Dans son article 6, la directive détaille les principes clés pour la qualité des données : loyauté, licéité, finalité, proportionnalités, etc. Elle décrit également le droit de la personne concernée par le traitement de ses données personnelles : droit d'information, droit d'accès et droit d'opposition. Enfin, la directive introduit un certain nombre d'obligation en matière de sécurité et de confidentialité des traitements et crée les autorités de contrôle, dont chaque État doit se doter.

---

[6] cf. 1.1.2 Règlement Général sur la Protection des Données

En somme, la directive 95/46 jette les bases d'un cadre légal européen de la protection des données personnelles afin d'harmoniser les différentes lois nationales déjà existantes sur le territoire de l'Union. Elle définit les termes centraux, dont celui de « données à caractère personnel », détaille les principes clés pour la qualité des données, précise des catégories particulières de données, instaure l'information de la personne concernée, ainsi que ses droits d'accès et d'opposition et crée les autorités nationales de contrôle. Quatorze ans après l'établissement des premiers principes internationaux à travers la Convention 108 du Conseil de l'Europe, l'Union européenne s'équipe donc, avec sa directive 95/46, d'un instrument juridique pour créer un environnement juridique harmonisé.

1.1.1.2.2 Charte des droits fondamentaux de l'Union européenne

La Charte des droits fondamentaux de l'Union européenne est un texte juridique contraignant pour les États membres (à l'exception du Royaume-Uni, de la Pologne et de la République tchèque, qui bénéficient d'une dérogation). Présentée en décembre 2000, mais finalement adoptée en décembre 2007, cette Charte vise à « *améliorer la protection des droits fondamentaux* », en étant une « *référence claire et forte, compréhensible* » (17). Ainsi, la Charte revient sur des droits déjà existants, mais inclut également de nouveaux droits, en matière de bioéthique et de protection des données personnelles par exemple.

Dans son chapitre II, consacré aux libertés, l'article 8 aborde précisément la question de la « *protection des données à caractère personnel* ». L'article déclare 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.* »

Ainsi, si la Charte des droits fondamentaux de l'Union européenne n'introduit ni changement ni nouveauté par rapport à la directive de 1995, elle inscrit la protection des données personnelles parmi les droits et libertés fondamentaux devant être garantis au sein de l'Union. La question de la protection des données personnelles devient ainsi un sujet aussi important que la liberté d'expression ou le droit à l'éducation.

Enfin, plus récemment, l'Union européenne a adopté un nouveau règlement en matière de protection des données personnelles, le règlement 2016/679, ou Règlement Général sur la Protection des Données (RGPD), abrogeant la directive 95/46 de 1995. Toutefois, ce nouveau texte induisant de nombreux changements et étant particulièrement d'actualité, puisqu'adopté

en 2016 et entrant en application en 2018, nous y consacrerons une partie spécifique ultérieurement[7].

1.1.1.3 Textes nationaux

Bien avant l'Union européenne, la France s'est équipée d'un cadre juridique en matière de protection des données personnelles. Ainsi, dès les années 1970, et à la suite des premières lois scandinaves, la France a adopté une première loi, la loi n°78-17, plus communément connue sous le nom de loi « Informatique et libertés ». Puis, dans les années 2000, une seconde loi est venue renforcer ce premier texte fondateur, tout en répondant à l'obligation de transposer en droit national la directive européenne de 1995.

Nous aborderons donc tour à tour ces deux grandes lois, n°78-17 (18) et n°2004-801 (19), qui définissent, encore aujourd'hui, le cadre légal de la protection des données personnelles en France.

1.1.1.3.1 Loi n°78-17, dite « Informatique et libertés »

Si les premières lois en matière de protection des données personnelles sont nées dans les années 1970 dans le nord de l'Europe, c'est essentiellement en réponse à une polémique nationale que la loi n°78-17 a été rédigée. En effet, en 1974, le journal *Le Monde* révèle au grand jour un projet confidentiel du Ministère de l'Intérieur : le projet SAFARI (4). Derrière cet acronyme exotique se cache la volonté du Gouvernement de créer un Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus (SAFARI), autrement dit un « mégafichier » permettant de connecter, grâce au numéro de sécurité sociale, les différents fichiers publics dont dispose l'État (3). C'est donc pour mieux contrôler les fichiers centraux, et ainsi répondre au risque de dérive vers un État *Big Brother*, que la loi de 1978 a été conçue.

Ainsi, l'article premier du texte inscrit dans la loi un « *objectif moral* » de l'informatique (4). Il est en effet déclaré que « *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* » (18). Et si ce paragraphe est critiqué par certains juristes pour sa formulation « *imprécise* », « *redondante* » et « *maladroite* », il affirme avec force la prépondérance de l'homme, de ses droits et de ses libertés sur l'outil informatique (4).

Les articles 4 et 5 introduisent quant à eux les premières définitions légales d'« *informations nominatives* » et de « *traitement automatisé d'informations nominat*ives ». Il est d'ailleurs intéressant de noter l'expression alors utilisée, d'« *informations nominatives* »,

[7] cf. 1.1.2 Règlement Général sur la Protection des Données

qui, pour plusieurs raisons[8], sera abandonnée quelques années plus tard, au profit d'une appellation plus appropriée : « données à caractère personnel ».

Quant au chapitre II de la loi, il crée et installe la Commission Nationale de l'Informatique et des Libertés (CNIL). Bien avant la directive 95/46 de l'Union européenne, la France s'équipe ainsi de cette Autorité Administrative Indépendante (AAI), en charge du contrôle de la protection des données personnelles. La loi dispose ainsi dans son article 6 que la CNIL doit « *veiller au respect des dispositions de la présent loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concernant avec elles et en contrôlant les application de l'informatique aux traitements des informations nominatives* » (18).

Premier texte en la matière, la loi n°78-17 du 6 janvier 1978 est aujourd'hui toujours en vigueur. Et bien que modifiée à plusieurs reprises, cette loi demeure un texte fondateur pour la protection des données personnelles en France.

1.1.1.3.2 Loi n°2004-801

Second texte clé sur le sujet de la protection des données personnelles en France, 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 (19) vient transposer en droit national la directive européenne n°95/46 (16) et modifie par conséquent la loi n°78-17, dite « Informatique et libertés » (18).

La loi définit tout d'abord plusieurs notions : « donnée à caractère personnel », « traitement automatisé de donnée à caractère personnel », « fichier de données à caractère personnel », « personne concernée », « responsable d'un traitement de données à caractère personnel », « destinataire d'un traitement de données à caractère personnel ». Rappelons d'ailleurs que le terme de « donnée à caractère personnelle » remplace l'appellation initiale d'« informations nominatives ». Le législateur énonce ensuite les grands principes énoncés dans la directive européenne : loyauté, licéité, finalité, proportionnalités, consentement, etc.

La loi revient également sur la Commission Nationale de l'Informatique et des Libertés (CNIL) et sur ses missions. Elle choisit ainsi de privilégier le contrôle *a posteriori* des fichiers par la Commission, tout en renforçant ses pouvoirs d'investigation. La loi confère aussi à la CNIL des pouvoirs de sanction administrative.

Enfin, la loi crée le rôle de « *correspondant à la protection des données à caractère personnel* », qui permet aux traitements pour lesquels le responsable a désigné un correspondant d'être « *dispensés des formalités* » de déclaration préalable. En effet, la plupart des traitements de données à caractère personnel sont désormais soumis à une déclaration auprès de la CNIL. Seules quelques catégories particulières de données doivent faire l'objet d'une autorisation *a priori*, par exemple les données biométriques ou génétiques.

---

[8] cf. 1.2.1.1.1 Données à caractère personnel

Avec la loi n°2004-801, la France répond donc à ses obligations, en transposant la directive européenne 95/46. Elle approfondit le cadre légal de la protection des données personnelles en disposant de nouvelles définitions et de nouveaux principes et renforce le rôle prépondérant de la Commission Nationale de l'Informatique et des Libertés (CNIL). Ce nouveau texte permet ainsi à la France de mieux répondre aux défis soulevés par des technologies toujours plus nombreuses et un monde numérique toujours plus ubiquitaire.

Le cadre juridique de la protection des données personnelles résulte donc de plusieurs années de lois et d'évolutions législatives, à toutes les échelles. Initiée dans les années 1970, cette volonté de régulation a conduit à la naissance d'un texte fondateur en France, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés ». Répondant initialement aux risques de constitution de « mégafichiers » aux mains de l'État, la loi sur la protection des données personnelles a dû aussi encadrer l'essor de la marchandisation des données. La menace change de camp est passe ainsi des pouvoirs publics aux entreprises privées.

En 1995, c'est au tour de l'Union européenne de légiférer. Compétente grâce au traité de Maastricht et en vertu de la libre circulation des marchandises, l'Union européenne adopte la directive 95/46, 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. Une directive européenne devant être transposée en droit national par les États, la France répond à son obligation et adopte 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.

Enfin, le récent règlement européen 2016/679 est venu compléter, mais aussi modifier le cadre juridique de la protection des données personnelles. Vingt ans après la directive 95/46, ce règlement attendu vient sans nul doute bouleverser les usages et les pratiques en vigueur.

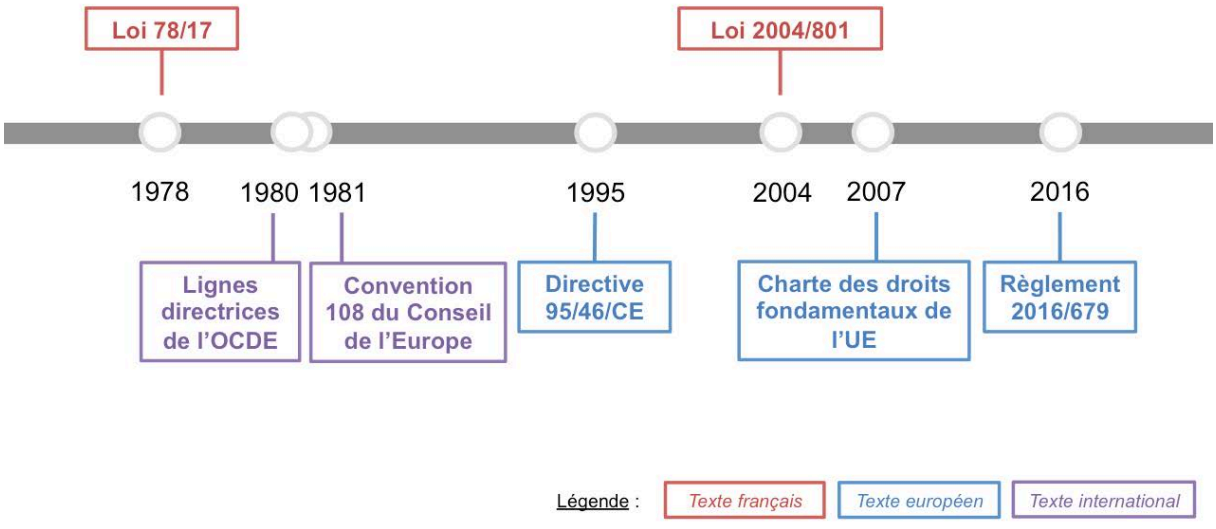


Figure 2. Chronologie des lois en matière de protection des données personnelles

Années après années, l'environnement juridique s'est donc étoffé, enrichi de définitions, de droits et de principes, formant ainsi un cadre juridique solide, mais qui doit toujours continuer à muer, au gré des évolutions technologiques et sociétales.

1.1.2 Règlement Général sur la Protection des Données

Dernier texte européen en la matière, le récent Règlement Général sur la Protection des Données (RGPD), également connu sous son appellation anglaise, *General Data Protection Regulation* (*GDPR*), cherche à la fois à moderniser, renforcer et harmoniser le cadre légal de la protection des données personnelles au sein de l'Union européenne. En outre, adopté en 2016, mais avec une entrée en application fixée à mai 2018, le Règlement Général sur la Protection des Données est un sujet plus que d'actualité !

1.1.2.1 Contexte

Avant de nous attacher à décrire les nouveautés introduites par le Règlement Général sur la Protection des Données, revenons tout d'abord sur son fondement, c'est-à-dire les différents éléments qui ont poussé l'Union européenne à de nouveau légiférer sur le sujet.

1.1.2.1.1 Fondement

Deux principaux arguments ont justifié l'adoption d'un nouveau texte européen relatif à la protection des données personnelles.

Premièrement, entre l'adoption de la première directive européenne en la matière, la directive 95/46, en 1995, et celle de ce nouveau règlement, en 2016, plus de vingt ans se sont écoulés. Ces deux décennies ont vu des avancées technologiques importantes, consacrant une place et un usage du numérique toujours plus importants dans notre société. La Commission européenne mettait ainsi en avant en 2012, lors de la présentation de son projet législatif, « *la rapidité des évolutions technologiques et la mondialisation* [qui] *modifient en profondeur la façon dont un volume sans cesse croissant de données à caractère personnel est collecté, consulté, utilisé et transféré* » (20). Réseaux sociaux, internet mobile, objets connectés sont ainsi autant de technologies aujourd'hui quotidiennes pour bon nombre de citoyens européens, mais qui étaient totalement inexistantes dans les années 1990. Une nouvelle loi européenne était alors nécessaire afin de mettre à jour le cadre juridique de la protection des données personnelles, de l'adapter à de nouveaux enjeux et de répondre à des questions qui ne se posaient pas en 1995.

Deuxièmement, une volonté d'homogénéisation était également à l'origine de ce règlement. Car si la directive 95/46 de 1995 a permis de définir un premier cadre légal

commun à l'échelle européenne, elle a également conduit à 28 transpositions différentes en droit national. En effet, l'Union européenne dispose de deux instruments pour légiférer : d'une part les directives, qui doivent être ensuite transposées à l'échelle de chaque pays en droit national, et les règlements, qui n'ont pas besoin d'être transposés et s'appliquent directement aux États. Avec un règlement, seules les interprétations du texte, par les tribunaux ou les autorités de contrôle peuvent varier au niveau national, conduisant à des disparités moins fortes entre les États, par rapport à une directive. Cette voie législative se révèle également plus rapide en ne nécessitant plus une loi de ratification et de transposition. Le choix du règlement pour cette nouvelle loi européenne marque donc une volonté claire d'harmonisation de la protection des données personnelles au sein de l'Union.

En somme, le Règlement Général sur la Protection des Données poursuit deux objectifs majeurs : la mise à jour du cadre légal européen en la matière (initialement basé sur la directive 95/46) et l'harmonisation des lois nationales pour une protection des données personnelles plus homogène au sein de l'Union européenne. (4)

1.1.2.1.2 Historique

Forte de ce constat et guidée par les deux objectifs évoqués plus haut, la Commission européenne a ouvert ce chantier législatif dès 2012, en partageant un projet de règlement. Dans sa communication d'alors, elle propose ainsi un nouveau « *cadre législatif solide et cohérent qui transcende les politiques de l'Union, renforce les droits des personnes physiques, consolide la dimension «marché unique» de la protection des données et réduit les charges administratives pesant sur les entreprises* ». (20)

Cette première version a été ensuite débattue, amendée puis adoptée par le Parlement européen en mars 2014. Ce fut ensuite au tour du Conseil de l'Union européenne de rendre sa copie, en juin 2015. Puis, en juillet, le Contrôleur Européen de la Protection des Données (CEPD), sorte de CNIL européenne, a remis ses recommandations sur le projet de règlement. Quelques mois plus tard, en décembre 2015, un texte consolidé, compromis entre la Commission, le Parlement et le Conseil, est rendu. Et finalement, le Parlement européen et le Conseil de l'Union européenne ont adopté formellement le règlement 2016/679, ou Règlement Général sur la Protection des Données, le 27 avril 2016. (21)(22)

Notons toutefois que, si le règlement 2016/679, ou Règlement Général sur la Protection des Données, concentre toute l'attention médiatique, ce texte appartient à un paquet législatif comprenant également une directive (Figure 3).

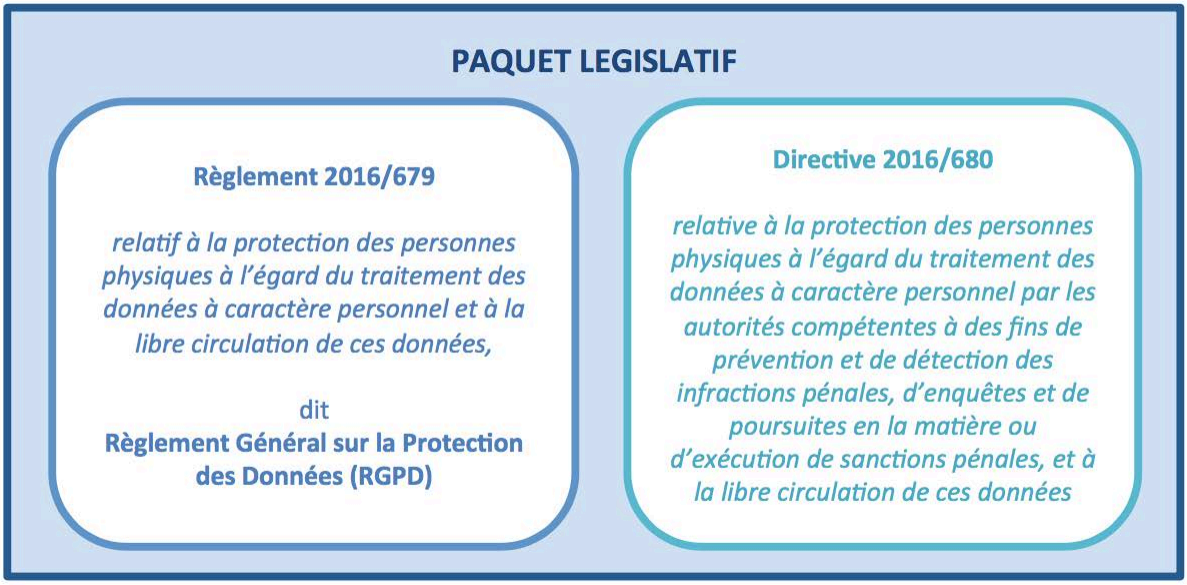


Figure 3. Paquet législatif regroupant le règlement 2016/679 et la directive 2016/680

Adoptée simultanément avec le RGPD, la directive 2016/680 se concentre davantage sur le traitement des données personnelles, par les autorités compétentes, à des fins répressives. Aussi, ce sujet s'éloignant de la problématique et du périmètre de notre travail, nous nous intéresserons ici exclusivement au Règlement Général sur la Protection des Données.

Ce chantier législatif, lancé par la Commission européenne en 2012, s'est conclu le 27 avril 2016 avec l'adoption de la directive 2016/680 et du règlement 2016/679, ce dernier abrogeant par ailleurs la directive précédente de 1995 (Figure 4).

1.1.2.2 Nouveautés introduites

Vingt ans après la directive 95/46 de 1995, le nouveau Règlement Général sur la Protection des Données vient donc répondre aux avancées technologiques, mais s'attache aussi à renforcer les droits des individus face au traitement de leurs données personnelles.

Dans le cadre de notre travail, et plus particulièrement de ce chapitre décrivant le cadre juridique de la protection des données personnelles, nous dresserons dans cette sous-partie une liste des principales nouveautés introduites par le règlement 2016/679. Cette présentation n'a pas l'ambition d'être exhaustive, mais vise à mettre en lumière les principaux changements apportés par ce règlement.

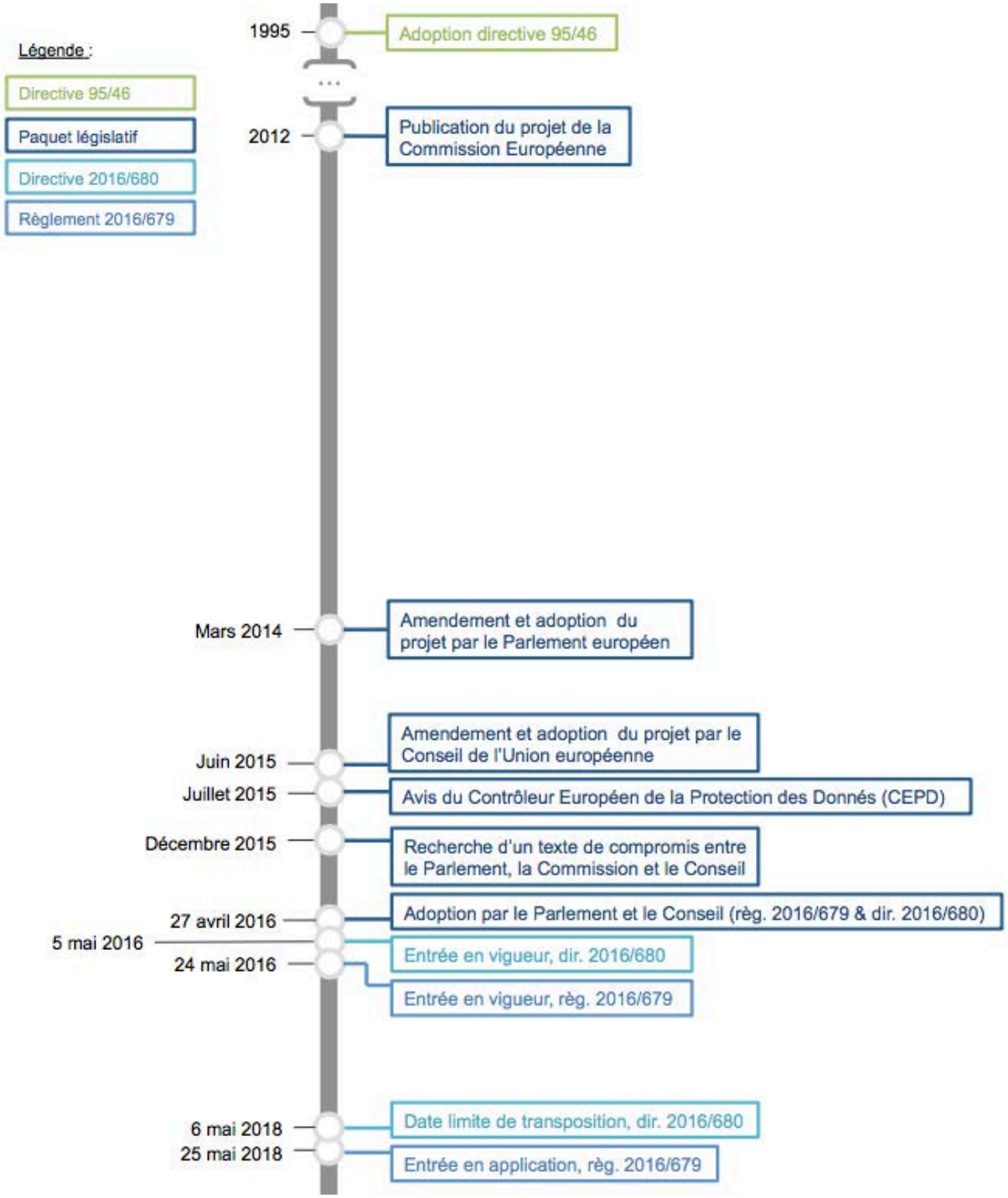


Figure 4. Historique de la préparation du RGPD

1.1.2.2.1 Nouvelles définitions

En termes de définitions, si le règlement ne modifie que très légèrement celles disposées par la directive 95/46, il en ajoute de nouvelles, dont certaines attendues depuis plusieurs années. Apparaissent ainsi à l'article 4 du règlement les définitions de :

- « limitation du traitement »,
- « profilage »,

- « pseudonymisation »,
- « violation de données à caractère personnel »,
- « données biométriques ».

Mais surtout, en matière de santé, ce sont deux nouvelles expressions qui sont définies par le règlement :

- les **données génétiques**, et
- les **données concernant la santé.**

Nous reviendrons sur les détails de cette dernière définition ultérieurement[9].

1.1.2.2.2 Nouveaux droits

Par ailleurs, le Règlement Général sur la Protection des Données renforce des droits déjà existants, tout en en créant de nouveaux. Le règlement introduit effectivement :

- le droit à l'effacement, aussi appelé « droit à l'oubli »,
- le droit à la limitation du traitement,
- le droit à la portabilité des données,
- le droit à réparation (en cas de dommage matériel ou moral lié à une violation du règlement).

1.1.2.2.3 Nouvelles responsabilités

Si les droits individuels se trouvent ainsi renforcés, les obligations pour le responsable du traitement sont également revues. Principale nouveauté, les formalités préalables, auparavant nécessaires à la mise en œuvre d'un traitement, conformément à la directive 95/46, sont abandonnées. Néanmoins, cet allègement administratif est permis en contrepartie d'une responsabilité renforcée. Ainsi, chaque responsable du traitement doit, en amont de la mise en œuvre de traitements présentant un risque élevé, réaliser une analyse d'impact. Il se doit dorénavant de tenir « *un registre des activités de traitement* ». Quant aux violations de données à caractère personnel, leur notification devient également obligatoire. Par ailleurs, le règlement s'inspire du « Correspondant Informatique et Libertés » (CIL) français, créé par la loi du 6 janvier 1978 modifiée, et instaure un « délégué à la protection des données », ou *DPO*, pour *Data Protection Officer*.

Le Règlement Général sur la Protection des Données, attendu depuis plusieurs années, répond à ses objectifs d'harmonisation et d'adaptation aux avancées technologiques, tout en accroissant les droits des individus. Ainsi, outre de nouveaux droits, le règlement définit des notions jusqu'à présent juridiquement floues, revoit les devoirs du responsable du traitement, encadre davantage les transferts de données en dehors de l'Union européenne et renforce les sanctions. Par conséquent, ce sont de nombreux changements qui attendent désormais les acteurs du traitement de données personnelles, mais aussi les États. Aussi, l'Union

[9] cf. 2.1.1 Définition des données de santé

européenne a-t-elle prévue une phase d'implémentation, afin de permettre à toutes les parties prenantes de se mettre en conformité avec ce nouveau cadre juridique.

1.1.2.3 Implémentation

Bien qu'adopté en avril 2016 par le Parlement européen, le Règlement Général sur la Protection des Données étant directement applicable à l'ensemble des États, un délai a ainsi été prévu avant son entrée en application. Avec une entrée en application du règlement fixée au 25 mai 2018, un délai de deux ans a ainsi été accordé aux différents acteurs du secteur, afin de permettre leur mise en conformité avec ce nouveau cadre. (21)

Tout d'abord, les États ont dû modifier leur droit interne, afin de l'adapter à ce nouveau cadre juridique européen. Aussi, en France, un projet de loi a été présenté en Conseil des ministres le 13 décembre 2017. Porté par la garde des Sceaux et ministre de la Justice, ce projet de loi vise à effectuer certaines adaptions de la loi n°78-17 du 6 janvier 1978 modifiée, afin de la mettre en conformité avec le nouveau règlement européen. Il tend également, dans son article 20, à autoriser le gouvernement à en réécrire certaines dispositions, par voie d'ordonnance. (23) Bénéficiant d'une procédure accélérée, engagée par le gouvernement, ce projet de loi a été étudié par chacune des deux chambres du parlement en première lecture et est, au 23 avril 2018, en nouvelle lecture au Sénat. (24)

Outre l'adaptation du cadre légal français, l'implémentation du Règlement Général sur la Protection des Données requiert également une prise en considération, et le cas échéant des changements idoines, de la part des organismes, publics comme privés, traitant des données personnelles.

La Commission Nationale de l'Informatique et des Libertés a donc publié un document destiné à faciliter l'implémentation de ces changements au sein des différents organismes concernés. En effet, ce nouveau règlement induit un changement de paradigme pour les responsables du traitement, en faisant disparaître les formalités préalables, au profit d'une responsabilité accrue des organismes. Ce document de la CNIL propose ainsi six étapes pour conduire l'implémentation de ce nouveau cadre légal en matière de protection des données personnelles :

1) « *Désigner un pilote* »,
2) « *Cartographier vos traitements de données personnelles* »,
3) « *Prioriser les actions* »,
4) « *Gérer les risques* »,
5) « *Organiser les processus internes* »,
6) « *Documenter la conformité* ». (25)

Depuis les années 1970, et jusqu'à 2016, le cadre juridique de la protection des données personnelles n'a donc cessé de se développer, tentant toujours de rattraper les évolutions technologiques et de protéger davantage les individus et leurs données.

1.1.3 Analyse du cadre légal

Comme nous l'avons vu précédemment, le cadre juridique de la protection des données personnelles est pluriel, avec des textes aux statuts et aux échelles différents. Cette pluralité s'explique par la nécessité des États à légiférer pour adapter leurs droits nationaux, mais aussi du besoin impérieux d'harmonisation internationale, face à un sujet qui, avec l'essor du numérique et la mondialisation, ne connaît parfois pas de frontières. Et c'est bien là le premier défi du cadre juridique des données personnelles : assurer son applicabilité et son application territoriales. Pour cela, le récent Règlement Général sur la Protection des Données se veut ambitieux, en s'appliquant à tout traitement de données dont l'activité est mise en œuvre sur le territoire de l'Union, mais aussi à tout traitement concernant des personnes se trouvant dans l'Union. Ce large champ d'application permet ainsi d'obtenir un texte pouvant atteindre les géants américains du numérique, au premier rang desquels se trouvent les célèbres GAFA[10]. Ces firmes, ont d'ailleurs acquis une telle hégémonie, par leur puissance économique et leur situation monopolistique, que les États dialoguent avec ces entreprises presque d'égal à égal. Le Danemark est, par exemple, devenu le premier pays au monde à nommer un ambassadeur numérique, auprès de ces sociétés (26). Aussi, face à ce nouveau paradigme et pour, une nouvelle fois, veiller à l'application de son règlement, l'Union européenne a prévu des amendes aux montants dissuasifs (« *jusqu'à 4% du chiffre d'affaires annuel mondial* » (22)). Ainsi, avec ses amendes revues à la hausse et son large champ d'application, le RGPD participe de rendre le cadre juridique des données personnelles applicables à tous, ce qui pouvait faire défaut aux textes précédents.

L'autre défi du cadre juridique de la protection des données personnelles est évidemment son risque inévitable d'obsolescence, au fur et à mesure des évolutions technologiques et sociétales. Le numérique se développe et devient de plus en plus ubiquitaire, nos usages des technologies évoluent et la loi arrive bien souvent après ces mutations. Cependant, la structure du cadre juridique des données personnelles permet de palier à ce risque d'obsolescence. En effet, ce cadre juridique repose sur quelques principes fondateurs[11], desquels découlent ensuite les autres dispositions légales. Ces principes, généraux par nature, sont ainsi suffisamment larges pour englober les usages et technologies passées, présentes, mais aussi futures. La loi française va même jusqu'à énoncer, à l'article 1 de la loi du 6 janvier 1978, dite « Informatique et libertés » : « *L'informatique doit être au*

[10] GAFA : Google, Apple, Facebook, Amazon.
[11] cf. 1.2.1.2 Principes

service de chaque citoyen. […] *Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* » (27). Cette réflexion presque philosophique en guise de préambule témoigne bien du caractère structuré et hiérarchisé du cadre juridique : un contexte, des principes fondateurs, puis des droits et des obligations. Toutefois, malgré cette robustesse structurelle, la problématique de la mise à jour régulière du cadre juridique des données personnelles demeure. Mais la réponse à ce travail perpétuel, tel le rocher de Sisyphe, pourrait se trouve dans d'autres formes de régulation, plus réactives et plus efficientes (*e.g.* la co-régulation, l'*accountability*, la *privacy by design*, etc. (12)).

Enfin, le cadre juridique de la protection des données personnelles repose aujourd'hui sur un triptyque composé des droits de la personnes concernée, des obligations du responsable du traitement et du contrôle d'une autorité. Le nouveau Règlement Général sur la Protection des Données vient par ailleurs consolider deux de ces piliers, en renforçant le droit des personnes et en responsabilisant encore davantage les acteurs du secteur. Néanmoins, ce cadre juridique pourrait se retrouver fragiliser par un déficit de notoriété. En effet, bien que le récent RGPD fasse la une des journaux spécialisés et soit sur toutes les lèvres parmi les experts en la matière, le grand public demeure, en majorité, ignorant de ses droits voire de ses devoirs. Du côté des responsables de traitement, si les grandes entreprises disposent des ressources nécessaires pour s'adapter et mettre en œuvre ce cadre juridique mis à jour, les entreprises de taille plus modeste doivent être davantage accompagnées. Quant aux personnes concernées, l'exercice de leurs droits implique la connaissance de ces droits. Or, la protection des données personnelles n'est pas encore devenu un sujet d'intérêt. En témoigne le *privacy paradox,* cette expression qui désigne la tendance à partager ses données personnelles, malgré la conscience du risque. En somme, l'enjeu est bien une prise de conscience collective de la problématique de la protection de nos données personnelles, qui est la clé pour un cadre juridique que chacun s'approprie.

Le cadre juridique de la protection des données personnelles est donc, au fil des années et des textes successifs, devenu un cadre robuste, car structuré autour de principes fondateurs. Le Règlement Général sur la Protection des Données, dernière pierre à cet édifice juridique, est venu, quant à lui, asseoir un large champ d'application, renforcer droits et devoirs et répondre à de nouveaux enjeux. Néanmoins, le risque d'obsolescence demeurant inhérent à toute loi touchant au numérique et aux nouvelles technologies, ce règlement n'échappera pas à une évaluation d'ici quelques années. Mais d'ici là, l'autre défi de ce cadre juridique est bien son appropriation par les citoyens, qu'ils soient responsables de traitement ou personnes concernées.

1.2 La protection des données personnelles : entre principes théoriques et mise en œuvre pratique

Tous ces textes successifs ont bâti le cadre légal de la protection des données personnelles. Ce cadre peut être présenté comme la combinaison de principes fondateurs avec trois piliers principaux.

1.2.1 Principes fondateurs

Au carrefour entre droits individuels et intérêts légitimes du traitement de données personnelles, les principes fondateurs en matière de protection des individus représentent le socle nécessaire à l'élaboration d'un cadre législatif juste et approprié.

1.2.1.1 Définitions

Quelles qu'elles soient, les différentes lois incluent toutes, dans leurs premiers articles, un certain nombre de définitions. En effet, le préalable à toute régulation est bien de définir l'objet que l'on souhaite réguler. Oscar Wilde a ainsi écrit « *Définir, c'est limiter* ». Concernant notre sujet, il convient donc définir plusieurs notions clés, au cœur de la protection des données personnelles.

1.2.1.1.1 Données à caractère personnel

Les données à caractère personnel, ou données personnelles, sont la substance même de notre sujet, cet objet que le législateur a souhaité protéger. Si l'appellation « données à caractère personnel » est désormais unanimement adoptée, elle a été précédée par une autre terminologie dans la loi française, celle d'« informations nominatives ».

En effet, la loi n°78-17 du 6 janvier 1978, dite loi « Informatique et libertés », parle d'« informations nominatives » et les définit comme étant « *les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* » (18). Cependant, à l'occasion de la loi n°2004-801 du 6 août 2004, transposant la directive européenne 95/46, le terme de « données à caractère personnel » est introduit. Les travaux parlementaires préparatoires à la loi de 2004 justifient ce changement de vocabulaire par trois raisons. Tout d'abord, cette nouvelle terminologie semble plus appropriée au regard de nouvelles « *mesures d'identification indirecte* » (28). Ensuite, ce revirement met fin à une confusion qui pouvait exister dans le droit français, puisque les lois n°78-17 du 6 janvier 1978 et n°78-753 du 17 juillet 1978 font toutes deux mention d'« informations nominatives », mais avec des définitions différentes. Enfin, il est avancé que l'épithète « *personnel* » offre une qualification plus large que « *nominatif* » et permettra de

mieux faire face aux évolutions technologiques et donc d'éviter une « *obsolescence rapide de la loi* » (28) (29).

Il est ainsi intéressant de voir comment chaque texte législatif successif a modifié la définition des « données à caractère personnel », en tentant d'y apporter toujours plus de précision (Tableau I).

Tableau I. Comparaison de la définition de "données à caractère personnel"

Convention 108	« *toute information concernant une personne physique identifiée ou identifiable* »
Directive 95/46/CE	« *toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* »
Règlement 2016/679	« *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* »
Loi 78-17	*"**informations nominatives**"*: « *informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale* »
Loi 2004-801	« *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.* »

Par ailleurs, si depuis 2004 l'expression de « données à caractère personnel » est disposée dans la loi française, la définition légale la plus récente provient du règlement européen 2016/679. Le règlement définit les données à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée entre une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » (22).

1.2.1.1.2 Traitement de données à caractère personnel

Une fois les données à caractère personnel définies, il convient de définir ce que le législateur entend par le traitement de données à caractère personnel. Et si la loi n°78-17 du 6 janvier 1978 (18), comme la Convention 108 du Conseil de l'Europe (10), emploie et définit le terme de « traitement automatisé », les textes plus récents (directive européenne 95/46, loi n°2004-801 du 6 août 2004 et règlement européen 2016/679) élargissent leur définitions à toute forme de traitement, automatisé ou non.

Ainsi, le règlement européen 2016/679 définit le « traitement de données à caractère personnel » comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* » (22). Cette formulation très large (« *toute opération* […] *appliquée à des données* »), ainsi que ce long inventaire d'actions possibles confèrent à cette définition force et amplitude. Le législateur semble avoir eu la volonté d'obtenir le champ d'application le plus large possible, en n'omettant aucune forme de traitement. Toute forme de traitement devrait ainsi tomber dans le champ de cette définition, soit en y étant expressément citée, soit en étant englobée dans la formulation initiale de « *toute opération* ».

1.2.1.1.3 Responsable du traitement

Autre notion centrale en matière de protection des données personnelles, celle du responsable du traitement. Absente de la loi n°78-17 du 6 janvier 1978, cette notion commence à apparaître avec la Convention 108 du Conseil de l'Europe, qui utilise la terminologie de « maître du fichier ». Néanmoins, c'est bien la directive européenne 95/46 qui introduit l'expression de « responsable du traitement », toujours employée aujourd'hui.

Le règlement européen 2016/679 définit le « responsable du traitement » comme « *la personne physique ou morale, l'autorité́ publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* » (22). Cette définition apporte en somme deux éléments : l'identification et le statut du responsable du traitement. En effet, en termes de statut, la définition précise que ce responsable peut être aussi bien une « *personne* » (« *physique ou morale* »), une « *autorité publique* », un simple « *service* » ou encore un « *organisme* ». S'agissant de l'identification, le responsable est ainsi défini que celui qui « *détermine les finalités et les moyens du traitement* ». La responsabilité du traitement diffère donc de la gestion pratique du traitement.

1.2.1.1.4 Données « sensibles »

Parmi les données personnelles, une catégorie particulière de données a été distinguée par le législateur. Communément dénommées « données sensibles », ces données se différencient des autres données personnelles, car il est, sauf exceptions prévues par la loi, interdit de les collecter ou les traiter. Il s'agit 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* » (30).

La loi dispose par ailleurs les exceptions à l'interdiction de collecte et de traitement :

- lorsque « *la personne concernée a donné son consentement exprès* »,
- lorsque « *les traitements* [sont] *nécessaires à la sauvegarde de la vie humaine* »,
- lorsque « *les traitements* [sont] *mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical* »,
- lorsque « *les traitements* [portent] *sur des données à caractère personnel rendues publiques par la personne concernée* »,
- lorsque « *les traitements* [sont] *nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice* »,
- lorsque « *les traitements* [sont] *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* […] »,
- lorsque « *les traitements statistiques* [sont] *réalisés par l'Institut national de la statistique et des études* »,
- lorsque « *les traitements* [sont] *nécessaires à la recherche, aux études et évaluations dans le domaine de la santé* […] ». (30)

1.2.1.1.5 Autres définitions

Outre les notions clés de « données à caractère personnel », de « traitement de données à caractère personnel » et de « responsable du traitement », les différents textes législatifs successifs ont également introduit et définit d'autres termes.

- **Fichier de données à caractère personnel**

Notion apparue dès les années 1980 avec la Convention 108 du Conseil de l'Europe, le « fichier de données à caractère personnel » est aujourd'hui défini par le règlement européen n°2016/679 comme « *tout ensemble structuré de données à caractère personnel accessibles*

selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique » (22).

❖ **Sous-traitant**

Le sous-traitement apparaît avec la directive européenne 95/46, mais c'est le terme de « sous-traitant » qui est repris dans le règlement européen 2016/679 et est défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* » (22).

❖ **Consentement de la personne concernée**

Comme nous le verrons ultérieurement, le recueil du consentement de la personne concernée est une obligation légale, lorsque ce dernier est la condition de la licéité du traitement. Ce consentement est défini comme suit par le règlement européen 2016/679 : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* » (22).

Cette définition est nécessaire, car le Règlement Général sur la Protection des Données entend bien renforcer le consentement des personnes concernées. En effet, comme le souligne à juste titre le considérant 40 du Règlement, la licéité d'un traitement repose soit sur le « *consentement de la personne concernée* », soit sur un autre « *fondement légitime prévu par la loi* » (22). Les conditions applicables au consentement sont par ailleurs détaillées à l'article 7 du règlement. En outre, cette définition modifie et ajoute quelques éléments par rapport à la définition précédente, disposée par la directive 95/46. L'adjectif « *éclairée* » vient ainsi remplacer l'épithète « *informée* » de la définition de 1995, mais surtout le qualificatif d'« *univoque* » est ajouté. De plus, la définition de 2016 insère de nouvelles précisions : la manifestation de volonté se fait « *par une déclaration ou par un acte positif clair* ». Ces menus changements textuels ont toutefois des conséquences non négligeables en pratique. Par cette nouvelle définition, le règlement met ainsi fin aux pratiques d'*opt-in* passif (*e.g.* case précochée) et d'*opt-out* (*i.e.* l'absence d'opposition vaut consentement, avec par exemple une case à cocher pour refuser un traitement).

❖ **Destinataire**

Également introduit par la directive européenne 95/46, la notion de « destinataire » est définie par le règlement européen 2016/679 comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers* » (22).

❖ **Tiers**

Outre la personne concernée, le responsable du traitement et le destinataire, le « tiers » est également défini dans la loi. Le règlement européen 2016/679 entend ainsi le « tiers »

comme « *une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel* » (22).

1.2.1.2 Principes

Outre un certain nombre de définitions, les différentes lois, successives et complémentaires, ont déterminé plusieurs principes clés en matière de protection des données personnelles. Ces principes sont les véritables fondements sur lesquels repose le cadre légal de la protection des données personnelles. Introduits notamment par la directive européenne 95/46, ils ont été repris et mis à jour à l'occasion du Règlement Général sur la Protection des Données. Le règlement fait ainsi mention de sept principes :

- principe de licéité, de loyauté et de transparence,
- principe de finalité,
- principe de minimisation des données,
- principe d'exactitude,
- principe de limitation de la conservation,
- principe d'intégrité et de confidentialité,
- principe de responsabilité.

1.2.1.2.1 Principe de licéité, de loyauté et de transparence

Premier principe disposé par le règlement 2016/679, l'article 5 commence en effet en déclarant que les données à caractère personnel doivent être « *traitées de manière licite, loyale et transparente au regard de la personne concernée* » (22). L'adjectif « *loyal* » est entendu comme « *sincère, franc, droit,* […] *qui observe les règles du jeu* », selon Gérard Cornu, professeur de droit reconnu, dans son ouvrage de référence *Vocabulaire juridique* (31)(4). Le qualificatif de « *loyal* » fait également écho, s'agissant de santé, au devoir du médecin de délivrer à son patient une information « *loyale, claire et appropriée* », conformément à l'article R. 4127-35 du Code de la santé publique (32). Quant à l'épithète « *licite* », toujours selon Gérard Cornu, son sens peut englober « *permis par un texte* », mais aussi « *conforme à l'ordre* public », voire « *aux bonnes mœurs* » (31)(4).

Les conditions de licéité d'un traitement sont par ailleurs énumérées à l'article 6 du règlement. Six cas de figure, dans lesquels un traitement est considéré comme licite, sont ainsi disposés :

- lorsque « *la personne concernée a consenti au traitement* »,
- lorsque « *le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie* »,
- lorsque « *le traitement est nécessaire au respect d'une obligation légale* »,
- lorsque « *le traitement est nécessaire à la sauvegarde des intérêts vitaux* » d'une personne physique,

- lorsque « *le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique* »,
- lorsque « *le traitement est nécessaire aux fins d'intérêts légitimes poursuivies par le responsable du traitement ou par un tiers* » (22).

Notons enfin que, par rapport à la directive 95/46 de 1995, le nouveau règlement ajoute la notion de transparence à ce premier principe. La transparence est effectivement l'une des ambitions du règlement, avec également la responsabilité renforcée des acteurs, car elle est la condition nécessaire tant pour le principe de loyauté que pour garantir un consentement des personnes concernées reposant sur une « *volonté* […] *éclairée* » (22).

1.2.1.2.2 Principe de finalité

Second principe clé énoncé par le règlement, le principe de finalité suppose que les données personnes doivent être collectées « *pour des finalités déterminées, explicites et légitimes* ». Il est ensuite ajouté que ces données ne peuvent être « *traitées ultérieurement d'une manière incompatible avec ces finalités* » (22). Seuls les traitements ultérieurs à des fins statistiques, de recherche ou d'archivage sont considérés comme compatibles avec les finalités initiales. Le principe de finalité est donc un principe central en matière de protection des personnelles, puisqu'il conditionne la collection ou le traitement de données à des finalités précises et justifiées.

1.2.1.2.3 Principe de minimisation des données

À la suite du principe de finalité, le principe de minimisation des données impose de ne collecter que les données nécessaires à la réalisation des finalités déterminées dans le cadre d'un traitement donné. Le règlement dispose et précise ainsi que les données personnelles doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » (22). Principes de finalité et de minimisation des données répondent donc tous deux au même objectif. Lorsqu'une personne accepte de partager ses données personnelles, elle s'expose potentiellement à un risque d'atteinte à sa vie privée, il convient alors de réduire ce risque autant que faire se peut.

1.2.1.2.4 Principe d'exactitude

Par ailleurs, si un individu accepte de partager ses données personnelles, il a le droit d'exiger que ses données soient correctes, il s'agit du principe dit d'exactitude. Ainsi, le règlement dispose que les données personnelles doivent être « *exactes et, si nécessaire, tenues à jour* » (22). Ce principe n'est donc pas sans faire écho au premier principe disposé par la loi, celui de loyauté, la personne concernée ayant droit à ce que ses données, collectées et traitées, soient « *exactes* ».

1.2.1.2.5 Principe de limitation de la conservation

Toujours afin de protéger les personnes concernées et de réduire le risque d'atteinte à leur vie privée, le règlement prévoit également le principe de limitation de la conservation. Il est ainsi mentionné que les données à caractère personnel doivent être « *conservées* […] *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* » (22). Seules des fins statistiques, de recherche ou d'archivage peuvent justifier une conservation plus longue.

Le principe de limite de durée de conservation repose donc sur le principe de finalité évoqué plus haut[12] et amène la justification du droit à l'effacement ou droit à l'oubli[13]. C'est ce même principe qui régit par exemple l'effacement des condamnations figurant au casier judiciaire après un certain délai. Les informations contenues dans un casier judiciaire sont effectivement conservées pour une durée limitée, disposée par le Code pénal, pour répondre à des finalités précises.

1.2.1.2.6 Principe d'intégrité et de confidentialité

De même, le principe d'intégrité et de confidentialité vise à garantir aux individus que leurs données personnelles, qu'ils ont consenti à partager, bénéficient d'une protection idoine. Nouveau principe introduit par le règlement, il est en effet disposé que les données personnelles doivent être « *traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées* » (22).

1.2.1.2.7 Principe de responsabilité

Enfin, dernier principe évoqué par le règlement, le principe de responsabilité place au cœur de la protection des données le responsable du traitement. Effectivement, l'article 5 du règlement se conclut par la phrase suivante : « *Le responsable du traitement est responsable du respect du paragraphe 1* [principes précédents] *et est en mesure de démontrer que celui-ci est respecté* » (22). Cette formulation est plus précise que celle de la directive 95/46, en ajoutant la notion de démonstration, et s'inscrit dans une volonté globale du règlement de renforcer le rôle des responsables de traitement et leur responsabilité.

En somme, ces grands principes jettent les fondations du cadre légal de la protection des données personnelles. En effet, si le traitement de données personnelles se justifie par des intérêts publics ou économiques, il expose les personnes concernées à un risque d'atteinte à

---

[12] cf. 1.2.1.2.2 Principe de finalité
[13] cf. 1.2.2.1.4 Droit à l'effacement

leur vie privée. Aussi ces principes visent-ils à protéger les individus contre ce risque. De ces principes clés découleront ensuite le reste de la loi, que l'on peut articuler autour de trois piliers.

1.2.2 Trois piliers

Sur la base des définitions et des principes énoncés précédemment, le cadre juridique de la protection des données personnelles peut ainsi être organisé autour de trois grands piliers : la personne concernée et ses droits, le responsable du traitement et ses obligations, l'autorité nationale et le contrôle qu'elle exerce.

1.2.2.1 Les droits de la personne concernée

Ainsi, outre les grands principes régissant la protection des données personnelles, le législateur a également introduit de nouveaux droits : droit d'accès, droit de rectification, droit d'opposition, droit au déréférencement, etc. Ces droits ont été introduits à l'échelle européenne par la directive 95/46, transposés en France par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2003-239 du 18 mars 2003 et par la loi n°2004-801 du 6 août 2004, puis récemment renforcés et complétés par le règlement 2016/679, ou Règlement Général sur la Protection des Données[14].

1.2.2.1.1 Droit d'accès

Premier droit de la personne concernée par le traitement de ses données personnelles, le droit d'accès. Le règlement 2016/679 décrit ce droit d'accès à l'article 15. Il dispose ainsi qu'une « *personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées* » (22). Le cas échéant, cette personne peut alors exiger l'accès à ses données personnelles et est en droit de demander certaines informations relatives au traitement, par exemple les finalités, les destinataires, la durée limite de conservation, etc.

1.2.2.1.2 Droit de rectification

Outre le droit d'accès, une personne concernée par le traitement de ses données à caractère personnel peut également demander à modifier ses données collectées, il s'agit du droit de rectification. Ce droit de rectification repose sur le principe d'exactitude, qui précise

[14] cf. 1.1.2 Règlement Général sur la Protection des Données

que les données doivent être « *exactes* » et « *tenues à jour* »[15]. L'article 16 du règlement 2016/679 déclare ainsi que « *la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes* » (22). La personne concernée peut également compléter les informations déjà collectées si ces dernières s'avèrent incomplètes.

1.2.2.1.3 Droit d'opposition

Par ailleurs, un droit d'opposition figure également dans la loi, qui permet à un individu de refuser le traitement de ses données à caractère personnel, dans le cadre défini par la loi. Ce droit d'opposition est prévu pour répondre aux situations où la licéité du traitement ne repose pas sur le consentement de la personne. En effet, dans cette situation, le retrait du consentement suffit à mettre fin au traitement, sans que cela ne relève d'une opposition.

S'agissant de ce droit d'opposition, le règlement 2016/679 dispose ainsi dans son article 21 qu'une « *personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant* » et dont la licéité du traitement repose sur les deux derniers cas de figure de l'article 6, *i.e.* lorsque le traitement est nécessaire « *à l'exécution d'une mission d'intérêt public* » ou « *aux fins des intérêts légitimes poursuivis par le responsable du traitement* ». De même, la personne concernée peut s'opposer à un traitement à « *fins de recherche scientifique ou historique* » ou à « *fins statistiques* », pour des « *raisons tenant à sa situation particulière* » et toujours sous réserve que ce traitement ne soit pas requis par une « *mission d'intérêt public* ». Enfin, elle peut également s'opposer au traitement de ses données personnelles lorsque ces dernières sont traitées « *à des fins de prospection* » (22).

Cependant, si le règlement précise clairement que ce droit est absolu en cas de prospection commerciale, le responsable du traitement peut refuser de répondre à ce droit d'opposition s'il « *démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice* » (22).

1.2.2.1.4 Droit à l'effacement

Le droit à l'effacement, aussi appelé droit à l'oubli, est l'une des nouveautés introduites par le règlement 2016/679. L'article 17 du règlement précise ainsi les situations dans lesquelles une personne peut demander au responsable du traitement l'effacement des données personnelles la concernant :

- lorsque « *les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées* »,

---

[15] cf. 1.2.1.2.4 Principe d'exactitude

- lorsque « *la personne concernée retire le consentement sur lequel est fondé le traitement* »,
- lorsque « *la personne concernée s'oppose au traitement* »,
- lorsque « *les données à caractère personnel ont fait l'objet d'un traitement illicite* », ou
- lorsque « *les données à caractère personnel doivent être effacées pour respecter une obligation légale* » (22).

Cependant, le règlement prévoit également des limites à ce droit à l'effacement. En effet, des situations peuvent exister où les droits entrent en concurrence, par exemple le droit à la liberté d'expression. Le droit à l'effacement ne s'applique donc pas si le traitement est requis pour :

- « *l'exercice du droit à la liberté d'expression et d'information* »,
- « *respecter une obligation légale* » ou « *exécuter une mission d'intérêt public* »,
- « *des motifs d'intérêt public dans le domaine de la santé publique* »,
- des fins « *archivistiques* », « *statistiques* » ou « de *recherche* »,« *la constatation, à l'exercice ou à la défense de droits en justice* » (22).

Enfin, ce droit à l'effacement, qui résulte d'une action positive d'un individu, ne doit pas être confondu avec la suppression automatique des données à l'issue d'une durée déterminée, en respect du principe de limitation de la durée de conservation[16].

1.2.2.1.5 Droit à la limitation du traitement

Le règlement 2016/679 prévoit aussi un droit à la limitation du traitement. Ainsi, en cas de limitation du traitement, les données personnelles concernées ne peuvent être traitées « *qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre* » (22). Ce droit à la limitation du traitement est détaillé à l'article 18 du règlement. Ainsi, ce droit ne peut être exercé par la personne concernée que dans certaines situations précises :

- en cas de contestation de l'exactitude des données, le temps que le responsable du traitement les vérifie,
- si le traitement est illicite et que la personne concernée invoque sont droit à la limitation plutôt que son droit à l'effacement,
- si le responsable du traitement n'a plus l'utilité des données mais « *celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice* »,

[16] cf. 1.2.1.2.5 Principe de limitation de la conservation

- en cas d'opposition au traitement, le temps que le responsable vérifie la légitimité des motifs avancés par la personne concernée.

En tout état de cause, le responsable du traitement se doit d'informer la personne concernée préalablement à la levée de la limitation du traitement.

1.2.2.1.6 Droit à la portabilité des données

Autre nouveauté introduite par le règlement 2016/679, le droit à la portabilité des données permet aux personnes concernées de « *recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et* […] *de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* » (22).

L'article 20 du règlement est consacré à ce droit à la portabilité des données et précise ainsi les situations dans lesquelles il peut être exercé, ainsi que ses limites. Par exemple, ce droit n'est pas applicable « *au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique* » ou s'il porte atteinte « *aux droits et libertés de tiers* » (22).

1.2.2.1.7 Droit à réparation

Le règlement 2016/679 prévoit enfin un droit à réparation. L'article 82 dispose ainsi que « *toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi* ». Cette disposition fait évidemment écho à l'article 1240 du Code civil, qui énonce que *« tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer* » (33), mais également à la notion juridique de responsabilité contractuelle. Et si ce droit à réparation peut ainsi apparaître comme redondant avec certaines articles du Code civil français, il a le mérite d'ôter toute ambiguïté potentielle. Mais surtout, n'oublions pas que ce règlement européen vise à harmoniser les différents cadres juridiques nationaux au sein de l'Union Européenne et si une certaine redondance peut voir le jour en France, ce n'est peut-être pas le cas dans d'autres pays européens.

1.2.2.1.8 Droit au déréférencement

Dernier droit en matière de protection des données personnelles, le droit au déréférencement est une forme d'application du droit d'opposition vis-à-vis des moteurs de recherches, *e.g.* Google®, Bing®, Yahoo®, etc. Il permet à un individu de demander à un

moteur de recherche de déréférencer des informations pouvant lui porter préjudice et liées à son nom. Ces informations, publiées sur des sites internet tiers, ne sont donc pas supprimées, mais elles n'apparaitront plus lors d'une recherche portant sur le nom de la personne concernée.

Le droit au déréférencement, s'il n'est pas explicitement disposé dans la loi, qu'elle soit européenne ou française, a ainsi été confirmé par l'arrêt du 13 mai 2014 de la Cour de justice de l'Union européenne (34). Cet arrêt, plus connu sous le nom d'arrêt *Google Spain*, est survenu après la saisie de la justice par un citoyen espagnol et réclamant de la part de l'américain Google®, le déréférencement de certains articles indexés à la recherche de son nom dans le moteur de recherche, au motif que ces articles pouvaient lui portait préjudice.

La jurisprudence européenne établit un droit au déréférencement, qui peut s'appliquer lorsque l'information référencée peut causer un « *préjudice* » à la personne concernée. Toutefois, ce droit ne saurait s'appliquer sur l'intérêt du public à avoir accès à l'information prévaut sur l'intérêt de la personne concernée à déréférencer cette information. Ainsi le droit au déréférencement n'est pas absolu, le moteur de recherche pouvant s'y opposer. Effectivement, le moteur de recherche doit apprécier la légitimité de chaque demande qu'il reçoit.

Droit d'accès, de rectification, d'opposition, d'effacement, de portabilité, de limitation du traitement, sont donc autant de nouveaux droits créés par le législateur, afin de garantir la protection des données à caractère personnel. Et bien que présentant certaines limites, détaillées à l'article 23 du règlement 2016/679, ils constituent sans aucun doute une progression des droits individuels.

1.2.2.2 Les devoirs du responsable du traitement

Le responsable du traitement, dont nous avons vu la définition précédemment[17], se trouve également au cœur de la protection des données personnelles, car c'est à lui qu'incombent les responsabilités et les obligations de garantir cette protection.

1.2.2.2.1 Obligations et responsabilités

Responsable du traitement et par conséquent des données personnelles qu'il est amené à traiter, le responsable se doit de répondre à un certain nombre d'obligations. Ces obligations découlent logiquement des principes de la protection des données personnelles instaurés par la loi[18]. Le règlement 2016/679 dispose ainsi dans son article 24 que « *le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour*

[17] cf. 1.2.1.1.3 Responsable du traitement
[18] cf. 1.2.1.2 Principes

s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement ». Dans cette partie, nous aborderons donc les principales obligations du responsable du traitement.

1.2.2.2.1.1 Devoir d'information

Tout d'abord, le responsable du traitement est tenu de fournir à la personne concernée certaines informations lorsque les données personnelles de cette personne sont collectées. Ces informations minimales à fournir sont listées à l'article 13 du règlement 2016/679, et comprennent, *inter alia* :

- « *l'identité et les coordonnées du responsable du traitement* »,
- « *les finalités du traitement* »,
- « *les destinataires ou les catégories de destinataires* »,
- « *la durée de conservation* ».

Ce devoir d'information en matière de données personnelles peut être mis en parallèle avec le droit du patient, en santé, à être informé « *sur son état de santé* » et sur les traitements et actes pouvant lui être proposés, conformément à l'article L. 1111-2 du Code de la santé publique (35).

L'article 14 du même règlement liste, quant à lui, les informations à fournir « *lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée* ». Par ailleurs, tout comme les droits de la personne concernée[19], cette obligation d'information est encadrée par certaines limites, prévues à l'article 23 du règlement.

1.2.2.2.1.2 Recueil du consentement

Lorsque le consentement est nécessaire à la mise en œuvre du traitement, le responsable du traitement doit par ailleurs pouvoir « *démontrer que la personne concernée a donné son consentement* », selon l'article 7 du règlement 2016/679. Il s'agit d'une autre obligation du responsable du traitement, que l'on peut supposer en lien avec le principe de « licéité, loyauté et transparence »[20].

1.2.2.2.1.3 Sécurité

Dans la droite ligne du principe « d'intégrité et de confidentialité »[21], le responsable du traitement est également tenu de mettre en œuvre « *les mesures techniques et*

---

[19] cf. 1.2.2.1 Les droits de la personne concernée
[20] cf. 1.2.1.2.1 Principe de licéité, de loyauté et de transparence
[21] cf. 1.2.1.2.6 Principe d'intégrité et de confidentialité

organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (22). Cette obligation de sécurisation, et nonobstant son importance, n'est donc pas une obligation de résultats, mais bien une obligation de moyens. Alors que l'obligation de résultats impose d'atteindre le ou les objectifs visés, l'obligation de moyens exige « seulement » de déployer les moyens nécessaires pour atteindre ces objectifs. Cette approche par obligation de moyen s'agissant de la sécurité est donc pragmatique, car le risque zéro n'existe pas.

1.2.2.2.1.4 Notification des violations de données

En cas de violation des données à caractère personnel sous sa responsabilité, le responsable du traitement doit notifier, « *dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance* », l'autorité de contrôle, si cette violation est « *susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* », conformément à l'article 33 du règlement 2016/679. En outre, l'article suivant ajoute que le responsable du traitement doit également informer la personne concernée, toujours dans les meilleurs délais, si cette violation est « *susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique* ».

Ce mécanisme de notification découle de la volonté du règlement de développer la responsabilité des acteurs du secteur et s'inscrit également dans un effort accru de transparence.

1.2.2.2.1.5 Analyse d'impact

Comme nous l'avons vu précédemment, le Règlement Général sur la Protection des Données opère un changement de paradigme, en remplaçant les formalités préalables par davantage de responsabilités des organismes traitant des données. Aussi, les anciennes déclarations et autorisations sont abandonnées au profit de nouveaux instruments, comme l'analyse d'impact. L'analyse d'impact doit être mise en œuvre par le responsable du traitement lorsqu'un traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* », selon l'article 35 (22). Si cette analyse d'impact conclut à un risque élevé, le responsable du traitement doit alors consulter l'autorité de contrôle, préalablement à la mise en œuvre de ce traitement.

1.2.2.2.1.6 Registre des activités de traitement

Autre nouveauté du règlement 2016/679, visant elle aussi à renforcer la responsabilité des acteurs du secteur, le registre des activités de traitement est décrit à l'article 30 du règlement. Chaque responsable du traitement doit ainsi tenir un registre des activités de traitement effectuées, comprenant, *inter alia*, les informations suivantes :

- « *nom et les coordonnées du responsable du traitement* »,
- « *finalités du traitement* »,

- « *description des catégories de personnes concernées et des catégories de données à caractère personnel* »,
- « *catégories de destinataires* »,
- « *délais prévus pour l'effacement des différentes catégories de données* »,
- « *description générale des mesures de sécurité techniques et organisationnelles* » (22).

1.2.2.2.2 Délégué à la protection des données

Le Règlement Général sur la Protection des Données, introduit également la fonction de délégué à la protection des données, ou DPO, pour *Data Protection Officer* en anglais. Nommé par le responsable du traitement, la désignation d'un délégué à la protection des données est requise lorsque :

- « *le traitement est effectué par une autorité publique ou un organisme public* »,
- « *les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui* […] *exigent un suivi régulier et systématique à grande échelle des personnes concernées* »
- « *les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données* [données sensibles] » (22).

L'article 39 du règlement détaille les missions du délégué à la protection des données :

- « *informer et conseiller* […] *sur les obligations* […] *en matière de protection des données* »,
- « *contrôler le respect du présent règlement* »,
- « *dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact* »,
- « *coopérer avec l'autorité de contrôle* »,
- « *faire office de point de contact pour l'autorité de contrôle* » (22).

Si le délégué à la protection des données est bien une nouveauté du règlement 2016/679, la France s'était déjà dotée d'une fonction similaire, avec la Correspondant Informatique et Libertés, ou CIL. Effectivement, le Correspondant Informatique et Libertés a été instauré par la loi n°2004-801 du 6 août 2004 et modifiant la loi n°78-17 du 6 janvier 1978. Selon l'article 22 de la loi n°78-17 modifiée, le Correspondant Informatique et Libertés est désigné par le responsable du traitement et est « *chargé d'assurer, d'une manière indépendante, le respect des obligations* » (30). Toutefois, si Correspondant Informatique et Libertés (CIL) et Délégué à la Protection des Données sont des fonctions analogues, des différences existent, notamment en matière de qualifications et de caractère obligatoire (dans certaines situations) (36).

1.2.2.3 Le contrôle d'une autorité

Instaurées dans le droit européen avec la directive 95/46 de 1995, les autorités de contrôle nationales ont vu leur pouvoir renforcé avec le nouveau règlement, 2016/679. En France, cette autorité de contrôle correspond à notre Commission Nationale de l'Informatique et des Libertés (CNIL).

1.2.2.3.1 Commission Nationale de l'Informatique et des Libertés

1.2.2.3.1.1 Statut et composition

Créée par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la Commission Nationale de l'Informatique et des Libertés, ou CNIL, s'est aujourd'hui imposée comme le « gendarme de la vie privée ».

Depuis sa naissance à la fin des années 1970, la Commission Nationale de l'Informatique et des Libertés existe sous le statut d'Autorité Administrative Indépendante. Une Autorité Administrative Indépendante (AAI) est une **«** *institution de l'État chargée, en son nom, d'assurer la régulation de secteurs considérés comme essentiels et pour lesquels le Gouvernement veut éviter d'intervenir trop directement* ». Exceptions au sein de l'administration française, les Autorités Administratives Indépendantes ne répondent à aucun ministère et le pouvoir exécutif ne peut leur adresser d'ordre ou de consigne. C'est d'ailleurs la Commission Nationale de l'Informatique et des Libertés qui fut la première Autorité Administrative Indépendante établie, cette expression apparaissant pour la première dans la loi n°78-17 du 6 janvier 1978. Aujourd'hui, de nombreuses Autorités Administratives Indépendantes existent, comme le Conseil Supérieur de l'Audiovisuel (CSA), le Défenseur des Droits ou encore la Haute Autorité de Santé (HAS) (37).

En termes de composition, la Commission Nationale de l'Informatique et des Libertés comprends 18 membres, à savoir :

- 6 représentants des hautes juridictions (2 membres ou anciens membres du Conseil d'État, de la Cour de cassation et de la Cour des comptes),
- 5 personnalités qualifiées,
- 4 parlementaires (2 députés et 2 sénateurs),
- 2 membres du Conseil économique, social et environnemental,
- 1 membre de la Commission d'accès aux documents administratifs (38)(30).

1.2.2.3.1.2 Missions et activités

Initialement chargée de « *veiller au respect des dispositions de la présente loi* [loi n°78-17 du 6 janvier 1978], *notamment en informant toutes les personnes concernées de leurs*

droits et obligations, en se concernant avec elles et en contrôlant les applications de l'informatique aux traitements des informations nominatives » (18), la Commission Nationale de l'Informatique et des Libertés a vu son rôle et ses missions évoluer au cours du temps, notamment avec la transposition en 2004 de la directive européenne 95/46.

Aujourd'hui, l'article 11 de loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par la loi n°2017-55 du 20 janvier 2017, dispose les deux missions conférées à la Commission Nationale de l'Informatique et des Libertés :

« *1° Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations ;*

2° Elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente loi. » (30)

De ces deux missions fixées par la loi découlent quatre actions principales pour la CNIL et décrites sur son site internet :

- « *Informer / protéger* »,
- « *Accompagner / conseiller* »,
- « *Contrôler et sanctionner* »,
- « *Anticiper* » (39).

Enfin, la Commission Nationale de l'Informatique et des Libertés dispose d'un pouvoir consultatif, pour conseiller le gouvernement, et d'un pouvoir réglementaire. La Commission est effectivement habilitée à établir et publier des « *normes* » et des « *règlements types en vue d'assurer la sécurité des systèmes* » (30). La CNIL peut également rendre des avis de conformité et délivrer des labels.

1.2.2.3.2 Sanctions

Si la loi encadre la protection des données personnelles par un certain nombre de droits et d'obligation, elle prévoit également des sanctions en cas de manquement. Ces sanctions peuvent être de deux ordres : pénales ou administratives.

1.2.2.3.2.1 Sanctions pénales

Les sanctions pénales liées au non-respect de la loi n°78-17 du 6 janvier 1978 sont décrites dans le livre II du Code pénal (chapitre VI « Des atteintes à la personnalité », section 5 « Des atteintes aux droits de la personne résultat des fichiers ou des traitements informatiques) (12). Le Code pénal prévoit ainsi les incriminations et sanctions suivantes (Tableau II).

Tableau II. Incriminations et sanctions pénales en matière de protection des données personnelles (non exhaustif), adapté de D. Forest, *Droit des données personnelles* (12)

Incriminations	Sanctions
Non-respect, y compris par négligence, des formalités préalables.	5 ans d'emprisonnement et 300 000 € d'amende (art. 226-16 du Code pénal)
Non-respect d'une norme simplifiée édictée par la CNIL.	*Idem* (art. 226-16-1-A du Code pénal)
Utilisation non autorisée du numéro d'inscription des personnes au RNIPP.	*Idem* (art. 226-16-1 du Code pénal)
Non-respect de l'obligation de sécurité.	*Idem* (art. 226-17 du Code pénal)
Collecte frauduleuse, déloyale ou illicite de données.	*Idem* (art. 226-18 du Code pénal)
Non-respect du droit d'opposition, notamment en cas de prospection commerciale, fondé sur des motifs légitimes.	*Idem* (art. 226-18-1 du Code pénal)
Traitement de données sensibles sans accord exprès de l'intéressé.	*Idem* (art. 226-19 du Code pénal)
Traitement de données personnelles concernant des infractions, condamnations ou mesures de sûreté hors les cas prévus par la loi.	*Idem* (art. 226-19 du Code pénal)
Traitement de données à des fins de recherche dans le demain de la santé sans information préalable ou malgré l'opposition de la personne.	*Idem* (art. 226-19-1 du Code pénal)
Non-respect de la durée de conservation des données.	*Idem* (art. 226-20 du Code pénal)
Divulgation de données en violation des droits de l'intéressé ayant pour effet de porter atteinte à sa considération ou à l'intimité de sa vie privée.	5 ans d'emprisonnement et 300 000 € d'amende 3 ans d'emprisonnement et 100 000 € d'amende si la divulgation a eu lieu par imprudence ou négligence (art. 226-22 du Code pénal)
Transfert de données vers un État n'offrant pas un niveau de protection suffisant.	5 ans d'emprisonnement et 300 000 € d'amende (art. 226-22-1 du Code pénal)

Par ailleurs, le Code pénal prévoit également des peines complémentaires pour les personnes morales incriminées (*e.g.* placement sous surveillance judiciaire, fermeture définitive, exclusion des marchés publics, etc.).

1.2.2.3.2.2 Sanctions administratives

La loi 2004-801 du 6 août 2004, qui transposait en droit français la directive européenne 95/46, a également étendu les pouvoirs de la Commission Nationale de l'Informatique et des Libertés. Aujourd'hui, la CNIL dispose d'un pouvoir de sanction administrative. Ce pouvoir est décrit dans le chapitre VII de la loi n°78-17 du 6 janvier 1978 modifiée. Ce pouvoir est exercé par une « *formation restreinte* » de la Commission, et composée par le président, les vice-présidents de la Commission, ainsi que trois membres élus par cette dernière en son sein.

Ainsi, la président de la CNIL peut « *mettre en demeure* [le responsable du traitement] *de faire cesser le manquement constaté* ». Si le responsable ne se conforme pas à cette mise en demeure, la formation restreinte de la CNIL peut alors « *prononcer, après une procédure contradictoire, les sanctions suivantes* » :

- « *un avertissement* »,
- « *une sanction pécuniaire* »,
- « *une injonction de cesser le traitement* » .(30)

Par ailleurs, en cas de « *violation des droits et libertés* », une « *procédure d'urgence* » (30) peut être enclenchée et permettre à la formation restreinte de la CNIL de décider :

- « *l'interruption de mettre en œuvre le traitement,*
- *l'avertissement,*
- *le verrouillage des données pour trois mois.* » (40)

Concernant les sanctions pécuniaires, ou amendes administratives selon l'expression choisie par le règlement 2016/679, ce dernier précise qu'elles doivent être « *effectives, proportionnées et dissuasives* » (22). Le montant maximal de ces amendes a été revu à la hausse par ce même règlement. Auparavant limitée à trois millions d'euros, (30), les amendes administratives peuvent désormais aller jusque dix ou vingt millions d'euros, ou 2 ou 4 % du chiffre d'affaires annuel mondial pour une entreprise, selon le type d'infractions, conformément à l'article 83 du règlement 2016/679 (22).

Dans la pratique, les principaux manquements relevés par la CNIL sont « *les sollicitations commerciales abusives, la gestion des fichiers clients, le manquement aux obligations d'information des personnes, l'absence de formalités préalables à la mise en œuvre du traitement* » (12). De plus, en 2009, 85% des mises en demeure de la CNIL (85) furent mises en conformité (12). En 2016, la CNIL a prononcé 82 mises en demeures et 13 sanctions (9 avertissements et 4 sanctions financières) (41). La CNIL déclare en effet dans son rapport en 2013 que « *la logique de la loi et de son application par la CNIL visent à la mise en conformité des organismes. Le processus mise en œuvre leur offre à plusieurs reprises cette possibilité, sachant qu'à chaque phase d'instruction, il leur est indiqué les mesures à prendre pour faire en sorte que la procédure engagée prenne fin.* In fine, *peu de cas ne sont pas résolus « à l'amiable »* » (42)(4).

Les sanctions, qu'elles soient pénales ou administratives, viennent donc clore le cadre légal de la protection des données personnelles. Et si certaines critiques sont formulées contre ce pouvoir de sanction administrative, confié non pas à un tribunal mais à une commission, ni les tribunaux ni la CNIL n'ont les ressources suffisantes pour traiter et surveiller tous les manquements à la loi en matière de protection des données personnelles. Aussi, les sanctions prononcées par la CNIL sont le résultat d'une politique définie, où, comme l'explique Fabrice Mattatia dans son ouvrage *Le droit des données personnelles*, « *l'exemplarité palliera le manque d'exhaustivité* » (4).

2 Protection des données personnelles au sein du système de santé

Depuis plusieurs années, le système de santé en France est confronté à de nombreux défis, parmi lesquels la désertification médicale, la diminution des ressources, le vieillissement de la population, etc. En parallèle à ces défis croissants, l'informatique connaît un essor sans précédent, envahissant tous les secteurs de notre société, santé comprise. Aussi le numérique peut-il apparaître comme vecteur de solutions, afin de répondre aux challenges de notre système de santé actuel. En guise d'exemple, nous pouvons citer la télémédecine, qui bénéficie de plus en plus d'expérimentations afin de pallier aux déserts médicaux, ou encore les dossiers médicaux partagés qui ambitionnent de faciliter la coordination des soins et d'ainsi offrir aux patients une meilleure prise en charge tout en réduisant les coûts.

Toutefois, cette montée en puissance du numérique et des autres nouvelles technologies de l'information et de la communication n'est pas sans poser un certain nombre de questions. Parmi ces interrogations, la problématique de la protection des données personnelles est cruciale et légitime, car les données personnelles et de santé relèvent de l'intime.

Dans cette deuxième partie, nous nous intéresserons donc à l'organisation et à la mise en œuvre de la protection des données personnelles au sein du système de santé en France. Pour cela, nous détaillerons tout d'abord la notion de données de santé, une notion nouvellement introduite dans le droit européen et bénéficiant d'un encadrement et de dispositions particulières et multiples. Nous nous intéresserons ensuite à la question de la responsabilité du traitement au sein du système de santé, en termes d'acteurs et d'obligations. Puis nous présenterons les autres parties prenantes à la protection des données personnelles en santé, avant de nous pencher sur une question critique, celle du partage des données de santé.

2.1 Le cas particulier des données de santé

Les données de santé, parce qu'elles touchent à une partie sensiblement intime de la vie privée, ne peuvent pas être considérées comme de simples données à caractère personnel. Le législateur, conscient de cet enjeu, les a donc très tôt distinguées du reste des données personnelles en en faisant une catégorie particulière de données. Dans cette partie, nous nous intéresserons aux particularités juridiques des données de santé : leur définition, leurs différentes protections, mais aussi leur hébergement, particulièrement encadré.

2.1.1 Définition des données de santé

Bien que reconnues comme une catégorie particulière de données personnelles par la directive européenne 95/46, les données de santé n'étaient alors pas clairement définies. Ni

cette directive, ni la loi n°2004-801 modifiant la loi n°78-17 du 6 janvier 1978, transposant cette directive, ne faisaient ainsi mention d'une quelconque définition des données de santé. Seul le Code de la santé publique permettait alors d'en appréhender les contours, par ses articles L. 1110-4 et L. 1111-7, respectivement relatifs au secret professionnel et au droit d'accès au dossier médical.

L'article L. 1110-4 du Code de la santé publique (C. santé publ.) dispose ainsi que le secret professionnel « *couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes* » (43).

Quant à l'article L. 1111-7 du Code de la santé publique, il précise que le dossier médical comprend les *« résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé* » (44). Cette liste, bien que non exhaustive, permet de mieux apprécier ce que les données de santé peuvent recouvrir en pratique.

Cependant, l'essor du numérique et des nouvelles technologies n'a pas manqué d'affecter le domaine de la santé. Aussi était-il devenu indispensable de donner une définition juridique aux données de santé. Le règlement européen 2016/679, ou Règlement Général sur la Protection des Données, est ainsi le premier texte juridique à offrir une définition des données de santé. Son article 4 dispose que les « données concernant la santé » signifient « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* » (22). Ce même article définit également les « données génétiques » comme étant « *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* » (22).

Après plusieurs années d'un certain flou juridique, le législateur a donc finalement doté les données de santé d'une définition, ne pouvant ignorer les enjeux de protection soulevés par cette catégorie de données particulièrement sensibles.

2.1.2 Une protection multiple

Les données de santé étant au carrefour de la protection des données personnelles et du droit de santé publique, elles bénéficient de plusieurs protections, différentes mais complémentaires.

2.1.2.1 Principe d'interdiction de traitement

Pour leur caractère particulièrement sensible et intime, les données relatives à la santé ont, avec la directive européenne 95/46 de 1995, été considérées comme une catégorie particulières de données personnelles, aux côtés des données relevant de « *l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale* » ou encore de « *la vie sexuelle* ». Cette disposition, transposée en droit français par la loi n°2004-801, modifiant la loi n°78-17 du 6 janvier 1978, interdit le traitement de ce type de données.

Néanmoins, des exceptions ont été prévues par le législateur afin que le traitement de ces données, dont les données de santé, puisse être autorisé et ainsi déroger à ce principe général d'interdiction. L'article 9 du règlement européen 2016/679 détaille ces différentes exceptions. Parmi elles, les situations suivantes peuvent s'appliquer au domaine de la santé :

- lorsque « *la personne concernée a donné son consentement explicite* »,
- lorsque « *le traitement est nécessaire* […] *en matière de droit du travail, de la sécurité sociale et de la protection sociale* »,
- lorsque « *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement* »,
- lorsque « *le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale* »,
- lorsque « *le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux* »,
- lorsque « *le traitement est nécessaire à des fins* […] *de recherche scientifique* » (22).

En somme, deux types d'exceptions existent : d'une part les exceptions reposant sur l'intérêt de la personne ou de la société, et d'autre part l'exception liée au consentement de la personne concernée. Cette dichotomie est importante, car tandis qu'une prise en charge médicale d'un patient n'exige qu'une information de ce dernier, le traitement de ses données dans d'autres situations nécessite le recueil express de son consentement.

2.1.2.2 Secret professionnel

Le secret professionnel est un devoir incombant à bon nombre de personnes, dans des corps de métiers variés. Néanmoins, quel que soit sa nature, le secret professionnel est garanti

par l'article 226-13 du Code pénal. Cet article dispose que « *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 15 000 euros d'amende* » (45). Seules trois exceptions sont prévues, à l'article 226-14, dans des situations précises (*i.e.* sujet, détenteur et destinataire du secret précis).

Par ailleurs, en matière de santé, ces dispositions du Code pénal ne sont les seules visant à protéger le secret professionnel. Principe ancestral de la médecine, ce secret est une condition *sine qua none* de la relation de confiance nécessaire entre un médecin et son patient. Le serment d'Hippocrate énonce ainsi : « *Admis(e) dans l'intimité des personnes, je tairai les secrets qui me seront confiés* » (46). Ce principe antique est également inscrit dans le droit français, plus précisément à l'article L. 1110-4 du Code de la santé publique. Cet article dispose que « *toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins* […] *a droit au respect de sa vie privée et du secret des informations la concernant* » (43).

Le secret professionnel relève donc à la fois d'une obligation légale et d'un devoir déontologique. En santé, le secret professionnel vient protéger deux intérêts, l'intérêt particulier d'un patient au respect de sa vie privée et de son intimité et l'intérêt plus général d'une société de maintenir la relation de confiance établie entre un professionnel de santé et son patient. Le secret professionnel constitue ainsi une protection forte des données de santé, complétant celle de la loi « Informatique et Libertés ».

2.1.2.3 Droit au respect de la vie privée

Déjà disposé par l'article L. 1110-4 du Code de la santé publique, le droit au respect de la vie privée et familiale est également consacré par le Code civil français, à l'article 9 (« *Chacun a droit au respect de sa vie privée* ») (47) et par la Convention européenne des droits de l'Homme, à l'article 8. Ce droit s'applique également en matière de données de santé, comme en témoignent la jurisprudence de la Cour européenne des droits de l'Homme.

Ainsi, la Cour, dans son arrêt du 25 février 1997, concernant l'affaire *Z c/ Finlande*, déclarait ainsi : « *Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique* […]. *Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général* » (48). Par ailleurs, dans cette même affaire, la Cour est confrontée à une catégorie de données encore plus spécifique : les données de santé relatives à la séropositivité. La Cour reconnaît à ces données un caractère « *extrêmement intime et sensible* » (48). Dans une autre arrêt, concernant l'affaire C. C. c/ Espagne, la Cour énonce même un « *principe de protection spéciale de la confidentialité des informations relatives à la séropositivité* » (49). En somme, la Cour européenne des droits de l'Homme protège elle aussi les données de santé, en vertu du droit au respect de la vie privée, disposé par la Convention européenne des droits de l'Homme. La Cour, tout en consacrant la sensibilité particulière des

données de santé, va même plus loin que le législateur, en distinguant un sous-ensemble encore plus sensible, les données relatives à la séropositivité.

La protection des données de santé est donc assurée par plusieurs instruments juridiques, répondant à des impératifs différents, mais permettant de rendre cette protection robuste.

2.1.3 Un hébergement encadré

Depuis plusieurs années, les dossiers médicaux s'informatisent, la collection de données de santé se fait de plus en plus présente, des hôpitaux jusqu'à nos *smartphones*, la quantité de données de santé s'accroit donc de façon considérable. Aussi, les données de santé étant des données particulièrement sensibles, le législateur s'est intéressé à leur hébergement, afin que ce dernier présente les garanties idoines.

2.1.3.1 Cadre légal

L'hébergement des données de santé est l'objet de l'article L. 1111-8 du Code de la santé publique. Cet article, dans sa version entrant en vigueur au 1er janvier 2019, dispose que « *toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social* […] *réalise cet hébergement dans les conditions prévues au présent article* » (50). Il est ajouté qu'un contrat est nécessaire pour la prestation d'hébergement de données de santé. Il est également précisé que les organismes hébergeurs ne peuvent utiliser les données dont ils ont la charge à d'autres fins que l'hébergement.

Mais surtout, l'article L. 1111-8, modifié par l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, et entrant en vigueur au 1er janvier 2019, requiert désormais des hébergeurs de données de santé qu'ils disposent d'un certificat de conformité (50)(51). À compter du 1er avril 2018, cette nouvelle disposition de la loi, la certification, viendra ainsi remplacer la procédure d'agrément utilisée jusqu'à présent. Par ailleurs, le décret n° 2018-137 du 26 février 2018 vient préciser les détails de cette nouvelle procédure de certification (52).

2.1.3.2 Procédure de certification

Avec cette nouvelle procédure, le législateur remplace l'agrément par un système de certification, délivré par un organisme accrédité par le COFRAC[22]. La certification s'appuiera

[22] Comité français d'accréditation

sur un référentiel dédié, ce dernier reposant quant à lui sur : des exigences des normes ISO (ISO 27001 sur le « système de gestion de la sécurité des systèmes d'information », ISO 20000 sur le « système de gestion de la qualité des services », et ISO 27018 sur la « protection des données à caractère personnel »), ainsi que sur des exigences spécifiques à l'hébergement de données de santé ». (53)

La procédure de certification commence tout d'abord par le choix d'un organisme certificateur, accrédité par le COFRAC. Ensuite, cet organisme réalise deux audits, le premier étant documentaire, le second sur site. Si, à l'issue de ces audits, l'hébergeur est conforme au référentiel de certification, alors l'organisme certificateur peut lui délivrer un certificat (Figure 5).

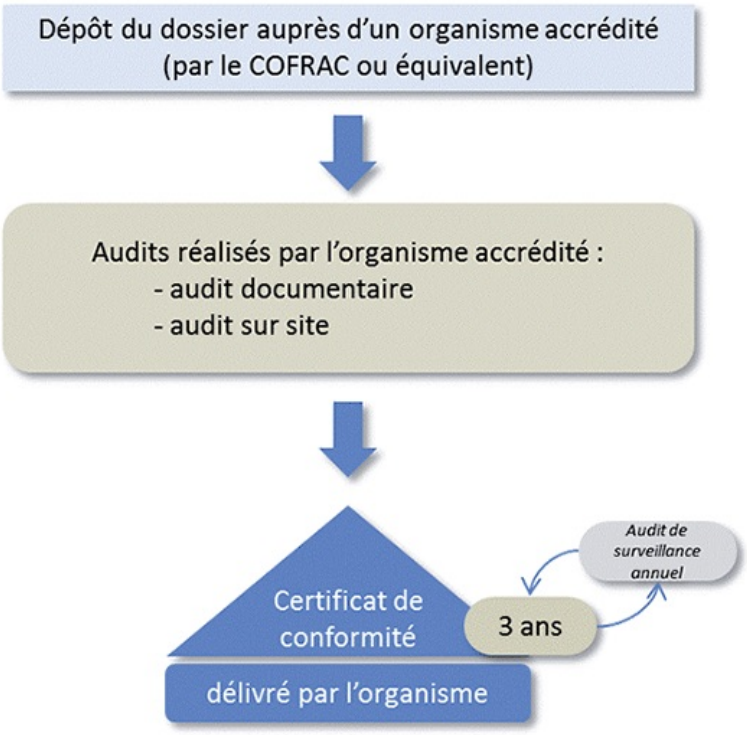


Figure 5. Procédure de certification des hébergeurs de données de santé (54)

Ce certificat est valide trois ans. Pendant cette période de validité, l'organisme certificateur est tenu de mener des audits de surveillance tous les ans. Par ailleurs, deux types de certificat peuvent être délivrés, correspondant à deux types d'hébergements distincts :

- le certificat « hébergeur d'infrastructure physique »,
- le certificat « hébergeur infogéreur ».

Le premier regroupe les activités de « *mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle* », tandis que le second correspond aux activités de « *mise à disposition d'infrastructure virtuelle, de mise à disposition de plateforme logicielle, d'infogérance et de sauvegarde externalisée* ». (55)

Ainsi, les données de santé, à la différence des autres données personnelles, doivent, en France, répondre à des requis précis en matière d'hébergement. Cette activité est encadrée par la loi et les hébergeurs de santé doivent être certifiés. De cette façon, et au regard de leur caractère particulièrement sensible, les données de santé bénéficient d'un haut niveau de sécurité en matière d'hébergement, démontré et répondant à des normes déterminées par l'État.

2.2 La responsabilité du traitement

Dans le triptyque de la protection des données personnelles, le responsable du traitement occupe une place centrale, aux côtés de la personne concernée et de l'autorité de contrôle. Dans cette partie, nous nous intéresserons donc à deux types de responsables du traitement du système de santé : l'établissement de santé et le professionnel de santé. Nous nous pencherons également sur leurs obligations en qualité de responsable du traitement, ainsi qu'à l'impact du nouveau Règlement Général sur la Protection des Données.

2.2.1 Deux types de responsables

Au sein du système de santé, nous pouvons identifier deux catégories de responsables de traitement : le professionnel de santé et l'établissement de santé. Et s'ils doivent tous deux répondre aux mêmes grands principes en matière de protection des données personnelles, la mise en œuvre de ces dispositions varie entre établissements et professionnels de santé. Par ailleurs, établissements et professionnels de santé collectent et traitent deux types de données personnelles : des données à caractère personnel « classiques », mais aussi des données de santé, au sens de la définition donnée par le règlement 2016/679[23]. Ils se doivent donc, en qualité de responsable du traitement, d'être vigilants et de veiller à respecter la loi s'appliquant pour chacun de ces deux types de données.

2.2.1.1 Le professionnel de santé

Les professions de santé sont disposées par la quatrième partie du Code de la santé publique et regroupent trois catégories de professionnels :

- les professionnels médicaux : « *médecins, sages-femmes et odontologistes* »,
- les professionnels de la pharmacie : « *pharmaciens, préparateurs en pharmacie* »,

[23] cf. 2.1.1 Définition des données de santé

- les professionnels auxiliaires médicaux : « *infirmiers, masseurs-kinésithérapeutes, pédicures-podologues, ergothérapeutes et psychomotriciens, orthophonistes et orthoptistes, manipulateurs d'électroradiologie médicale et techniciens de laboratoire médical, audioprothésistes, opticiens-lunetiers, prothésistes et orthésistes, diététiciens, aides-soignants, auxiliaires de puériculture et ambulanciers* » (56).

Mais quels qu'ils soient, les professionnels de santé sont tous amenés, dans leur pratique quotidienne, à collecter, traiter ou utiliser des données personnelles et notamment des données personnelles de santé. Ils se retrouvent donc, de fait, confrontés à la problématique de la protection des données personnelles, dont celles des données de santé.

Toutefois, la qualification du professionnel de santé dépend de ses conditions d'exercice. Lorsqu'il exerce en libéral, seul, le professionnel de santé est considéré comme le responsable du traitement. Il doit donc répondre à toutes les obligations qui lui incombent. En revanche, au sein d'une activité collective (*e.g.* cabinet de groupe, réseaux de soins, etc.), la responsabilité du professionnel de santé est limitée lorsque les outils informatiques sont mutualisés. (57)

Le Conseil National de l'Ordre des Pharmaciens, dans son guide relatif à la confidentialité des données, précise ainsi que le pharmacien d'officine, gérant ou associé, est considéré comme responsable des traitements destinés à « *des fins de gestion de la pharmacie et d'analyse statistique des ventes de médicaments* » (58). En effet, conformément à la définition légale du responsable du traitement[24], le pharmacien devient responsable dès lors qu'il « *détermine les finalités et les moyens du traitement* » (22).

2.2.1.2 L'établissement de santé

Les établissements de santé sont définis par l'article L. 6111-1 du Code de la santé publique, comme les établissements assurant « *le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes* » et menant « *des actions de prévention et d'éducation à la santé* » (59). Parmi les établissements, nous trouvons donc les centres hospitaliers, les cliniques privés, les EHPAD[25], etc. Cette large définition comprend ainsi les établissements de santé publics comme privés, ces derniers regroupant les établissements privés d'intérêt collectif et privés à but lucratif.

Maillons essentiels du système de santé, ces établissements collectent de nombreuses données personnelles. L'établissement de santé est considéré comme responsable du traitement de ces données. Et de cette fonction découlent pour l'établissement toutes les obligations faites au responsable du traitement[26]. Toutefois, lorsqu'un établissement de santé réalise des opérations pour le compte d'un tiers, cet établissement devient alors un sous-traitant, et non plus le responsable du traitement (60).

---

[24] cf. 1.2.1.1.3 Responsable du traitement

[25] Etablissements d'Hébergement pour Personnes Agées Dépendantes

[26] cf. 1.2.2.2 Les devoirs du responsable du traitement

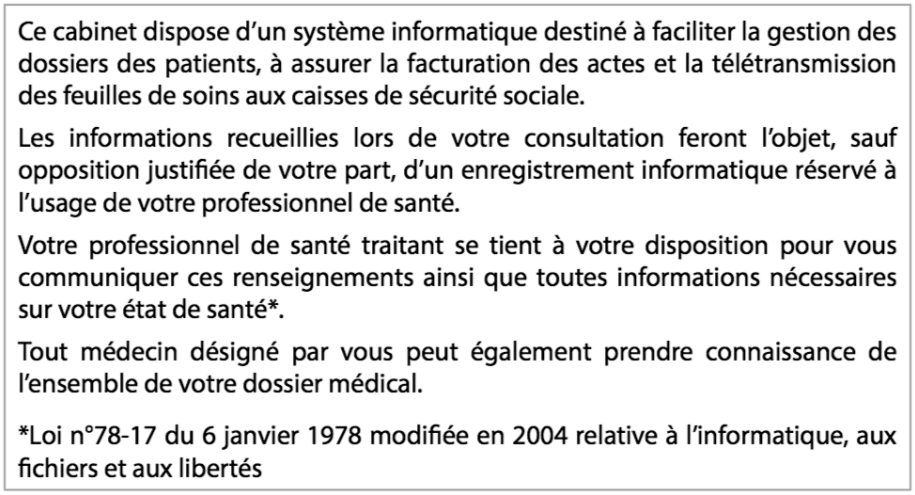
En somme, chaque établissement de santé doit donc définir ses obligations et responsabilités au regard de sa qualification juridique : sous-traitant ou responsable du traitement.

2.2.1.3 Obligations

En tant que responsables du traitement, les établissements et les professionnels de santé doivent répondre à un certain nombre d'obligations, en matière d'information du patient, de conservation et de sécurité des données et de formalités préalables.

2.2.1.3.1 Information

Tout d'abord, le professionnel ou l'établissement de santé étant amené à collecter et traiter les données personnelles de ses patients, il est tenu de les en informer. En effet, chaque patient a le droit de connaître un certain nombre d'informations relatives au traitement de ses données personnelles[27]. La CNIL et l'ASIP Santé recommandent donc aux professionnels de santé exerçant en libéral d'apposer au sein de leur cabinet une affiche d'information à destination des patients. La CNIL propose à cet effet un modèle dans son guide à destination des professionnels de santé (Figure 6).



Ce cabinet dispose d'un système informatique destiné à faciliter la gestion des dossiers des patients, à assurer la facturation des actes et la télétransmission des feuilles de soins aux caisses de sécurité sociale.

Les informations recueillies lors de votre consultation feront l'objet, sauf opposition justifiée de votre part, d'un enregistrement informatique réservé à l'usage de votre professionnel de santé.

Votre professionnel de santé traitant se tient à votre disposition pour vous communiquer ces renseignements ainsi que toutes informations nécessaires sur votre état de santé*.

Tout médecin désigné par vous peut également prendre connaissance de l'ensemble de votre dossier médical.

*Loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés

Figure 6. Exemple d'affiche d'information aux patients (61)

Cette obligation s'ajoute à un autre devoir d'information, qui « *incombe à tout professionnel de santé* ». L'article L. 1111-2 du Code la santé publique dispose en effet que « *toute personne a le droit d'être informée sur son état de santé* » (35). En outre, l'article R. 4127-35 du Code de la santé publique précise, s'agissant des médecins, qu'ils doivent à leurs patients « *une information loyale, claire et appropriée sur son état, les investigations et les soins qu'il[s] propose[nt]* » (32).

[27] cf. 1.2.2.2.1.1 Devoir d'information

2.2.1.3.2 Conservation

En vertu du principe de limitation de la conservation[28], les données personnelles ne peuvent être conservées indéfiniment. Concernant les établissements de santé, la durée de conservation est disposée par l'article R. 1112-7 du Code de la santé publique. Cette durée est de vingt ans à compter du dernier séjour ou de la dernière consultation au sein de l'établissement (62). Quant aux professionnels de santé, la loi n'impose pas de durée spécifique. Il est donc d'usage de suivre la règle applicable aux établissements de santé, *i.e.* un archivage de vingt ans. Cette recommandation est formulée par l'ASIP Santé dans son mémento consacré à la sécurité et rédigé conjointement avec la DSSIS (Délégation à la Stratégie des Systèmes d'Information de Santé). (57)

2.2.1.3.3 Sécurité

La sécurité est un autre enjeu de la protection des données personnelles, selon le principe d'intégrité et de confidentialité[29] et cette question est d'autant plus critique lorsqu'elle inclut des données de santé.

2.2.1.3.3.1 Mesures générales de sécurité

Dans son guide à destination des professionnels de santé (61), la CNIL détaille quelques mesures élémentaires de sécurité qui devraient être mises en place :

- protection de l'accès aux données par mot de passe,
- protection de l'accès aux locaux et aux postes informatiques,
- utiliser d'un logiciel anti-virus,
- réalisation de sauvegardes chiffrées régulières,
- etc.

Ces mesures générales de sécurité s'appliquent aussi bien aux professionnels et établissement de santé, qu'à toute personne impliquée dans le traitement de données personnelles. Aussi, pour plus de précisions, il convient de se référer au guide de la CNIL dédié à la sécurité des données personnelles (63).

Outre ces mesures élémentaires de sécurité, pouvant s'appliquer à tous, les professionnels de santé doivent également veiller à garantir la sécurité de leurs échanges électroniques. Aussi, l'utilisation de systèmes de messagerie et de télécopie doit répondre à des critères de sécurité suffisants. Il est ainsi préférable d'avoir recours à un système de messagerie interne et sécurisé. Si un tel système n'est pas disponible, l'utilisation d'une

---

[28] cf. 1.2.1.2.5 Principe de limitation de la conservation
[29] cf. 1.2.1.2.6 Principe d'intégrité et de confidentialité

messagerie standard est possible, à la condition de transmettre les données personnelles sous forme de pièces jointes chiffrées.

2.2.1.3.3.2 Mesures spécifiques à la santé

Afin de répondre au caractère particulièrement sensible des données de santé, des mesures de sécurité spécifiques sont également prévues, venant accompagner les mesures générales précédentes. Tout d'abord, l'article R. 1110-2 du Code de la santé publique précise que le responsable du traitement doit « *gérer la liste nominative des professionnels habilités à accéder aux informations médicales* […] *et la tenir à la disposition des personnes concernées par ces informations* » (64).

Par ailleurs, le 15 mai 2007, le gouvernement a adopté le décret n° 2007-960 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique, dit « décret confidentialité ». Ce décret déclare que des référentiels doivent être **«** *définis par arrêtés du ministre chargé de la santé* » afin d'encadrer la conservation informatique d'informations médicales. Mais surtout, ce décret précise que « *l'utilisation de la carte de professionnel de santé* […] *est obligatoire* » pour l'accès « *par des professionnels de santé aux informations médicales à caractère personnel* » (65).

Enfin, l'État a également entrepris de régir de façon plus précise la sécurité des systèmes d'information de santé. Face aux enjeux et aux risques que présente l'usage toujours plus important des technologies de l'information dans le champ de la santé, l'État, entouré des différents acteurs du secteur, a donc publié sa Politique Générale de Sécurité des Systèmes d'Information de Santé, ou PGSSI-S (66). Cette politique est un corpus documentaire comprenant quatre catégories de documents :

- des guides pratiques organisationnels, à destination des professionnels de santé,
- des référentiels techniques, à destination des industriels et des maîtres d'œuvre,
- des guides pratiques spécifiques, à destination des responsables de traitement,
- des guides juridiques, à destination de tous les utilisateurs des systèmes d'information. (67)

Les différents guides et référentiel composant ce corpus documentaire sont disponibles sur le site internet de l'ASIP Santé. Ils couvrent des sujets variés, comme l'identification et l'authentification des acteurs de santé, les règles en matière de dispositifs connectés, la mise en place d'un accès Wifi, la sauvegarde, le plan de continuité informatique, la gestion des habilitations d'accès, etc. (68)

En somme, la sécurité revêtant un aspect particulièrement critique, notamment s'agissant de données de santé, des mesures générales et spécifiques tentent d'apporter le meilleur niveau de protection possible à ces données sensibles.

2.2.1.3.4 Formalités préalables

Si les formalités préalables auprès de la CNIL, pour déclarer ou autoriser un traitement, risquent fort probablement d'être revues à la suite du Règlement Général sur la Protection des Données, ces formalités demeurent toujours valables au moment de la rédaction de nos travaux.

Les professionnels et établissements de santé doivent ainsi s'enquérir de démarches auprès de la CNIL préalablement à la mise en œuvre d'un traitement de données personnelles. La Commission dresse une liste de ces formalités dans son guide à destination des professionnels de santé (61) (Tableau III).

Tableau III. Fichiers des professionnels de santé et leur déclaration à la CNIL, adapté du Guide de la CNIL à destination des professionnels de santé (61)

Catégorie	Finalité du fichier	Formalités déclaratives	Autres formalités
Professions libérales de santé	Gestion administrative et médicale des patients	Norme Simplifiée n°50	Utilisation obligatoire de la Carte Professionnelle de Santé (CPS)
Pharmacie	Gestion courant de la pharmacie et dossier pharmaceutique	Norme Simplifiée n°52	
Laboratoires d'analyses de biologie médicale	Gestion courante du laboratoire	Norme Simplifiée n°53	
Opticiens	Gestion administrative des clients	Norme Simplifiée n°54	-

Nous pouvons ainsi constater que ces formalités déclaratives sont pour la plupart des normes simplifiées, *i.e.* un cadre précis établi par la CNIL pour un type de traitement déterminé. Pour ce type de traitement, le responsable adresse simplement à la Commission une déclaration dite simplifiée s'engageant à être en conformité avec la norme correspondante. Par ailleurs, ce même guide liste également les formalités concernant les établissements de santé (Tableau IV).

Tableau IV. Fichiers d'un établissement de santé et leur déclaration à la CNIL, adapté du Guide de la CNIL à destination des professionnels de santé (61)

Finalité du fichier	Formalités déclaratives	Autres formalités
Gestion administrative	Déclaration Normale (DN)	-
Gestion des repas		-
Gestion du dossier médical		-
Gestion des urgences, du laboratoire, du service de radiologie…		-
Frappe de comptes rendus et de courriers médicaux par un prestataire en Europe		Signature d'une clause de confidentialité avec le

		prestataire
Constitution d'une cohorte mono-centrique de patients		-
Programme de Médicalisation des Systèmes d'Information (PMSI)		-
Programme d'éducation thérapeutique (mono-centrique)		Si le programme concerne uniquement les patients de l'établissement

Sécurité, formalités préalables, conservation, information, les obligations du responsable du traitement, qu'il soit professionnel ou établissement de santé, sont donc multiples en matière de protection des données personnelles.

2.2.2 Conséquences du RGPD[30]

Comme nous l'avons vu précédemment, le Règlement Général sur la Protection des Données (RGPD), ou règlement 2016/679, apporte bon nombre de changements en matière de protection des données personnelles. En matière de santé, la première nouveauté du règlement est d'enfin apporter une définition aux données de santé, comme nous l'avons vu précédemment[31]. Mais cette nouveauté n'est pas le seul changement introduit par le règlement et affectant le domaine de la santé. Les responsables de traitements, et notamment les établissements de santé, ne sont donc pas épargnés par ces modifications législatives et ont dû, ou vont devoir, se préparer à ces changements juridiques.

L'ASIP Santé, en collaboration avec la CNIL, a donc rédigé une fiche pratique à destination des établissements de santé afin de faciliter leur préparation et l'implémentation du RGPD (60). Ainsi, les établissements de santé devront mettre en œuvre les nouvelles obligations du responsable du traitement, comme la tenue d'un registre par exemple. Ils devront également procéder à des analyses d'impact préalables dans le cas de certains traitements. Les établissements de santé peuvent notamment être concernés dans le cas de traitement de « *données de santé à grande échelle* » (60).

De plus, les établissements publics doivent désormais désigner un délégué à la protection des données, conformément à l'article 37 du règlement 2016/679. Alors qu'auparavant le Correspondant Informatique et Libertés était facultatif, le délégué à la protection des données devient donc obligatoire pour les établissements publics. Quant aux établissements privés, ils sont tenus de disposer d'un délégué à la protection des données uniquement si les traitements mis en œuvre « *exigent un suivi régulier et systématique à grande échelle des personnes concernées* » (22). Toutefois, le règlement prévoit la possibilité

[30] Règlement Général sur la Protection des Données (règlement 2016/679)
[31] cf. 2.1.1 Définition des données de santé

pour les établissements de mutualiser cette fonction, en ne disposant que d'un seul délégué à la protection des données pour plusieurs entités différentes.

Par ailleurs, la fiche de l'ASIP Santé rappelle que, le Règlement Général sur la Protection des Données créant de nouveaux droits pour les personnes concernées (*e.g.* droit à l'effacement, droit à la portabilité des données[32]), il est nécessaire pour les établissements de santé de mettre à jour leurs systèmes d'information afin de permettre la mise en œuvre pratique de ces droits.

Enfin, le Règlement Général sur la Protection des Données impose désormais au responsable du traitement de notifier à l'autorité de contrôler toute violation de données personnelles. Par conséquent, les établissements et professionnels de santé doivent eux aussi se plier à cette obligation légale. En outre, et conformément à l'article L. 1111-8-2 du Code de la santé publique, récemment modifié à par l'ordonnance 2018-20 du 17 janvier 2018, les établissements de santé sont tenus de signaler « *sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information* » (69).

2.3 Autres parties prenantes

Outre les établissements et les professionnels de santé, la protection des données personnelles au sein du système de santé impliquent aussi d'autres parties prenantes. Parmi ces autres acteurs, nous retrouvons la CNIL, en qualité d'autorité de contrôle, l'ASIP Santé, une agence publique dédiée au numérique en santé, mais aussi le patient, qui n'est autre que la personne concernée par ces traitements de données.

2.3.1 Le patient

Dans le triptyque responsable du traitement, personne concernée et autorité de contrôle, le patient occupe donc le rôle de personne concernée, au sein du système de santé. À ce titre, le patient dispose de plusieurs droits, prévus tant par la loi n°78/17, dite « Informatique et Libertés », que par le Code de la santé publique. Dans cette partie, nous nous intéresserons plus particulièrement à l'exercice du droit d'accès et du droit d'opposition pour les patients au sein du système de santé.

2.3.1.1 Droit d'accès

En tant que personne concernée par le traitement de ses données personnelles, le patient est bien entendu autorisé à demander l'accès à ses données personnelles de santé,

[32] cf. 1.1.2.2.2 Nouveaux droits

conformément au droit d'accès disposé par la loi n°78-17 du 6 janvier 1978 modifiée et par le règlement européen 2016/679[33]. Mais le patient a également le droit d'accéder à son dossier médical conformément à l'article L. 1111-7 du Code de la santé publique, créé par la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, qui déclare explicitement que « *toute personne a accès à l'ensemble des informations concernant sa santé* ». Ces informations comprennent entre autres les « *résultats d'examen, comptes rendus de consultation, d'intervention, d'exploration ou d'hospitalisation, des protocoles et prescriptions thérapeutiques mis en œuvre, feuilles de surveillance, correspondances entre professionnels de santé* » (44). Le droit d'accès en santé est donc doublement encadré par la loi.

Ce même article du Code de la santé publique précise également certaines modalités de ce droit d'accès. Tout d'abord, le patient peut accéder à ses données soit lui-même, *i.e.* directement, soit indirectement, c'est-à-dire en faisant appel au médecin de son choix, qui consultera alors ses données à la place du patient. De la même façon, l'article 43 de la loi n°78-17 du 6 janvier 1978 modifiée énonce que, dans le cadre du droit d'accès 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* » (30).

En termes de délai, le professionnel de santé ou l'établissement visé par une demande de droit d'accès, dispose d'un délai maximum de huit jours pour y répondre. Ce délai est toutefois porté à deux mois dans le cas d'informations de plus de cinq ans (61)(44). L'exercice de ce droit d'accès est gratuit, seul le remboursement des coûts de reproduction et d'envoi des documents, le cas échéant, peut être demander au patient.

Enfin, l'article L. 1111-7 du Code de la santé publique prévoit également deux autres situations : lorsque le patient est mineur ou lorsque le patient est décédé. Dans le premier cas, le droit d'accès doit alors être exercé par « *les titulaires de l'autorité parentale* ». Dans le second cas, il est disposé que les ayants droit, le concubin ou le partenaire du patient décédé peuvent avoir accès au dossier médical, dans les conditions prévues par l'article L. 1110-4, c'est-à-dire « *pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits* » (43).

2.3.1.2 Droit d'opposition

Le droit d'opposition est également prévu à la fois par le Code de la santé publique et la loi n°78-18 du 6 janvier 1978 modifiée. Cependant, chacune de ces deux lois évoque des droits d'opposition différents. Le Code de la santé publique tout d'abord, entend le droit d'opposition comme l'opposition au partage et à l'échange d'informations entre

[33] cf. 1.2.2.1.1 Droit d'accès

professionnels de santé. Ce droit est disposé à l'article L. 1110-4 du Code de la santé publique et il est précisé que les personnes doivent être informées de ce droit et qu'elles ont la possibilité de l'exercer à tout moment (43). Quant au droit d'opposition de la loi n°78-18 du 6 janvier 1978 modifiée, il permet à un individu de s'opposer au traitement de ses données personnelles. Ce droit est détaillé à l'article 38 de la loi. Ce même article apporte toutefois quelques précisions et limites à ce droit d'opposition. Ainsi, si ce droit est gratuit, il doit surtout être fondé sur des « *motifs légitimes* » et il ne peut s'appliquer « *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* » (30).

Si les cas sont rares, il existe toutefois des situations dans laquelle la CNIL a estimé légitime la demande d'un patient. Ainsi, un patient, pris en charge aux Hospices civils de Lyon, a eu gain de cause lorsqu'il a demandé l'effacement des informations concernant ses hospitalisations. En effet, ne voulant pas révéler la pathologie dont il était atteint, il ne souhaitait pas que son beau-frère, médecin dans le même établissement, puis avoir accès à ses informations (70). Enfin, qu'il y ait accord ou non entre le patient et le professionnel ou l'établissement de santé concernant l'exercice d'un droit d'opposition, la CNIL conseille que l'effacement d'informations au sein d'un dossier médical soit tracé et identifié par une mention idoine (70).

2.3.2 La CNIL

La Commission Nationale de l'Informatique et des Libertés, ou CNIL, veille au respect de la loi en matière de protection de toutes les données personnelles, y compris les données de santé. Aussi la CNIL joue-t-elle un rôle majeur dans la protection des données personnelles de santé. En effet, et jusqu'à peu, le traitement de données de santé était soumis à un régime strict de formalités préalables auprès de la CNIL. Cependant, comme nous l'avons vu précédemment, l'entrée en vigueur du Règlement Général sur la Protection des Données change ce paradigme et réduit ces formalités préalables[34].

La CNIL, sur son internet, déclare ainsi que les traitements de données de santé relevant des exceptions au principe d'interdiction[35] feront désormais l'objet d'une simple déclaration (contrairement à une autorisation auparavant) (71). Par ailleurs, et concernant la recherche en santé, la CNIL a rédigé une méthodologie de référence. Cette méthodologie de référence (MR-001) correspond à la délibération n° 2016-262 du 21 juillet 2016 portant modification de la méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales (MR-001) et s'applique au domaine de la recherche en santé, avec recueil « *consentement exprès ou écrit, libre et éclairé* » des

[34] cf. 1.1.2.2.3 Nouvelles responsabilités
[35] cf. 2.1.2.1 Principe d'interdiction de traitement

personnes concernées (72). Dans le cadre de cette méthodologie de référence, le responsable du traitement doit simplement adresser un engagement de conformité à cette méthodologie en guise de formalité préalable.

Enfin, si la CNIL dispose de prérogatives en matière de recommandations, elle n'en demeure pas moins une autorité de contrôle qui se doit de veiller au respect de la loi en vigueur. Les sanctions de la Commission font d'ailleurs souvent la une des journaux, comme l'amende infligée en janvier 2018 au distributeur Darty® suite à un incident de sécurité (73).

Mais les établissements de santé n'échappent pas, eux non plus, au contrôle de la CNIL, comme en témoigne la mise en demeure du centre hospitalier de Saint-Malo en 2013 (74). Dans sa délibération, la Commission justifie sa décision par deux manquements de la part de cet établissement : d'une part un manquement à **«** *l'obligation de veiller à la sécurité et à la confidentialité des données* » et d'autre part un manquement à « *l'obligation de respecter la vie privée et les libertés individuelles* ». Ces manquements sont intervenus dans le cadre d'une prestation externe de codage d'actes médicaux, où des « *tiers non autorisés* » avaient « *accès à des données couvertes par le secret médical* » (75). Suite à cette mise en demeure de la CNIL, le centre hospitalier de Saint-Malo s'est rapidement mis en conformité et la procédure a pu être refermée vingt-deux jours plus tard. Cet exemple illustre bien que les établissements de santé ne sont pas exempts du contrôle de la CNIL. Par ailleurs, une situation unique peut induire des manquements multiples, la protection des données personnelles de santé répondant à la fois aux obligations du Code de la santé publique et de la loi du 6 janvier 1978 dite « Loi Informatique et Libertés ».

Enfin, plus récemment, c'est la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés (CNAMTS) qui a été mise en demeure par la CNIL. La Commission, dans sa décision n° MED-2018-006 du 8 février 2018, justifie cette mise en demeure au regard d'un « *manquement à l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée* », relatif à la sécurité. (76)

Malgré l'existence d'une agence dédiée au numérique en santé, et nonobstant le changement de paradigme induit par le Règlement Général sur la Protection des Données, la CNIL demeure en France l'autorité de contrôle et ainsi l'acteur de référence en matière de protection des données personnelles, de santé ou non.

2.3.3 L'ASIP Santé

L'ASIP Santé, pour Agence des Systèmes d'Informations Partagés de Santé, est l'agence publique en charge des questions de santé et de numérique, ou de numérique en santé. L'ASIP Santé est donc une autre partie prenante en matière de protection des données de santé.

2.3.3.1 Statut et organisation

2.3.3.1.1 Statut

L'ASIP Santé (Agence des Systèmes d'Informations Partagés de Santé) se définit dans son rapport d'activités comme un « *opérateur du ministère de la Santé* » (77), mais c'est sous le statut de Groupement d'Intérêt Public (GIP) qu'elle a été créée en 2009. En effet, l'ASIP Santé est venue remplacer le GIP-DMP[36], dédié au Dossier Médical Personnel, et le GIP-CPS[37], consacré à la Carte de Professionnel de Santé (78). Conformément à l'arrêté du 18 septembre 2013 portant approbation de sa convention constitutive, l'ASIP Santé a été mise en place pour une durée de quinze ans, soit jusqu'en 2024 (78).

2.3.3.1.2 Gouvernance et organisation

En qualité de Groupement d'Intérêt Public (GIP), l'ASIP Santé est gouvernée par une assemblée générale, regroupant des représentants des institutions et organismes suivants :

- l'État,
- la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS),
- la Caisse nationale de solidarité pour l'autonomie. (78)

L'ASIP Santé, ainsi que son assemblée générale, est présidée par une « *personne qualifiée nommée par le ministre en charge de la santé* » (78). En outre, l'ASIP Santé est dotée d'un directeur, pour encadrer ses différentes activités et assurer la bonne gestion de l'agence. Depuis 2015, l'ASIP Santé est présidée par Patrice Legrand, administrateur civil honoraire, et est dirigée par Michel Gagneux, inspecteur général des affaires sociales (79).

En matière d'organisation, l'ASIP Santé se structure autour de services fonctionnels, de deux directions (à la stratégie et aux affaires médicales) et de trois pôles (Figure 7) :

- « urbanisation et services de confiance », en charge d'outils comme la Carte Professionnel de Santé (CPS) ou le Répertoire Partagé des Professionnels de Santé (RPPS),
- « projets e-santé », en charge des projets de systèmes d'information de santé,
- « appui aux acteurs et relations avec les clients ». (80)

[36] GIP-DMP : Groupement d'Intérêt Public – Dossier Médical Personnel
[37] GIP-CPS : Groupement d'Intérêt Public – Carte de Professionnel de Santé

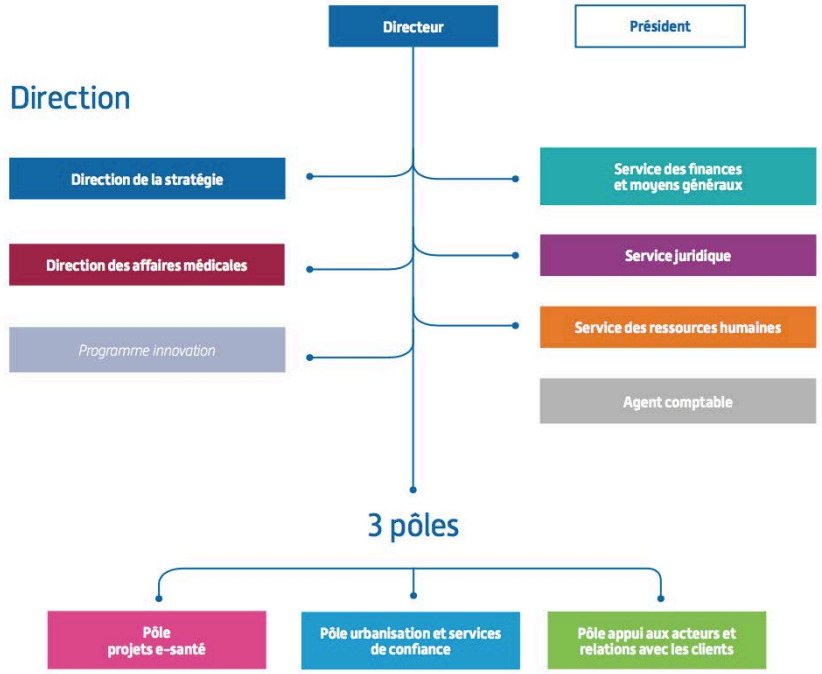


Figure 7. Organigramme de l'ASIP Santé (80)

2.3.3.2 Missions et activités

2.3.3.2.1 Missions

Issue de la fusion des Groupements d'Intérêt Public (GIP) en charge de la Carte de Professionnel de Santé et du Dossier Médical Personnel, l'ASIP Santé a été fondée avec comme ambition d'assurer la coordination des projets nationaux mêlant santé et numérique. L'ASIP Santé énonce ainsi sur son site internet ses trois principales missions :

- « *conduire des projets d'envergure nationale* »,
- « *créer les conditions de l'essor de la e-santé* »,
- « *déployer les usages en soutenant l'innovation*. » (81)

Par ailleurs, un Contrat d'Objectifs et de Performance (COP) signé avec l'État en janvier 2017, définit pour l'agence un objectif stratégique, quatre axes stratégiques et vingt-six objectifs opérationnels. Son objectif stratégique est ainsi de « *contribuer à l'amélioration de la coordination des prises en charge des patients dans les domaines sanitaire et médico-social dans le cadre de leur parcours de soins, et de favoriser la coopération entre les professionnels des champs sanitaire, médico-social et social grâce à l'usage de systèmes d'information adaptés à leurs besoins et un large recours aux technologies de l'information et de la communication* ».

Quant à ses quatre axes stratégiques, ils visent à :

- « *Définir et promouvoir le cadre national d'urbanisation des systèmes d'information de santé et du domaine médico-social* »,

- « *Assister les pouvoirs publics dans la conception et la mise en œuvre des programmes nationaux de santé et des projets de systèmes d'information de portée nationale* »,
- « *Favoriser la diffusion des usages et de l'innovation en santé numérique* »,
- « *Assurer l'efficience et la performance de l'agence* ». (82)

2.3.3.2.2 Activités

De ses missions, découlent un certain nombre d'activités dont s'occupe l'ASIP Santé. Parmi ces activités, et outre la coordination de projets comme la Carte de Professionnel de Santé et du Dossier Médical Personnel, l'ASIP Santé est impliquée ou gère différents projets comme :

- DIAPASON (Débit Intervenant Après le PArcours de SOi**N**s), pour faciliter le paiement, par carte bancaire, des patients dans les établissements de santé,
- le Cadre d'Interopérabilité des Systèmes d'Information de Santé (CI-SIS),
- diverses certifications,
- le label « *e-Santé logiciel maisons et centres de santé* »,
- le programme SI-Samu[38],
- etc. (83)

Mais en s'intéressant à l'informatique en santé, les activités de l'ASIP Santé couvrent également la question de la sécurité de ces systèmes d'informations et donc aussi celle de la protection de ces données. L'ASIP Santé est par exemple responsable de la cellule Accompagnement Cybersécurité des Structures de Santé (ACSS), participe à la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) ou encore conseille les hébergeurs de données de santé quant à leurs obligations légales (83). En matière d'hébergement des données de santé, l'ASIP Santé a également joué un rôle central dans leur régulation, en assurant le secrétariat des procédures d'agréments et ce depuis 2009 (84).

Aussi, de par ses larges missions et son expertise unique vis-à-vis du numérique en santé, l'ASIP Santé s'installe comme un acteur incontournable en matière de données de santé et leur protection.

2.4 Echange et partage de données en santé

Les professionnels de santé sont amenés, dans leur pratique quotidienne, à travailler avec différents interlocuteurs, qu'ils soient d'autres professionnels de santé ou non, et par conséquent à échanger et partager avec eux des données personnelles, dont des données de santé. Cette pratique collaborative a par ailleurs tendance à s'accroitre au sein des

[38] SI-Samu : Système d'Information du Samu (Service d'Aide Médicale Urgente)

professionnels de santé, avec l'essor des prises en charge multidisciplinaires. Dans cette partie, nous nous attacherons donc tout d'abord à décrire le périmètre de ces échanges et partages, avant de nous intéresser plus particulièrement à des exemples concrets de partage de données personnelles de santé.

2.4.1 Champs d'application et définitions

Le professionnel de santé, dans le cadre de son activité, est potentiellement amené à échanger avec de nombreux interlocuteurs. Cependant, en vertu de la protection des données de santé[39], l'échange et le partage des données personnelles de santé ne peuvent se faire que dans des cas précis, au profit de destinataires clairement désignés. L'arrêté du 25 novembre 2016 définit l'échange comme la communication d'« *informations à un ou plusieurs destinataires clairement identifiés par un émetteur connu* ». Quant au partage de données, il est entendu comme la mise à disposition d'information à des « *catégories de professionnels fondés à en connaître des informations* » (85).

2.4.1.1 Echange et partage avec d'autres professionnels de santé

Si l'échange et le partage de données personnelles de santé entre professionnels de santé est autorisé par la loi, grâce à la notion de secret professionnel partagé, ils sont néanmoins strictement encadrés, par l'article L. 1110-4 du Code de Santé Publique. Cet article dispose qu'un professionnel de santé peut « *échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social* » (43).

La notion d'« équipe de soin » est définie à l'article L. 1110-12 du Code de Santé publique, comme « *ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes, et qui :*

- *1° Soit exercent dans le même établissement de santé,* […] *ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale ;*
- *2° Soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge ;*

[39] cf. 2.1.2 Une protection multiple

- 3° *Soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée* » (86).

L'arrêté du 25 novembre 2016 illustre ce dernier point par quelques exemples d'équipes de soins répondant à ce critère : « *l'équipe de soins dans le cadre des projets « Territoire de soins numérique »* », « *l'équipe de soins dans le cadre de l'activité de régulation médicale dite partagée* », ou encore « *l'équipe de soins transfusionnelle* » (85). Quant aux « *structure[s] de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale* », le décret n°2016-996 du 20 juillet 2016 liste les organismes répondant à cette notion, tels que « *les groupements hospitaliers de territoire* », « *les fédérations médicales inter-hospitalières* » ou encore « *les maisons et les centres de santé* » (87).

Enfin, l'article L. 1110-4 du Code de la santé publique précise que le consentement préalable de la personne concernée est requis pour le partage d'informations entre des professionnels de santé ne faisant pas partie de la même équipe de soin. (43) Ainsi, au sein d'une maison ou d'un centre de santé, la loi n° 2011-940 du 10 août 2011 modifiant la loi HPST[40], précise que les informations d'un patient sont considérées comme « *confiées* […] *aux autres professionnels de santé de la structure* » à condition que le consentement du patient ait été recueilli et que les professionnels de santé adhérent au projet de santé (88).

En somme, même si les professionnels de santé sont tous soumis à l'obligation déontologique et légale du secret professionnel, l'échange et le partage d'informations entre professionnels demeurent précisément encadré par la loi, au nom du respect de la vie privée du patient.

2.4.1.2 Echange et partage avec d'autres interlocuteurs

Les professionnels de santé étant soumis au secret professionnel, ils ne sont pas, en principe, autorisés à partager des données avec d'autres interlocuteurs. Cependant, il existe plusieurs situations pour lesquelles un échange est autorisé par la loi. Tout d'abord, le décret n°2016-994 du 20 juillet 2016 précise également l'article L. 1110-4 du Code la santé publique, en énonçant une liste d'autres catégories de professionnels, des champs social et médico-social, pouvant participer à l'échange ou au partage d'informations relatives à un patient. Parmi ces professionnels, nous retrouvons par exemples les psychologues, les ostéopathes, les assistants de service social, etc (89).

Par ailleurs, il est disposé par l'article L. 161-29 du Code de la sécurité sociale que les professionnels de santé communiquent aux organismes d'assurance maladie les codes des « *actes effectués* » et des « *prestations servies* » (90). Aussi, afin de garantir la confidentialité de ces informations, « *seuls les praticiens-conseils et les personnels placés sous leur autorité*

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

ont accès aux données nominatives » et « *le personnel des organismes d'assurance maladie est soumis au secret professionnel* ».

Autre situation prévue par la loi, les déclarations obligatoires de certaines maladies, auxquelles sont tenues les professionnels de santé. Nous reviendrons plus en détails sur ce cas ultérieurement[41].

Enfin, il existe des tiers autorisés, qui sont habilités à recevoir des données personnelles de santé, mais seulement dans certains cas précis et pour un accès restreint et ponctuel. Parmi ces tiers autorisés, nous trouvons :

- les autorités judiciaires (dans le cadre d'une enquête préliminaire, d'une enquête de flagrance ou d'une instruction, par réquisition judiciaire ou commission rogatoire),
- les experts (nommés par une juridiction administrative ou civile, après consentement de la personne concernée). (61)

Notons ainsi que les tiers autorisés ne comprennent pas les employeurs, ni les assurances (61).

2.4.2 Exemples d'échange et de partage de données de santé

Afin d'illustrer l'échange de données de santé, nous détaillerons dans cette partie quatre exemples :

- la déclaration obligatoire de certaines maladies,
- la télémédecine,
- le Dossier Médical Personnel (DMP)
- la vente de médicaments en ligne.

2.4.2.1 Déclaration obligatoire de certaines maladies

L'article L. 3113-1 du Code de la santé publique énonce que certaines maladies doivent faire l'objet d'une « *transmission obligatoire de données individuelles à l'autorité sanitaire* », afin de répondre à des objectifs de santé publique et de sécurité sanitaire. Cette obligation de déclaration incombe à tous les médecins, responsables de services et laboratoires de biologie médicale, du secteur public comme du secteur privé.

L'enjeu en matière de protection des données personnelles est de garantir l'anonymat des personnes atteintes par ces maladies. Le processus d'anonymisation débute par le médecin déclarant, qui génère un code de seize caractères, sur la base du nom, du prénom, du sexe et

[41] cf. 2.4.2.1 Déclaration obligatoire de certaines maladies

de la date de naissance du patient. Ce code est le seul élément d'identification devant figurer sur le formulaire de déclaration. La déclaration est ensuite transmise à l'Agence Régionale de Santé (ARS), puis à l'Agence Nationale de Santé Publique (ANSP), ou Santé Publique France (anciennement l'Institut national de Veille Sanitaire (InVS)). La déclaration subit alors un second processus d'anonymisation par l'Institut. Seul le médecin déclarant dispose de la correspondance entre le code généré et l'identité du patient. Cette liste de correspondance doit être conservée pendant six mois, avant d'être, *in fine*, détruite. L'anonymisation est donc dite double et irréversible : double par les deux anonymisations successives du médecin déclarant et de l'ANSP et irréversible car l'ANSP ne peut retrouver l'identité du patient, seul le médecin déclarant en a la capacité. (61)

Ce premier exemple illustre donc la conciliation d'intérêts de santé publique avec le respect des droits individuels, à travers un système d'anonymisation double et irréversible. En effet, il y a un intérêt de santé publique à suivre certaines maladies, afin de prévenir des risques d'épidémies, mais aussi pour piloter et définir des politiques de santé publique. Néanmoins, cet intérêt collectif n'empiète pas sur l'intérêt individuel, puisque l'anonymat garantit le respect de la vie privée.

2.4.2.2 Télémédecine

La télémédecine est définie par l'article L. 6316-1 du Code de la santé publique comme « *une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication* » (91). Elle constitue donc un exemple intéressant, où des données personnelles de santé sont amenées à être échangées grâce aux nouvelles technologies. Le décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine, qui encadre cette pratique, liste cinq actes de télémédecine :

- « *la téléconsultation* »,
- « *la téléexpertise* »,
- « *la télésurveillance médicale* »,
- « *la téléassistance médicale* »,
- « *la réponse médicale qui est apportée dans le cadre de la régulation médicale* ». (92)

En termes de conditions de mise en œuvre, un acte de télémédecine requiert le « *consentement libre et éclairé* » du patient. Ce consentement est impératif pour l'acte de télémédecine en tant qu'acte médical, mais également pour l'acte de télémédecine en tant que traitement de données personnelles. Par ailleurs, chaque acte doit garantir « *l'authentification du professionnel de santé* », « *l'identification du patient* », « *l'accès des professionnels de santé aux données médicales du patients* » (92). L'authentification du professionnel participe ainsi des mesures de sécurité protégeant les données personnelles du patient. Enfin, chaque acte doit être mentionné dans le dossier médical du patient et faire l'objet d'une fiche d'observation, qui doit reprendre les informations suivantes : « *le compte rendu de la*

réalisation de l'acte », « *les actes et les prescriptions médicamenteuses* », « *l'identité des professionnels de santé* », « *la date et l'heure de l'acte* », « *le cas échéant, les incidents techniques* ». (92)

La CNIL précise en outre que les dispositifs utilisés dans une activité de télémédecine doivent présenter un haut niveau de sécurité, incluant les caractéristiques supplémentaires suivantes : *« la confidentialité des données, le chiffrement des données transmis, la traçabilité des connexions, l'intégrité des données et la mise en place d'un archivage sécurisé* ». Elle ajoute également que les logiciels ou les autres technologies utilisés doivent répondre aux référentiels de l'ASIP Santé. L'ensemble de ces dispositifs a pour ambition de répondre à l'obligation de sécurité que se doit d'assurer le responsable du traitement. Enfin, l'activité de télémédecine doit également faire l'objet d'une demande d'autorisation préalable auprès de CNIL. (61)

L'exemple de la télémédecine est donc intéressant car il s'agit d'une activité qui devrait tendre à se développer, avec l'essor des nouvelles technologies et la nécessité de répondre au phénomène de désertification médicale. Mais surtout, la télémédecine doit concilier l'intimité de l'examen médical et de la relation patient – médecin, avec les exigences techniques, notamment en termes de sécurité, afin de garantir le respect du secret médical et de la vie privée et la protection des données personnelles traitées au cours de cet acte.

2.4.2.3 Dossier Médical Partagé (DMP)

Initialement connu sur le nom de Dossier Médical Personnel, ce dossier médical informatique est désormais intitulé Dossier Médical Partagé (DMP). Le DMP a été créé en 2004, par la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie et est désormais disposé à l'article L. 1111-14 du Code de la santé publique. Non obligatoire, le Dossier Médical Partagé peut être créé pour tout bénéficiaire de l'assurance maladie (93). Plusieurs caractéristiques différencient ce Dossier Médical Partagé d'autres dossiers médicaux partagés. En effet, si ce dossier avait été initialement qualifié de « personnel », c'est bien parce que lié au patient, il est destiné à le suivre partout et tout au long de sa vie. De plus, ce dossier a été pensé comme un dossier où le patient en était le maître, en pouvant le consulter et en décider les accès.

Une fois inscrit dans la loi et disposé par le Code de la santé publique, le Dossier Médical Partagé a été autorisé par la CNIL et est mise en œuvre par la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés, ou CNAMTS (94). La CNAMTS est donc le responsable du traitement du Dossier Médical Partagé. Pour assurer le fonctionnement de ce projet, les données de santé collectées sont hébergées par un prestataire agréé, à savoir le groupement solidaire constitué entre des filiales d'ATOS Origin et de La Poste (95). La licéité de ce traitement repose sur le consentement du patient, préalable à toute création de dossier. Par ailleurs, outre le recueil de ce consentement, ce dossier exige bien entendu un haut niveau de sécurité pour les données hébergées, mais aussi des accès avec authentification des professionnels de santé (grâce à leur Carte de Professionnel de Santé) et traçabilité des accès

et des consultations. Comme les dossiers partagés des réseaux de santé, le Dossier Médical Partagé (DMP) impliquent des standards de sécurité stricts, mais à une échelle considérablement plus importante. L'exemple du Dossier Médical Partagé illustre donc bien le cas particulier des données de santé, où se mêlent des cadres juridiques différents, entre protection des données personnelles et secret médical.

2.4.2.4 Vente en ligne de médicaments

Bien que la vente en ligne de médicaments se soit développée plus tardivement en France que dans d'autres pays européens, cette pratique s'est désormais installée dans notre pays, depuis le 2 janvier 2013. Les articles L. 5125-33 à L. 5125-44 du Code de la santé publique encadrent ainsi la vente en ligne de médicaments, ou « *commerce électronique de médicaments* », qui est défini comme « *l'activité économique par laquelle le pharmacien propose ou assure à distance et par voie électronique la vente au détail et la dispensation au public des médicaments à usage humain et, à cet effet, fournit des informations de santé en ligne* » (96). Aussi, le pharmacien souhaitant vendre des médicaments sur internet doit se conformer aux dispositions du Code de la santé publique :

- adossement obligatoire du site de vente en ligne à une officine physique,
- autorisation du site de vente en ligne par le directeur de l'Agence Régionale de Santé (ARS),
- seuls peuvent être vendus en ligne les médicaments non soumis à prescription obligatoire,
- etc.

Toutefois, l'exercice de vente, et donc de dispensation de médicaments, sur internet impliquant le recueil de données personnelles, dont des données de santé, le pharmacien doit également veiller à respecter la loi en la matière afin de garantir la protection des données personnelles qu'il traite. Ainsi, conformément à la loi n°78-17 du 6 janvier 1978 modifiée et aux bonnes pratiques de dispensation définies par le Code de la santé publique, l'arrêté du 20 juin 2013 relatif aux bonnes pratiques de dispensation des médicaments par voie électronique précise que le pharmacien doit notamment veiller :

- à l'hébergement des données par un organisme agréé,
- à la sécurité et la confidentialité des données,
- au recueil du consentement,
- à l'information de la personne concernée, quant à la mise en œuvre du traitement et de ses droits.

Il est également précisé que les données de santé collectées lors de la dispensation en ligne de médicaments sont conservées pour une durée de trois ans (97).

La vente en ligne de médicaments est donc un autre exemple intéressant car le pharmacien souhaitant la mettre en œuvre doit répondre à des lois diverses : commerce électronique, Code de la santé publique et protection des données personnelles.

3 Etude de cas : le dossier pharmaceutique

Si la protection des données personnelles repose sur de grands principes théoriques, qu'en est-il en pratique ? Comment s'articule le triptyque du responsable du traitement, de la personne concernée et de l'autorité de contrôle de façon concrète ? Afin de tenter de répondre à ces interrogations, nous avons souhaité intégrer à nos travaux une étude de cas. Plusieurs possibilités s'ouvraient alors, mais nous avons décidé de nous intéresser au dossier pharmaceutique pour deux raisons. Tout d'abord, le dossier pharmaceutique s'est installé, depuis plusieurs années maintenant, dans le paysage officinal français, amenant les pharmaciens à intégrer ce nouvel outil dans leur pratique professionnelle quotidienne. Ensuite, ce projet de dossier pharmaceutique est unique, car outre le traitement de données personnelles, dont des données de santé, ce projet est mis en œuvre par une institution ordinale.

Pour ces différentes raisons, notre étude de cas porte donc sur le dossier pharmaceutique. Et après avoir présenté ce nouvel outil mis à la disposition des pharmaciens, nous essaierons de l'étudier sous l'angle de la protection des données personnelles. Enfin, nous conclurons en envisageant l'impact de futurs changements sur le dossier pharmaceutique et toujours au regard de la protection des données personnelles.

3.1 Le dossier pharmaceutique : un nouvel outil pour les pharmaciens

3.1.1 Historique

En 2004, le projet du Dossier Médical Personnel (DMP) voit le jour, à travers la loi n°2004-810 relative à l'assurance maladie. Cependant, écartés des discussions concernant le DMP, les pharmaciens réfléchissent, de leur côté, à un dossier comprenant les informations relatives aux traitements médicamenteux des patients, ces informations étant absentes du DMP. Ainsi, à l'occasion de la Journée de l'Ordre National des Pharmaciens, en novembre 2004, un atelier « Dossier patient personnalisé » est organisé, prémices du dossier pharmaceutique (DP). Dans la foulée, une mission de réflexion interne à l'Ordre est lancée, aboutissant à l'adoption du projet de dossier pharmaceutique par le Conseil National de l'Ordre des Pharmaciens (CNOP) au mois de septembre 2005. Quelques mois plus tard, en décembre, une étude de faisabilité est initiée. (98)

Le chantier du dossier pharmaceutique désormais ouvert, les travaux se poursuivent, et à la fin de l'année 2006, l'Ordre désigne l'entité chargée d'héberger les données du dossier pharmaceutique[42]. (98)

Alors que le projet du Dossier Médical Personnel stagne, celui du dossier pharmaceutique progresse de façon significative en 2007, avec l'adoption de la loi n°2007-127 du 30 janvier 2007. En effet, cette loi introduit un nouvel article au Code de la sécurité sociale, l'article L161-36-4-2 relatif au dossier pharmaceutique. Le DP entre ainsi dans la loi. (99)(100)

À la suite de cette naissance législative, la Commission Nationale de l'Informatique et des Libertés, par sa délibération n°2007-106 du 15 mai 2007, autorise une expérimentation de six mois du dossier pharmaceutique, dans six départements (Doubs, Meurthe-et-Moselle, Nièvre, Pas-de-Calais, Rhône, et Seine-Maritime) (101). En novembre 2007, puis en février 2008, saisie par le Conseil National de l'Ordre des Pharmaciens, la CNIL prolonge par deux fois cette expérimentation pour trois et six mois supplémentaires, respectivement (102)(103).

Le 2 décembre 2008, à l'issue de ces expérimentations, la CNIL, sur demande du Conseil National de l'Ordre des Pharmaciens**,** autorise la généralisation du dossier pharmaceutique, par sa délibération n°2008-487 du 2 décembre 2008 (103). Par ailleurs, quelques jours plus tard, le cadre juridique du dossier pharmaceutique se précise, avec la parution du décret n°2008-1326, le 15 décembre 2008 (98)(104).

En 2009, alors que la généralisation du dossier pharmaceutique débute, 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 HPST, transfère les articles relatifs au DMP et au DP du Code la sécurité sociale au Code de la santé publique (98).

À la suite de sa généralisation à l'échelle nationale, le dossier pharmaceutique a connu plusieurs extensions, afin d'intégrer de nouveaux acteurs. Ainsi, en 2011, les Pharmacies à Usage Intérieur, ou PUI, (*i.e.* les pharmacies des hôpitaux) ont eu accès au dossier pharmaceutique. Bénéficient également d'un accès, aux données anonymes, **«** *le ministre chargé de la santé, l'Agence nationale de sécurité du médicament et des produits de santé* [ANSM] *et l'Institut national de veille sanitaire*[43] [InVS] » (105). Puis en 2013, le décret n° 2013-31 est publié, autorisant l'accès de certains services hospitaliers (*e.g.* gériatrie, urgence, réanimation) au DP, dans le cadre d'une expérimentation (99)(106).

L'année 2013 a également été celle du changement d'hébergeur. En effet, suite au renouvellement de ce marché, un nouvel opérateur a remporté l'appel d'offres[44] (99)(107).

---

[42] cf. 3.2.1.5 Hébergement des données

[43] Depuis 2016, Agence National de Santé Publique (ANSP), ou Santé Publique France.

[44] cf. 3.2.1.5 Hébergement des données

Enfin, récemment, les médecins exerçant au sein d'établissements de santé ont été autorisés à accéder au dossier pharmaceutique, grâce à la loi du 26 janvier 2016 et le décret 2017-878 du 9 mai 2017 (108). Cependant, l'accès pour les pharmaciens biologistes, prévu dans le Projet de Loi de Financement de la Sécurité Sociale (PLFSS) 2018, a quant à lui été censuré par le Conseil Constitutionnel, en décembre 2017. Néanmoins, cette décision reposant sur une question de forme, l'Ordre a annoncé son intention de réitérer cette proposition d'extension, par l'intermédiaire d'un autre « *vecteur législatif* » (109).

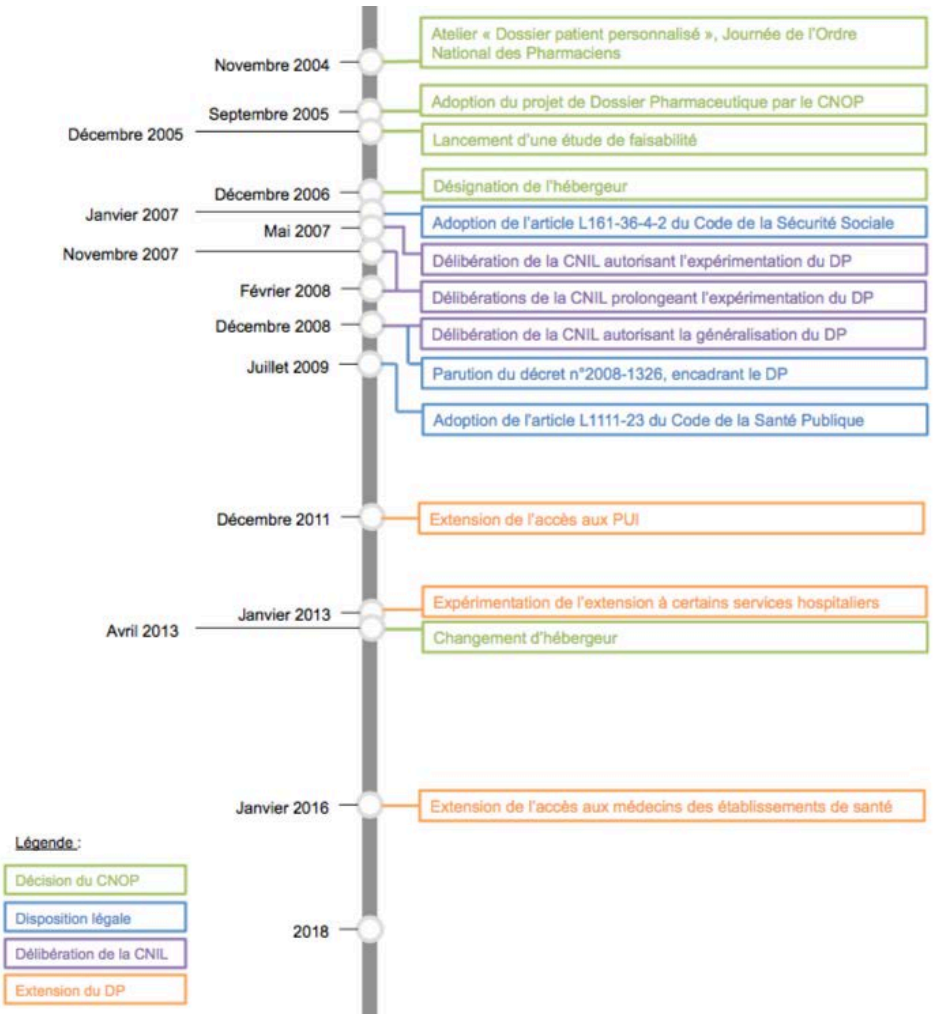


Figure 8. Chronologie du dossier pharmaceutique

Depuis plus de dix ans, le dossier pharmaceutique s'est donc considérablement développé (Figure 8). Quelques chiffres permettent de mieux apprécier son importance actuelle. Au 30 octobre 2017, 99,9% des officines françaises étaient raccordées au dossier pharmaceutique, soit plus 21 000 pharmacies. Cette excellente couverture du territoire atteint même 100% dans quatre départements sur cinq (et notamment en Meurthe-et-Moselle). Par ailleurs, outres les pharmacies, près de 380 établissements de santé sont également raccordés au dossier pharmaceutique. Enfin, toujours au 30 octobre 2017, 47,7 millions de Dossiers Pharmaceutiques étaient créés, dont 36,2 millions étaient actifs.

3.1.2 Objectif et cadre légal

Le dossier pharmaceutique est disposé par l'article L1111-23 du Code de la santé publique (110). Il est également encadré par le décret n°2008-1326 du 15 décembre 2008 (104). Enfin, la mise en œuvre du dossier pharmaceutique a été autorisée par la CNIL, par la délibération n°2008-487 du 2 décembre 2008 (103).

L'article L1111-23 du Code de la santé publique énonce l'ambition du dossier pharmaceutique. Le dossier pharmaceutique vise à « *favoriser la coordination, la qualité, la continuité des soins et la sécurité de la dispensation des médicaments* » (110). Mais derrière de cette ambition légale, l'objectif du dossier pharmaceutique est avant tout de lutter contre le risque iatrogène. La iatrogénie représente en effet un enjeu de santé publique important et dont la part liée aux médicaments est non négligeable. Par ailleurs, une enquête nationale, l'ENEIS[45], a montré que 51,2% des Effets Indésirables Graves (EIG) médicamenteux étaient évitables (111).

Le dossier pharmaceutique, en conservant l'historique médicamenteux des patients, permet donc aux pharmaciens d'éviter les interactions et les contre-indications, luttant ainsi contre le risque iatrogène. Par ailleurs, cet historique permet également aux pharmaciens de disposer d'informations supplémentaires afin de conseiller au mieux les patients et de remplir leur rôle vis-à-vis de la conciliation médicamenteuse.

Enfin, grâce à des nouvelles fonctionnalités, le dossier pharmaceutique participe également aux procédures d'alertes sanitaires, de rappels de lots, de ruptures d'approvisionnement, etc[46].

3.1.3 L'Ordre National des Pharmaciens

Différence notable du dossier pharmaceutique par rapport aux autres dossiers médicaux partagés, et notamment vis-à-vis du Dossier Médical Partagé (DMP), le dossier pharmaceutique a été porté et est toujours mis en œuvre par ses utilisateurs premiers, les pharmaciens, au travers de leur ordre professionnel : l'Ordre National des Pharmaciens.

3.1.3.1 Statut, organisation et fonction

Depuis 1945, l'Ordre National des Pharmaciens est l'institution ordinale regroupant et représentant les pharmaciens exerçant en France. Personne morale de droit privé, l'Ordre National des Pharmaciens opère néanmoins des missions de service public. L'article L4231-1 du Code de la santé publique dispose les quatre missions de l'Ordre National des Pharmaciens :

---

[45] ENEIS : Enquête Nationale sur les Effets Indésirables graves liés aux Soins
[46] cf. 3.1.5 Plusieurs Dossiers Pharmaceutiques

- « *assurer le respect des devoirs professionnels* »,
- « *assurer la défense de l'honneur et de l'indépendance de la profession* »,
- « *veiller à la compétence des pharmaciens* »,
- « *contribuer à promouvoir la santé publique et la qualité des soins* ». (112)

L'Ordre National des Pharmaciens est dirigé par le Conseil National de l'Ordre des Pharmaciens, ou CNOP, dont les missions sont fixées par l'article L4231-2 du Code de la santé publique (113). Ce Conseil National coordonne notamment les activités des différents conseils centraux des sections de l'ordre. En effet, l'Ordre National des Pharmaciens comprend sept sections, chargées de représenter les différents secteurs d'activités où peuvent exercer les pharmaciens : officine (section A pour les titulaires, section D pour tous les pharmaciens salariés), industrie (section B), distribution (section C), outre-mer (section E), biologie médicale (section F), hôpital (section H).

Les fonctions de l'Ordre National des Pharmaciens regroupent donc des activités variées, de l'inscription au tableau à la défense de la pharmacie devant les tribunaux, en passant par la gestion des plaintes au niveau des chambres de disciplines, le développement professionnel continu ou encore la mise en œuvre et la gestion du dossier pharmaceutique.

3.1.3.2 Gestion du dossier pharmaceutique

Depuis l'adoption du projet en 2005, l'Ordre National des Pharmaciens porte et gère le dossier pharmaceutique[47]. Et si l'hébergement des données est sous-traité à un prestataire agréé, c'est bien l'Ordre National des Pharmaciens qui est la personne morale chargée de la mise en œuvre du dossier pharmaceutique, conformément à l'article L1111-23 du Code de la santé publique (110).

Plus exactement, la maîtrise d'œuvre du dossier pharmaceutique est sous la responsabilité du Conseil National de l'Ordre des Pharmaciens. Et afin de faciliter la gouvernance de ce projet, le CNOP peut s'appuyer sur plusieurs comités :

- un comité d'éthique,
- un comité de suivi,
- un comité de pilotage. (114)

Outre ces comités, le Conseil National de l'Ordre des Pharmaciens a également initié plusieurs évaluations du dossier pharmaceutique, par l'intermédiaire d'études dédiées (*e.g.* l'étude DOPI-OFFI[48] ou l'étude IPADAM[49]) et d'un comité scientifique d'évaluation. (115)

---

[47] cf. 3.1.1 Historique

[48] DOFI-OFFI : Apport du Dossier pharmaceutique sur les interventions pharmaceutiques en pharmacies d'officine.

La maîtrise d'œuvre du Conseil National de l'Ordre des Pharmaciens repose également sur une direction de l'Ordre, à savoir la Direction des Technologies en Santé (DTS), qui assure la gestion quotidienne du dossier pharmaceutique et mène régulièrement des enquêtes de satisfaction sur les différentes fonctionnalités. (116)

Par ailleurs, le Conseil National de l'Ordre des Pharmaciens travaille, dans le cadre du dossier pharmaceutique, en lien étroit avec plusieurs partenaires, dont les autorités sanitaires, les associations de patients, les laboratoires pharmaceutiques, les établissements de santé, les Agences Régionales de Santé (ARS), etc.

Enfin, le dossier pharmaceutique peut également faire l'objet de contrôle de la part de deux entités indépendants : d'une part la CNIL, en matière de protection des données personnelles, et d'autre part la Cour des comptes. (114)

3.1.4 Fonctionnement

Le dossier pharmaceutique (DP) est donc un dossier électronique comprenant l'historique médicamenteux du patient, sur les quatre derniers mois. Cet historique médicamenteux comprend tout type de médicaments : avec ou sans ordonnance, remboursé ou non, délivré en officine ou en PUI. Non obligatoire, ce dossier peut être créé pour tout « *bénéficiaire de l'assurance maladie* », après recueil de son consentement. Le pharmacien officinal est « *tenu* » d'alimenter ce dossier lors de l'acte de dispensation, sauf opposition du patient. Quant au pharmacien exerçant dans une Pharmacie à Usage Intérieur (PUI), ils « *peuvent* » consulter et alimenter le dossier pharmaceutique. (110)

En termes de financement, le modèle économique du dossier pharmaceutique s'appuie sur trois sources différentes :

- l'Ordre National des Pharmaciens, par un financement provenant des cotisations ordinales,
- les autorités sanitaires, par des conventions-cadres.
- les autres utilisateurs (*e.g.* établissements de santé, industriels), par des conventions de service.

En 2016, le coût moyen du dossier pharmaceutique, par patient et par an, s'établissait à 7,3 centimes d'euros. (108)

3.1.5 Plusieurs Dossiers Pharmaceutiques

Outre son déploiement sur l'ensemble du territoire national, le dossier pharmaceutique a également vu son champ d'action élargi et ses usages étendus. En effet, aujourd'hui, cinq

---

[49] IPADAM : Interventions Pharmaceutiques À propos du Dossier pharmaceutique et de l'Auto-Médication.

fonctionnalités supplémentaires sont adossées au dossier pharmaceutique (DP) originel, dit DP-Patient :

- le DP-Rupture,
- le DP-Alerte,
- le DP-Rappel/Retrait,
- le DP-Vaccins,
- le DP-Suivi sanitaire.

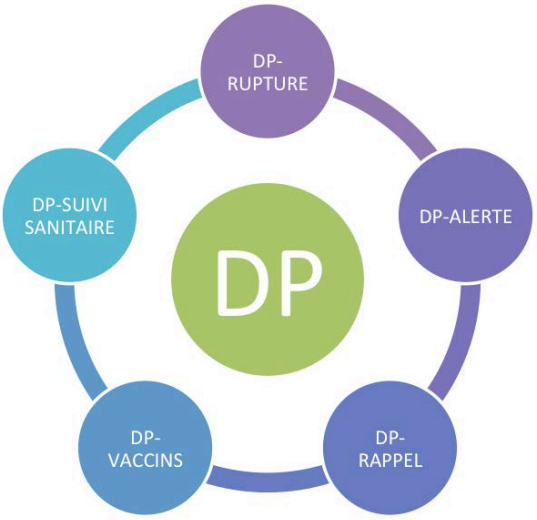


Figure 9. Les différentes fonctionnalités adossées au dossier pharmaceutique (adapté à partir de (108))

Le DP-Vaccins, tout d'abord, permet de séparer les vaccins des autres produits de santé dispensés, afin de conserver les données attenantes plus longtemps (21 ans). Disponible depuis septembre 2016, le DP-Vaccins joue un véritable rôle de santé publique, permettant au pharmacien d'assurer un suivi de la vaccination des patients (108). Cette fonctionnalité DP-Vaccin est encadrée par le décret n°2015-208 du 24 février 2015 et est autorisée par la délibération n°2015-452 du 17 décembre 2015 de la CNIL (117)(118).

Le DP-Suivi sanitaire est, quant à lui, l'outil permettant aux autorités publiques d'accéder aux données, anonymes, de dispensation. En effet, la loi n°2011-2012 a rendu possible l'accès au dossier pharmaceutique pour le ministère en charge de la santé, l'Autorité Nationale de Sécurité du Médicament et des produits de santé (ANSM) et l'Agence Nationale de Santé Publique (ANSP) (anciennement Institut national de Veille Sanitaire (InVS)) (105). Cette fonctionnalité du dossier pharmaceutique permet donc à ces entités d'avoir accès aux données anonymes de dispensation, organisées par zone géographique et par classe d'âge. La Direction Générale de la Santé (DGS) a notamment eu recours au DP-Suivi sanitaire dans le cadre d'un suivi des dispensations de contraceptifs oraux. (108)

Le DP-Rappel permet de faciliter les procédures de rappels de lots. Cette fonctionnalité est opérationnelle depuis 2009, grâce à une convention-cadre entre l'Afssaps[50] (désormais ANSM) et le CNOP, et des conventions de services entre l'Ordre et les laboratoires exploitants. La procédure de rappel de lot via le DP-Rappel implique l'ANSM, qui initie et valide l'alerte, et le pharmacien responsable du laboratoire exploitant, qui rédige et diffuse l'alerte. Cet outil se révèle donc particulièrement efficace et rapide, puisque les officines peuvent ainsi être prévenues en « *un quart d'heure maximum* ». (108)

Sur le même principe, le DP-Alerte permet aux autorités de santé, notamment la Direction Générale de la Santé (DGS) ou l'Autorité Nationale de Sécurité du Médicament et des produits de santé (ANSM), de diffuser des alertes, plus ou moins urgentes, et relatives à des produits de santé. Depuis 2016, les laboratoires exploitants peuvent également demander à utiliser ce système d'alerte, après accord de l'ANSM. (108)

Enfin, le DP-Rupture est lui aussi un système d'alertes, mais d'alerte « *remontantes* », c'est-à-dire en provenance des officines. De façon pratique, des alertes sont générées et transmises aux laboratoires exploitants, lorsque des médicaments sont déclarés « *manquants* » dans les pharmacies. Cette information « *de terrain* », permet ainsi aux laboratoires exploitants de mieux gérer les situations de ruptures de stock. (108)

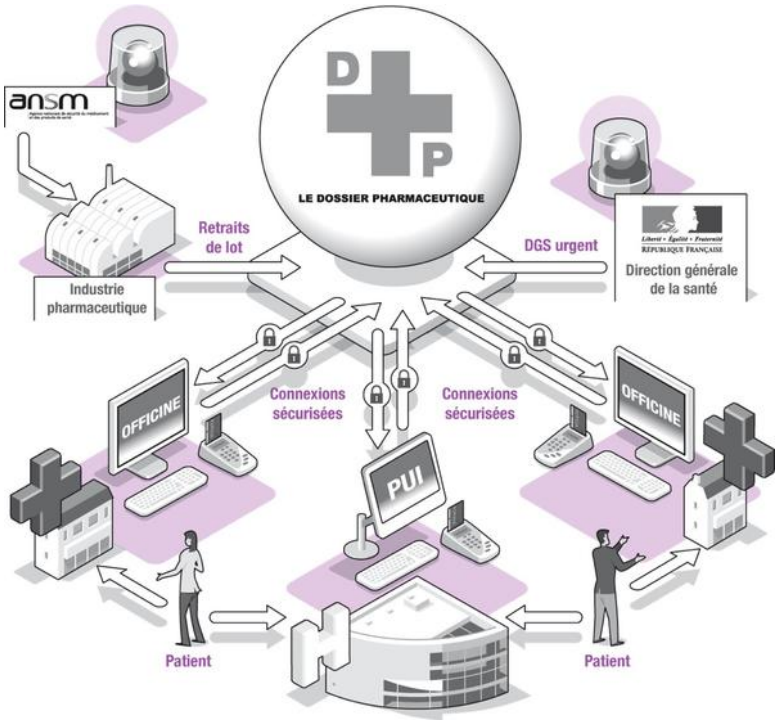


Figure 10. Circuit et interactions du dossier pharmaceutique (119)

[50] Afssaps : Agence française de sécurité sanitaire des produits de santé

Comme le montre la figure ci-dessus (Figure 10), le dossier pharmaceutique s'est donc totalement installé dans le paysage pharmaceutique français, en multipliant les usages et les interactions, afin de répondre à plusieurs enjeux de santé publique et de sécurité sanitaire.

3.2 Le dossier pharmaceutique au regard de la protection des données personnelles

3.2.1 Responsabilité du traitement

Conformément à l'article L1111-23 du Code de la santé publique, c'est au Conseil National de l'Ordre des Pharmaciens que revient la mission d'assurer la « *mise en œuvre du dossier pharmaceutique* » (110). En conséquence, la CNIL, dans sa délibération n°2008-487 du 2 décembre 2008, autorise le dossier pharmaceutique « *sous l'égide du CNOP* » (103). De même, au regard de la loi du 6 janvier 1978, le Conseil National de l'Ordre des Pharmaciens est considéré comme le responsable du traitement mis en œuvre dans le cadre du dossier pharmaceutique. À ce titre, le CNOP est tenu d'assurer le respect des principes de la protection des données personnelles, notamment en matière de sécurité des données et de durée de conservation.

3.2.1.1 Sécurité des données

En matière de sécurité tout d'abord, en tant que responsable du traitement, le Conseil National de l'Ordre des Pharmaciens se doit de « *prendre toutes précautions utiles* […] *pour préserver la sécurité des données* », selon l'article 34 de la loi n°78-17 du 6 janvier 1978 modifiée (18). Le CNOP a donc prévu plusieurs mesures afin de garantir la sécurité des données traitées.

Ainsi, l'accès au dossier pharmaceutique d'un patient est conditionné à la lecture de sa carte Vitale personnelle et de la Carte de Professionnel de Santé du pharmacien. Pour identifier le patient à partir de sa carte Vitale, un Numéro dossier pharmaceutique, ou NDP, est utilisé. Ce numéro est déterminé à partir du nom de famille, du prénom, du numéro de série de la carte du rang gémellaire (103). À titre de comparaison, le Dossier Médical Partagé, ou DMP, utilise un identifiant national de santé calculé (INS-C), également dérivé et calculé à partir de certaines données d'identité présentes sur la carte Vitale (NIR, jour de naissance, nom) (120).

Par ailleurs, les données d'identité des patients et leurs données de santé sont dissociées, *i.e.* séparées en deux bases de données. Toutes les données sont également dédoublées, afin d'être stockées sur deux sites distincts, mais bénéficiant tous deux de mesures visant à garantir la sécurité physique des infrastructures.

Enfin, toutes les données traitées sont bien évidemment cryptées et l'échange de données entre la plateforme d'hébergement et les officines est sécurisé grâce à des procédures d'authentification et du chiffrement (103).

3.2.1.2 Durée de conservation des données

Autre principe de la protection des données personnelles, la limitation de la durée de conservation[51] s'applique également au dossier pharmaceutique. Néanmoins, différentes durées de conservation s'appliquent selon le type de médicament, afin de répondre à différents risques et enjeux sanitaires. Ainsi, et conformément à l'article R1111-20-12 du Code de la santé publique, les informations de dispensation sont accessibles dans le dossier pharmaceutique pendant quatre mois. Puis ces données sont encore conservées pendant trente-deux mois supplémentaires, afin de pouvoir informer le patient en cas d'alerte sanitaire (121).

Deux catégories de médicaments font toutefois l'objet d'une conservation allongée. Toujours selon l'article R1111-20-12 du Code de la santé publique, les médicaments biologiques voient ainsi les informations relatives à leur dispensation accessibles pendant trois ans et cette durée est portée à vingt et un ans pour les vaccins. Dans ces deux cas précis, et à l'issue de ces durées respectives, les données demeurent encore conservées pendant trente-deux mois supplémentaires, comme pour les autres catégories de médicaments. (121)

En somme, différentes durées de conservation des données au sein du dossier pharmaceutique existent (Tableau V), afin de concilier enjeux sanitaires et principe de limitation de la durée de conservation.

Tableau V. Durées de conservations des données en fonction du type de médicaments au sein du dossier pharmaceutique (121)

	Durée de conservation avec accessibilité[1]	**Durée de conservation supplémentaire[2]**	**Durée de conservation totale**
Médicaments (non biologiques)	4 mois	32 mois	3 ans
Médicament biologiques	3 ans	32 mois	5 ans et 8 mois
Vaccins	21 ans	32 mois	23 ans et 8 mois

[1]Durée durant laquelle les données sont accessibles pour les pharmaciens (d'officine ou de PUI) et les médecins des établissements de santé.
[2]Durée durant laquelle les données sont conservées sans être accessibles, en cas d'alerte sanitaire

[51] cf. 1.2.1.2.5 Droit à la limitation du traitement

3.2.1.3 Information des patients

Comme tout autre responsable du traitement, le Conseil National de l'Ordre des Pharmaciens est tenu d'informer les personnes concernées du traitement de leurs données. Ce devoir d'information est d'autant plus important qu'il est nécessaire afin de recueillir le consentement du patient. Cependant, le défi lié du dossier pharmaceutique est, pour le CNOP, de s'assurer que l'information soit bien délivrée au patient, par l'intermédiaire des pharmaciens d'officine.

En effet, le pharmacien se doit d'informer le patient préalablement à toute création de dossier pharmaceutique. Ce devoir d'information répond à une obligation de la loi n°78-17 du 6 janvier 1978 modifiée, s'agissant de la protection des données personnelles. Le décret n°2008-1326 du 15 décembre 2008 dispose ainsi que le patient doit « *avoir pris connaissance des informations relatives à la création, l'utilisation et la clôture du dossier pharmaceutique* […]*, communiquées par le pharmacien d'officine* ». Par ailleurs, ce décret ajoute qu'à la suite de la création du dossier, le pharmacien d'officine doit remettre au patient une attestation de création. (104) Une brochure à destination du grand public a également été prévue par le Conseil National de l'Ordre des Pharmaciens et doit, elle aussi, être remise au patient lors de la création d'un dossier pharmaceutique. (122) Cette brochure permet au patient de conserver une documentation écrite présentant le dossier pharmaceutique, en complément de l'information orale délivrée par le pharmacien.

Par ailleurs, ce devoir d'information du pharmacien en amont de toute ouverture d'un dossier pharmaceutique peut également être rapprochée du devoir d'information qui incombe à tout professionnel de santé, conformément à l'article L. 1111-2 du Code de la santé publique. Cet article dispose en effet que « *toute personne a le droit d'être informée sur son état de santé* » et que cette information porte sur « *les différentes investigations, traitements ou actions de prévention* » (35). Or, d'une part le dossier pharmaceutique peut, indirectement, informer sur l'état de santé d'un patient, et d'autre part, ce dossier peut être perçu comme un outil de prévention des risques d'effets indésirables médicamenteux iatrogènes. Le devoir d'information du pharmacien s'inscrit donc également dans une lecture large de cet article L. 1111-2 du Code de la santé publique.

Enfin, le Conseil National de l'Ordre des Pharmaciens étant très soucieux de respecter les droits des patients, il a fait de cette question un « *impératif éthique* » (108). Aussi, le CNOP a-t-il noué un partenariat avec France Assos Santé[52], afin de veiller au respect des droits des patients. Ce partenariat s'est notamment traduit par une ligne téléphonique, la ligne Santé Info Droits, à destination des patients.

[52] auparavant Collectif Inter-associatif Sur la Santé (CISS).

3.2.1.4 Recueil du consentement du patient

Si l'information du patient est la première étape préalable à la création d'un dossier pharmaceutique, elle n'est pas la seule. En effet, le pharmacien d'officine est tenu de recueillir le « *consentement exprès* » du patient, conformément au décret n°2008-1326 du 15 décembre 2008 et à la loi n°78-17 du 7 janvier 1978 modifiée (104).

Par ailleurs, afin d'éviter des sollicitations multiples et inopportunes de patients réfractaires, l'autorisation de la CNIL précise que le refus d'ouvrir un dossier pharmaceutique est enregistré. En effet, le numéro du dossier pharmaceutique, ainsi que la date de refus, sont consignés, afin de ne pas proposer l'ouverture d'un dossier plus de trois fois (103). Il est également possible de faire part de son refus de création directement au Conseil National de l'Ordre des Pharmaciens. Une formulaire dédié est d'ailleurs disponible sur le site internet de l'Ordre (123). En 2015, ce sont ainsi plus d'un million et demi de refus de créations qui ont été recensés par le Conseil National de l'Ordre des Pharmaciens (116).

3.2.1.5 Hébergement des données

Si le Conseil National de l'Ordre des Pharmaciens est bien la personne morale chargée de mettre en œuvre le dossier pharmaceutique, il n'en assure pas directement l'hébergement des données. En effet, comme nous avons pu le voir précédemment[53], l'hébergement de données de santé est une activité spécifiquement réglementée et encadrée. Aussi le CNOP a-t-il décidé de confier cette activité d'hébergement à un prestataire extérieur. De 2006 à 2013 c'est ainsi la société SANTEOS qui avait été retenue pour cette prestation d'hébergement de données de santé. Mais au renouvellement du marché et après mise en concurrence, la société Docapost BPO, du groupe La Poste, a été choisie. Après un agrément en mars 2013, le transfert des données entre les deux hébergeurs s'est opéré en avril 2013. (124)

Enfin, outre ses obligations en matière de sécurité, de conservation et d'information, le Conseil National de l'Ordre des Pharmaciens, en qualité de responsable du traitement du dossier pharmaceutique, doit également veiller à ce que les patients puissent exercer leurs droits.

3.2.2 Droits des patients

En effet, dans le cadre du traitement de leurs données personnelles et de santé pour la mise en œuvre du dossier pharmaceutique, les personnes concernées par ce traitement ne sont autres que les patients. À ce titre, les patients bénéficient donc de plusieurs droits, disposés

[53] cf. 2.1.3 Un hébergement encadré

par la loi n°78-17 du 6 janvier 1978 modifiée : droit d'accès, droit de rectification, droit d'opposition et droit à l'effacement.

3.2.2.1 Droit d'accès

Comme pour tout traitement de données personnelles, la personne concernée, ici le patient, peut demander à avoir accès à ses données. Ce droit d'accès découle donc de la loi n°78/17 du 6 janvier 1978, mais aussi de l'article L. 1111-7 du Code de la santé publique, qui dispose en effet « *toute personne a accès à l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit* » (44). Le dossier pharmaceutique ne fait pas exception, et le patient est en droit de demander une copie de son dossier. Une copie des informations relatives à la dispensation de médicaments durant les quatre derniers mois, peut ainsi être demandée à tout pharmacien d'officine ou médecin d'un établissement de santé, sur présentation de la carte Vitale, voire d'une pièce d'identité, la copie sera alors remise directement au patient, accompagnée d'une attestation d'édition.

Pour accéder au contenu même du dossier pharmaceutique, il faut en revanche en faire la demande auprès du Conseil National de l'Ordre des Pharmaciens. Cette demande sera alors transmise par le CNOP au médecin du prestataire en charge de l'hébergement des données. Notons que dans ces deux situations, le droit d'accès est indirect, le patient devant impérativement passer par un tiers (*e.g.* pharmacien, CNOP) afin de demander l'accès à son dossier. Mais nous pouvons subodorer qu'à terme, un accès direct pour les patients soit mis en place, avec un accès en ligne, comme pour le Dossier Médical Partagé (DMP).

Enfin, il est également possible pour les patients d'accéder aux traces d'interventions sur leur dossier pharmaceutique. Ces traces d'intervention comprennent les actes « *de création, consultation, mise à jour, clôture, rectification ou édition d'une copie* » (125). La demande pour ce type d'informations doit, elle aussi, être adressée au CNOP. Afin de faciliter ces démarches, des formulaires sont disponibles en téléchargement sur le site de l'Ordre. (123)

3.2.2.2 Droit de rectification

Une fois le dossier pharmaceutique créé, le patient est en droit de demander la modification de ses données personnelles y figurant, en vertu du droit de rectification. Ce droit est d'ailleurs explicitement cité par le décret n°2008-1326 du 15 décembre 2008 (104). Cette demande peut s'effectuer auprès de tout pharmacien d'officine et permet ainsi au patient de rectifier les données personnelles le concernant.

3.2.2.3 Droit d'opposition

Le droit d'opposition, au sens du Règlement Général sur la Protection des Données, ne s'applique pas au dossier pharmaceutique, ce dernier reposant sur le consentement des personnes. Néanmoins, la mise en œuvre pratique du dossier pharmaceutique prévoit tout de

même pour le patient des possibilités d'« oppositions » ponctuelles. Le patient peut en effet s'opposer soit à l'inscription au dossier pharmaceutique de la dispensation de certains médicaments, soit à la consultation de son dossier par un pharmacien ou un médecin d'établissement de santé. Ces oppositions sont simplement à communiquer directement au pharmacien ou au médecin. Le patient se verra alors remettre une attestation de refus d'alimentation ou de refus de consultation, respectivement. (123)

Toutefois, le professionnel de santé (pharmacien ou médecin) confronté à ce type d'opposition se doit également de rappeler au patient l'intérêt du dossier pharmaceutique. La consultation et l'alimentation exhaustive du dossier pharmaceutique permettent en effet de prévenir certains risques potentiels d'effets indésirables iatrogènes. Ce devoir d'information fait au professionnel de santé est issu de l'article L. 1111-2 du Code de la santé publique, qui précise en effet que l'information délivré par le professionnel « *porte sur les différentes investigations, traitements ou actions de prévention qui sont proposés, leur utilité, leur urgence éventuelle, leurs conséquences* […] *et sur les conséquences prévisibles en cas de refus* » (35).

3.2.2.4 Droit à l'effacement

Enfin, afin de respecter le droit à l'effacement des patients, ces derniers peuvent en demander la clôture de leur dossier pharmaceutique. Il suffit pour cela d'en faire la demande à tout pharmacien d'officine, qui, une fois le dossier clôturé, remet une attestation de clôture. (123)

Par ailleurs, sans exercice actif du droit à l'effacement, tous les Dossiers Pharmaceutiques sont automatiquement clos après trois ans d'inactivité. En effet, l'article R1111-20-12 du Code de la santé publique précise, qu'à l'issue de la durée totale de conservation[54], les données sont détruites par l'hébergeur (121). Notons d'ailleurs que ces clôtures automatiques sont nettement plus importantes que les clôtures sur demande, 1,7 million contre 4 300, respectivement, en 2015 (116).

Droit d'accès, droit de rectification, droit d'opposition et droit à l'effacement, les différents droits disposés par la loi du 6 janvier 1978 modifiée sont donc applicables et appliqués dans le cadre du dossier pharmaceutique.

3.2.3 Contrôle de la CNIL

Dans le triptyque de la protection des données personnelles, et comme nous l'avons vu précédemment[55], la Commission Nationale de l'Informatique et des Libertés occupe le rôle

[54] cf. 3.2.1.2 Durée de conservation des données
[55] cf. 1.2.2.3 Le contrôle d'une autorité et 2.3.2 La CNIL

d'autorité de contrôle, une fonction qu'elle exerce donc également vis-à-vis du dossier pharmaceutique.

3.2.3.1 Autorisation et déclaration

Ainsi, la première mission de la CNIL a été de rendre des avis, puis de répondre aux demandes d'autorisations de mise en œuvre du dossier pharmaceutique. Et après avoir tout d'abord autorisé une expérimentation, prolongée à plusieurs reprises[56], la Commission Nationale de l'Informatique et des Libertés a officiellement autorisé « *les traitements de données personnelles permettant la mise en œuvre généralisé du dossier pharmaceutique* », par sa délibération n°2008-487 du 2 décembre 2008 (103).

Par ailleurs, outre cette autorisation initiale, la CNIL s'est également prononcée sur les évolutions et extensions du dossier pharmaceutique. La Commission a ainsi autorisé l'extension aux Pharmacies à Usage Intérieur (PUI) ainsi que l'allongement de la durée de conservation des données pour les médicaments biologiques et les vaccins, par ses délibérations n°2013-26 du 17 janvier 2013 et n°2015-452 du 17 décembre 2015, respectivement (126)(118). Plus récemment, la CNIL a également rendu un avis sur le projet de décret élargissant l'accès au dossier pharmaceutique aux médecins des établissements de santé, à travers sa délibération n° 2017-111 du 13 avril 2017 (127).

Outre ces diverses autorisations, la Commission Nationale de l'Informatique et des Libertés est également l'organisme auprès duquel les formalités de déclarations doivent être accomplies (103).

3.2.3.2 Contrôle et gestion des plaintes

Si la Commission Nationale de l'Informatique et des Libertés exerce une mission de contrôle *a priori*, notamment par l'intermédiaire du mécanisme d'autorisation, elle dispose également d'un pouvoir de contrôle *a posteriori*. Le « gendarme de la vie privée » assure donc la gestion des plaintes s'agissant de la protection des données personnelles. La CNIL a ainsi déclaré, en octobre 2016, avoir reçu plusieurs plaintes relatives au dossier pharmaceutique. Ces plaintes portaient sur un manquement bien précis, à savoir l'absence de recueil du consentement, plusieurs assurés sociaux dénonçant en effet l'ouverture de dossier à leur insu. En conséquence, la Commission a tenu à rappeler les règles relatives au dossier pharmaceutique, notamment en matière d'ouverture, et les différents droits dont disposent les patients[57] (125).

---

[56] cf. 3.1.1 Historique
[57] cf. 3.2.2 Droits des patients

La CNIL tient donc bien son rôle d'autorité de contrôle s'agissant du dossier pharmaceutique, tant *a priori* qu'*a posteriori*.

3.3 Le dossier pharmaceutique : perspectives et évolutions

Depuis plus de dix ans, le projet de dossier pharmaceutique a su évoluer, pour parvenir jusqu'à sa version actuelle. Mais il y a fort à parier que le dossier pharmaceutique va continuer son évolution, pour faire face tant à des changements extérieurs, comme le nouveau cadre juridique induit par le Règlement Général sur la Protection des Données, qu'à des améliorations internes, avec le développement de nouvelles fonctionnalités.

3.3.1 Impact du RGPD

Nous l'avons vu dans notre première partie[58], le cadre légal de la protection des données personnelles va prochainement évoluer, avec l'entrée en application, le 25 mai 2018, du fameux RGPD, le Règlement Général sur la Protection des Données, également connu sous son matricule officiel, le règlement n°2016-679. Ce nouveau règlement précise certaines notions, notamment celle de données de santé, mais introduit également de nouvelles obligations pour les responsables de traitement, ainsi que de nouveaux droits pour les personnes concernées. Aussi allons-nous tâcher dans cette partie de réfléchir à l'impact de ces nouvelles dispositions vis-à-vis du dossier pharmaceutique.

3.3.1.1 De nouvelles responsabilités

Parmi les nouvelles obligations faites aux responsables de traitement[59], l'une des plus symboliques est certainement la désignation d'un délégué à la protection des données, ou *DPO*, pour *Data Protection Officer* en anglais. Le Conseil National de l'Ordre des Pharmaciens, en qualité de responsable du traitement du dossier pharmaceutique, devra donc procéder à la nomination d'un délégué à la protection des données.

Par ailleurs, outre la création d'un registre des activités de traitement, le CNOP devra également revoir ses procédures afin d'implémenter l'obligation de notification des violations des données.

---

[58] cf. 1.1.2.3 Implémentation
[59] cf. 1.1.2.2.3 Nouvelles responsabilités

3.3.1.2 De nouveaux droits

En matière de protection des personnes concernées, le Règlement Général sur la Protection des Données, ou RGPD, a également introduit de nouveaux droits[60]. Parmi ces droits nouvellement créés, le plus emblématique est probablement le droit à l'effacement, ou droit à l'oubli. Disposé dans le RGPD, ce droit à l'effacement est toutefois déjà prévu dans le cadre du dossier pharmaceutique. En effet, il est d'ores-et-déjà possible pour les patients titulaires d'un dossier pharmaceutique de demander la clôture de ce dernier. En outre, et en tout état de cause, tous les Dossiers Pharmaceutiques sont clos après 36 mois d'inactivité[61].

Le Règlement Général sur la Protection des Données introduit également d'autres droits, tels que le droit à la limitation du traitement, le droit à réparation et le droit à la portabilité des données. Néanmoins, s'agissant de ce dernier, le droit à la portabilité des données, il ne saurait s'appliquer au dossier pharmaceutique, ce traitement n'étant réalisé que par un seul et unique opérateur. En revanche, les droits à réparation et à la limitation du traitement sont, *a priori*, bien applicables dans le cadre du dossier pharmaceutique.

3.3.2 Nouvelles fonctionnalités

Comme nous avons pu le constater précédemment[62], le dossier pharmaceutique s'est transformé au fil des années, en élargissant ses accès, en gagnant de nouvelles fonctionnalités et en maillant la quasi-totalité du territoire national. Dans la continuité de ces premières évolutions, le dossier pharmaceutique va, sans nul doute, poursuivre son développement. Et alors que sa couverture territoriale frôle déjà les 100%, ce sont de nouvelles fonctionnalités qui devraient faire évoluer le dossier pharmaceutique dans les prochaines années.

Depuis sa création, le dossier pharmaceutique n'a, en effet, cessé d'étendre son accès, directement ou à l'issue de phases d'expérimentation. Le dossier pharmaceutique s'est ainsi progressivement ouvert aux pharmaciens des Pharmacies à Usage Intérieur (PUI) et aux médecins des établissements de santé. Et nul doute que cette volonté d'élargissement des accès va continuer à jalonner l'actualité du dossier pharmaceutique. Ainsi, récemment, l'Ordre National des Pharmaciens avait proposé d'étendre aux pharmaciens biologistes l'accès au DP. Insérée au Projet de Loi de Financement de la Sécurité Sociale (PLFSS), cette disposition a toutefois été retoquée par le Conseil Constitutionnel en décembre 2017, pour des « *raisons de procédure* ». Néanmoins, dans un communiqué de presse, l'Ordre a réitéré son intention de rendre le dossier pharmaceutique accessible aux pharmaciens biologistes (109).

Autre catégorie de professionnels de santé, que d'aucuns souhaiteraient voir également bénéficier d'un accès au dossier pharmaceutique : les médecins libéraux. À la suite de leurs confrères hospitaliers, les médecins libéraux pourraient donc eux aussi, à l'avenir, consulter le dossier pharmaceutique (108). Ce besoin d'ouvrir le DP aux médecins libéraux a, par

---

[60] cf. 1.1.2.2.2 Nouveaux droits
[61] cf. 3.2.2.4 Droit à l'effacement
[62] cf. 3.1.1 Historique

exemple, été mentionné par l'Institut National du Cancer (INCa), dans son rapport sur le « Parcours de soins d'un patient traité par anticancéreux oraux » (128).

Néanmoins, ces différentes extensions, si elles représentent certainement une amélioration dans la coordination des soins, n'en demeurent pas moins une modification des finalités et des destinataires de ce traitement. Aussi, et comme elle le fit pour les précédentes extensions, la CNIL devra délibérer en amont, afin de veiller au respect de la loi n°78-17 du 6 janvier 1978.

Outre de nouveaux accès, le dossier pharmaceutique pourrait également contenir davantage d'informations. La question d'inclure la posologie des médicaments délivrés a ainsi été soulevée dans une publication de l'Ordre (108). De même, les actes du pharmacien correspondant, notion disposée par l'article L5125-1-1 A du Code de la santé publique, dans le cadre d'un protocole de soins, pourraient aussi intégrer le dossier pharmaceutique. Cependant, encore une fois, ces éventuelles modifications devront recevoir l'autorisation préalable de la CNIL.

L'Ordre National des Pharmaciens réfléchit également à simplifier les démarches pour les patients. Est ainsi envisagée la dématérialisation du consentement (requis préalable à l'ouverture de tout dossier pharmaceutique) (108). Néanmoins, nous pouvons anticiper que la mise en œuvre de cette dématérialisation devra être discutée bien en amont avec la CNIL, notamment compte tenu des plaintes reçues par plusieurs par patients, pour l'ouverture de dossiers à leur insu[63].

Une autre évolution majeure pour les patients dans l'exercice de leurs droits a également été avancée par l'Ordre : la possibilité, pour les patients, d'accéder à leur dossier pharmaceutique en ligne (108). Ce changement de modalité d'accès permettrait ainsi aux patients de disposer d'un accès direct (comme pour le Dossier Médical Partagé (DMP)) et non plus indirect comme actuellement[64]. Nul doute qu'une telle mise à jour faciliterait grandement l'exercice du droit d'accès pour les patients. Cependant, une telle mise à jour soulève également plusieurs questions, notamment en matière de sécurité, et devra donc, elle aussi, faire l'objet de discussions et d'échanges avec la CNIL.

Enfin, d'autres fonctionnalités sont également évoquées par l'Ordre National des Pharmaciens. Nous pouvons citer par exemple l'ouverture automatique de fenêtres dites *pop-up* pour les rappels vaccinaux ou encore le blocage de la dispensation de médicaments visés par une procédure de rappel de lot (108). Ces nouveautés du dossier pharmaceutique permettraient de renforcer son utilité, sans, *a priori*, exiger une consultation préalable de la CNIL.

[63] cf. 3.2.3.2 Contrôle et gestion des plaintes
[64] cf. 3.2.2.1 Droit d'accès

Force est de constater, que le dossier pharmaceutique va poursuivre son développement dans les prochaines années. Entre adaptations à des contraintes extérieures et améliorations internes, l'avenir du dossier pharmaceutique nous apparaît donc tout aussi riche que dynamique. Mais pour continuer de faire de ce projet une réussite, tant pour les professionnels de santé et les autorités sanitaires que pour les patients, le Conseil National de l'Ordre des Pharmaciens devra toujours veiller à la protection des données qui lui sont confiées, comme il a déjà su le faire jusqu'à présent.

Conclusion

Au cours de nos travaux, nous nous sommes attachés à décrire la protection des données personnelles au sein du système de santé en France, tant à travers des principes théoriques que sous le prisme d'une étude de cas, à savoir l'exemple du dossier pharmaceutique.

En effet, dans une première partie, nous sommes revenus sur la protection des données personnelles, en abordant son cadre juridique, en construction et évolution depuis plus de quarante ans, mais aussi les principes clés qui fondent cette protection. Nous avons également introduit les trois piliers de la protection des données personnelles : le responsable du traitement, la personne concernée et l'autorité de contrôle.

Dans une deuxième partie, nous nous sommes intéressés au cœur de notre sujet, c'est-à-dire la protection des données personnelles au sein de notre système de santé. Nous avons tout d'abord porté notre attention sur une catégorie particulière de données personnelles, les données de santé, qui, au regard de leur grande sensibilité, bénéficient de protections multiples, relevant de lois diverses. Puis, nous nous sommes penchés sur la responsabilité du traitement dans le système de santé et les diverses obligations qui en découlent, tant pour le professionnel que pour l'établissement de santé. Nous avons également abordé le rôle joué par d'autres parties prenantes, des patients à la CNIL, en passant par l'ASIP Santé. Enfin, nous avons clôturé cette deuxième partie en nous intéressant au partage des données de santé, une pratique de plus en plus nécessaire, dans des activités variées, mais une pratique particulièrement et spécifiquement encadrée.

Quant à notre troisième et dernière partie, nous l'avons consacré à une étude de cas, à savoir l'exemple du dossier pharmaceutique. Après une présentation de ce dossier partagé, outil unique car porté par les professionnels eux-mêmes, via leur institution ordinale, nous avons tâché d'étudier le dossier pharmaceutique sous l'angle de la protection des données personnelles, c'est-à-dire à travers le triptyque du responsable du traitement, de la personne concernée, ici le patient, et de l'autorité de contrôle. Enfin, avant de refermer cette étude de cas, nous nous sommes intéressés à quelques perspectives d'évolutions futures du dossier pharmaceutique, tant pour s'adapter à des contraintes extérieures, que pour s'améliorer en se dotant de nouvelles fonctionnalités internes.

Le système de santé doit donc parvenir à répondre à des obligations multiples, issues de cadres juridiques différents. D'une part, ce système s'inscrit dans un environnement spécifique, la santé, et doit ainsi répondre à un certain nombre de devoirs, notamment en matière de secret médical ou de respect de la vie privée. D'autre part, en traitant des données personnelles, et notamment celles des patients, le système de santé est également soumis au cadre légal de la protection des données personnelles.

Heureusement, dans un monde toujours plus connecté et dans un environnement toujours plus globalisé, le système de santé, de par sa structure et son fonctionnement, échappe aux nombreuses questions relatives à la territorialité et aux frontières. Car si nous

nous sommes concentrés dans nos travaux sur le cadre juridique français, voire européen, les lois relatives à la protection des données personnelles varient d'un pays à l'autre. Ainsi, alors qu'un certain nombre d'acteurs doivent composer, dans leurs activités internationales, avec des cadres juridiques nationaux variés, le système de santé n'est pas concerné par cette problématique.

Néanmoins, le système de santé n'échappe pas à d'autres défis. Tandis que le numérique occupe une place toujours plus ubiquitaire dans notre société, le secteur de la santé n'est pas épargné et voit lui aussi ses pratiques changer. Et si la France progresse dans cette direction, à son rythme, d'autres pays ont déjà intégré le numérique à leur système de santé dans des proportions nettement plus importantes. L'Estonie fait ainsi figure de référence en la matière, avec un usage du numérique dans la plupart des activités publiques : *e-identity*, *e-governance*, mais aussi *e-health*. L'e-santé estonienne regroupe ainsi deux programmes majeurs, les dossiers médicaux et les prescriptions électroniques, avec une implémentation quasi totale, puisque 99% des prescriptions sont numériques et 95% des données de santé sont numérisées (129). Aussi, dans un système de santé avec un tel poids du numérique, les enjeux liés à la protection des données personnelles s'en retrouvent démultipliés. Il est donc crucial que l'essor du numérique au sein de système de santé, soit accompagné par un niveau de protection des données personnelles constant et robuste.

Enfin, si nous nous sommes concentrés sur le système de santé dans le cadre de nos travaux, c'est tout le domaine de la santé qui présente des défis particuliers au regard de la protection des données personnelles. Les données de santé ne sont pas en effet l'apanage de ce système et ces dernières sont manipulées et traitées par d'autres acteurs et pour d'autres finalités. De façon non exhaustive, nous pouvons ainsi citer la recherche biomédicale, avec le rôle central du promoteur, qu'il soit public ou privé, la protection sociale, organisée, en France, autour de plusieurs caisses nationales, ou encore les applications de santé, ou de bien-être, qui envahissent notre quotidien et nos téléphones. Récemment, un amendement au projet de loi visant à mettre en conformité la loi française avec le nouveau Règlement Général sur la Protection des Données a proposé d'étendre la dérogation faite à l'Assurance Maladie de traiter des données personnelles de santé aux « *organismes d'assurance maladie complémentaire* » (130), preuve s'il en est que la question des données personnelles de santé est bien d'actualité. Autant d'autres défis pour la protection des données personnelles de santé donc, « *mais ceci est une autre histoire* », comme a écrit Rudyard Kipling.

Bibliographie

1. CNIL. Une donnée à caractère personnel, c'est quoi ? | Besoin d'aide | CNIL [Internet]. [cité 5 févr 2018]. Disponible à: https://www.cnil.fr/fr/cnil-direct/question/492

2. Boston Consulting Group (BCG). The Value of Our Digital Identity. 2012.

3. Gentot M. La protection des données personnelles à la croisée des chemins. Dans: La protection de la vie privée dans la société d'information. 2002.

4. Mattatia F. Le droit des données personnelles. 2e éd. Eyrolles; 2016.

5. OCDE. A propos de l'OCDE - OCDE [Internet]. [cité 11 janv 2018]. Disponible à: http://www.oecd.org/fr/apropos/

6. OCDE. Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. 1980.

7. Résolution de l'Assemblée Générale des Nations Unies n°45/95 sur les fichiers de données personnelles informatisées du secteur public et privé et des organisations internationales. 45/95 déc 14, 1990.

8. Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, adopté par le Comité des Ministres du Conseil de l'Europe le 26 septembre 1973, lors de la 224e réunion des Délégués des Ministres. 1973.

9. Résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, adopté par le Comité des Ministres du Conseil de l'Europe le 20 septembre 1974, lors de la 236e réunion des Délégués des Ministres. 1974.

10. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. janv 28, 1981.

11. Conseil de l'Europe. Parties à la Convention pour la protection des données [Internet]. Protection des données. [cité 11 janv 2018]. Disponible à: https://www.coe.int/fr/web/data-protection/convention108/parties

12. Forest D. Droit des données personnelles. Lextenso; 2011.

13. Conseil de l'Europe. Modernisation de la "Convention n° 108" sur la protection des données [Internet]. [cité 18 janv 2018]. Disponible à: https://www.coe.int/fr/web/portal/28-january-data-protection-day-factsheet

14. Convention de sauvegarde des droits de l'homme et des libertés fondamentales. avr 11, 1950.

15. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (version initiale). 78-17 janv 6, 1978.

16. 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. 95/46/CE oct 24, 1995.

17. Pourquoi une Charte des droits fondamentaux ? - Qu'est-ce que la citoyenneté européenne ? Découverte des institutions - Repères - vie-publique.fr [Internet]. 2016 [cité 9 janv 2018]. Disponible à: http://www.vie-publique.fr/decouverte-institutions/union-europeenne/ue-citoyennete/citoyennete-europeenne/pourquoi-charte-droits-fondamentaux.html

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

19. 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. 2004-801 août 6, 2004.

20. Commission européenne. « Protection de la vie privée dans un monde en réseau Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle », COM(2012) 9 final. 2012.

21. CEPD. Évolution historique du règlement général sur la protection des données [Internet]. Le Contrôleur Européen de la Protection des Données. [cité 8 janv 2018]. Disponible à: /data-protection/data-protection/legislation/history-general-data-protection-regulation_fr

22. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement Général sur la Protection des Données). 2016/679 avr 5, 2016.

23. Projet de loi relatif à la protection des données personnelles. déc 13, 2017.

24. Assemblée Nationale. Assemblée nationale - Société : protection des données personnelles [Internet]. [cité 23 avr 2018]. Disponible à: http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp

25. Règlement européen sur la protection des données personnelles : se préparer en 6 étapes [Internet]. [cité 18 janv 2017]. Disponible à: https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

26. In world first, Denmark to name a 'digital ambassador' [Internet]. 2017 [cité 23 avr 2018]. Disponible à: https://www.thelocal.dk/20170127/in-world-first-denmark-to-name-a-digital-ambassador

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

28. Türk A. Rapport n°218 sur le projet de loi, adopté par l'Assemblée national, 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, déposé le 19 mars 2003. p. 47.

29. Eynard J. Les données personnelles. Michalon; 2013.

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

31. Cornu G. Vocabulaire juridique. 11e éd. Presse Universitaires de France; 2016.

32. Code de la santé publique - Article R4127-35. Code de la santé publique.

33. Code civil - Article 1240. Code civil.

34. Arrêt du 13 mai 2014 de la Cour de justice de l'Union européenne. mai 13, 2014.

35. Code de la santé publique - Article L1111-2. Code de la santé publique.

36. CNIL. Le CIL et le futur délégué à la protection des données | CNIL [Internet]. [cité 19 janv 2018]. Disponible à: https://www.cnil.fr/fr/le-cil-et-le-futur-delegue-la-protection-des-donnees

37. Qu'est-ce qu'une autorité administrative indépendante (AAI) ? [Internet]. vie-publique.fr. [cité 16 janv 2018]. Disponible à: http://www.vie-publique.fr/decouverte-institutions/institutions/administration/organisation/etat/aai/qu-est-ce-qu-autorite-administrative-independante-aai.html

38. CNIL. Le fonctionnement | CNIL [Internet]. [cité 16 janv 2018]. Disponible à: https://www.cnil.fr/fr/le-fonctionnement

39. CNIL. Les missions | CNIL [Internet]. [cité 16 janv 2018]. Disponible à: https://www.cnil.fr/fr/les-missions

40. CNIL. La procédure de sanction de la CNIL | CNIL [Internet]. [cité 15 janv 2018]. Disponible à: https://www.cnil.fr/fr/la-procedure-de-sanction-de-la-cnil

41. CNIL. CNIL en bref 2017 [Internet]. 2017 [cité 16 janv 2018]. Disponible à: https://www.cnil.fr/fr/la-cnil-en-france

42. CNIL. 34e rapport. 2013 p. 51.

43. Code de la santé publique - Article L1110-4. Code de la santé publique.

44. Code de la santé publique - Article L1111-7. Code de la santé publique.

45. Code pénal - Article 226-13. Code pénal.

46. Ordre National des Médecins. Le serment d'Hippocrate | Conseil National de l'Ordre des Médecins [Internet]. [cité 22 janv 2018]. Disponible à: https://www.conseil-national.medecin.fr/le-serment-d-hippocrate-1311

47. Code civil - Article 9. Code civil.

48. Arrêt du 25 février 1997 de la Cour européenne des droits de l'Homme, affaire Z c. Finlande, requête n°22009/93. févr 25, 1997.

49. Arrêt du 6 octobre 2009 de la Cour européenne des droits de l'Homme, affaire C.C. c. Espagne, requête n°1425/06. oct 6, 2009.

50. Code de la santé publique - Article L1111-8. Code de la santé publique janv 1, 2019.

51. Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel. janv 12, 2017.

52. Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel. 2018-137 févr 26, 2018.

53. ASIP Santé. Hébergement des données de santé : nouveaux référentiels | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 22 janv 2018]. Disponible à: http://esante.gouv.fr/actus/services/hebergement-des-donnees-de-sante-nouveaux-referentiels

54. ASIP Santé. Certification des hébergeurs de données de santé | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 12 févr 2018]. Disponible à: http://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/procedures-pour-les-hebergeurs-de-donnees-de-sante

55. ASIP Santé. Evolution de la procédure d'agrément des hébergeurs de données de santé. 2017.

56. Qui sont les professionnels de santé ? - La protection de la santé Découverte des institutions - Repères - vie-publique.fr [Internet]. 2017 [cité 14 avr 2018]. Disponible à: http://www.vie-publique.fr/decouverte-institutions/protection-sociale/professionnels-sante/qui-sont-professionnels-sante.html

57. ASIP Santé, DSSIS. Mémento de sécurité informatique pour les professionnels de santé en exercice libéral - Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S). 2013.

58. Guide_Confidentialite-DonneesSante-janvier_2013.pdf.

59. Code de la santé publique - Article L6111-1. Code de la santé publique.

60. ASIP Santé. Établissements de santé : préparez-vous au règlement européen sur la protection des données personnelles (RGPD). 2017.

61. CNIL. Guide - Professionnels de santé. 2011.

62. Code de la santé publique - Article R1112-7. Code de la santé publique.

63. CNIL. Guide - La sécurité des données personnelles. 2010.

64. Code de la santé publique - Article R1110-2. Code de la santé publique.

65. 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). 2007-960 mai 15, 2007.

66. La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 30 janv 2018]. Disponible à: http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-0

67. ASIP Santé, DSSIS. Principes fondateurs - Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S). 2013.

68. ASIP Santé. Espace de publication | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 30 janv 2018]. Disponible à: http://esante.gouv.fr/pgssi-s/espace-publication

69. Code de la santé publique - Article L1111-8-2. Code de la santé publique.

70. Samarcq N, Briois S. Données de santé à caractère personnel, les enjeux de la diffusion des TIC. Expertise [Internet]. nov 2010 [cité 25 janv 2018]; Disponible à: http://www.afcdp.net/-Donnees-de-Sante-

71. CNIL. Traitement des données de santé : une logique de simplification et de responsabilisation accrue des acteurs | CNIL [Internet]. [cité 22 janv 2018]. Disponible à: https://www.cnil.fr/fr/traitement-des-donnees-de-sante-une-logique-de-simplification-et-de-responsabilisation-accrue-des

72. Délibération n° 2016-262 du 21 juillet 2016 portant modification de la méthodologie de référence pour les traitements de données personnelles opérés dans le cadre des recherches biomédicales (MR-001). 2016-262 juill 21, 2016.

73. CNIL. DARTY : sanction pécuniaire pour une atteinte à la sécurité des données clients | CNIL [Internet]. [cité 29 janv 2018]. Disponible à: https://www.cnil.fr/fr/darty-sanction-pecuniaire-pour-une-atteinte-la-securite-des-donnees-clients

74. Sfez B. Données de santé : des obligations de sécurité spécifiques pour les professionnels de la santé. [Internet]. [cité 29 janv 2018]. Disponible à: https://www.village-justice.com/articles/Donnees-sante-obligations-securite,15638.html

75. Décision 2013-037 du 25 septembre 2013 mettant en demeure X. 2013-037 sept 25, 2013.

76. Décision MED-2018-006 du 8 février 2018 mettant en demeure la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés. MED-2018-006 févr 8, 2018.

77. ASIP Santé. Rapport d'activités 2016. 2017.

78. 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 ». sept 18, 2013.

79. ASIP Santé. Nomination de M. Patrice LEGRAND | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 25 janv 2018]. Disponible à: http://esante.gouv.fr/actus/politique-publique/nomination-de-m-patrice-legrand

80. ASIP Santé. Notre organisation | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 25 janv 2018]. Disponible à: http://esante.gouv.fr/asip-sante/qui-sommes-nous/notre-organisation

81. ASIP Santé. Missions | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 25 janv 2018]. Disponible à: http://esante.gouv.fr/asip-sante/qui-sommes-nous/missions

82. Contrat d'objectifs et de performance entre l'Etat et l'ASIP Santé - 2016-2018 [Internet]. 2017 [cité 25 janv 2018]. Disponible à: http://esante.gouv.fr/actus/politique-publique/l-asip-sante-publie-son-contrat-d-objectifs-et-de-performance-cop

83. ASIP Santé. Services | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 25 janv 2018]. Disponible à: http://esante.gouv.fr/services

84. ASIP Santé. Hébergement des données de santé : pourquoi passer directement à la certification ? | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 19 févr 2018]. Disponible à: http://esante.gouv.fr/actus/politique-publique/hebergement-des-donnees-de-sante-pourquoi-passer-directement-a-la

85. Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins visée au 3° de l'article L. 1110-12 du code de la santé publique.

86. Code de la santé publique - Article L1110-12. Code de la santé publique.

87. Décret n° 2016-996 du 20 juillet 2016 relatif à la liste des structures de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale dans lesquelles peuvent exercer les membres d'une équipe de soins. 2016-996 juill 20, 2016.

88. Loi n° 2011-940 du 10 août 2011 modifiant certaines dispositions de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires. 2011-940 août 10, 2011.

89. Décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel. 2016-994 juill 20, 2016.

90. Code de la sécurité sociale - Article L161-29. Code de la sécurité sociale.

91. Code de la santé publique - Article L6316-1. Code de la santé publique.

92. Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine. 2010-1229 oct 19, 2010.

93. Code de la santé publique - Article L1111-14. Code de la santé publique.

94. Délibération n° 2016-258 du 21 juillet 2016 portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'un traitement de données à caractère personnel

dénommé « dossier médical partagé » (demande d'avis n° 16017107). 2016-258 juill 21, 2016.

95. Caisse nationale de l'assurance maladie des travailleurs salariés. Conditions d'utilisation - DMP [Internet]. [cité 30 janv 2018]. Disponible à: http://www.dmp.gouv.fr/mentions-legales

96. Code de la santé publique - Article L5125-33. Code de la santé publique.

97. Arrêté du 20 juin 2013 relatif aux bonnes pratiques de dispensation des médicaments par voie électronique. juin 20, 2013.

98. Parrot J. Le dossier pharmaceutique ou la réussite d'un projet mené par une profession. Trib Santé. 23 nov 2011;(32):101-9.

99. Alegre O. Le dossier pharmaceutique [Thèse pour le diplôme d'Etat de docteur en pharmacie]. Université Picardie Jules Verne; 2015.

100. Code de la sécurité sociale - Article L161-36-4-2. Code de la sécurité sociale.

101. Délibération n° 2007-106 du 15 mai 2007 portant autorisation des applications informatiques nécessaires à la mise en oeuvre de la phase expérimentale du dossier pharmaceutique. 2007-106 mai 15, 2007.

102. Délibération n° 2007-367 du 29 novembre 2007 portant prorogation de la phase expérimentale du dossier pharmaceutique. 2007-367 nov 29, 2007.

103. Délibération n° 2008-487 du 2 décembre 2008 portant autorisation des traitements de données personnelles permettant la mise en œuvre généralisée du dossier pharmaceutique. 2008-487 déc 2, 2008.

104. Décret n° 2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique. 2008-1326 déc 15, 2008.

105. Loi n° 2011-2012 du 29 décembre 2011 relative au renforcement de la sécurité sanitaire du médicament et des produits de santé - Article 23. 2011-2012 déc 29, 2011.

106. Décret n° 2013-31 du 9 janvier 2013 fixant les conditions de l'expérimentation relative à la consultation du dossier pharmaceutique par les médecins exerçant dans certains établissements de santé. 2013-31 janv 9, 2013.

107. Ordre National des Pharmaciens. Changement d'hébergeur pour le Dossier Pharmaceutique - Communications - Ordre National des Pharmaciens [Internet]. [cité 22 févr 2018]. Disponible à: http://www.ordre.pharmacien.fr/Communications/Communiques-de-presse/Changement-d-hebergeur-pour-le-Dossier-Pharmaceutique

108. Ordre National des Pharmaciens. Le Dossier Pharmaceutique. Les Cahiers de l'Ordre National des Pharmaciens. nov 2017;(12).

109. Ordre National des Pharmaciens. PLFSS 2018 : le Conseil constitutionnel censure l'ouverture du DP aux pharmaciens biologistes - Communications - Ordre National des

Pharmaciens [Internet]. [cité 23 févr 2018]. Disponible à: http://www.ordre.pharmacien.fr/Communications/Les-actualites/PLFSS-2018-le-Conseil-constitutionnel-censure-l-ouverture-du-DP-aux-pharmaciens-biologistes

110. Code de la santé publique - Article L1111-23. Code de la santé publique.

111. DGOS. Qualité de la prise en charge médicamenteuse - Outils pour les établissements de santé [Internet]. 2012 [cité 22 févr 2018]. Disponible à: http://solidarites-sante.gouv.fr/IMG/pdf/Guide_qualite_de_la_prise_en_charge_medicamenteuse.pdf

112. Code de la santé publique - Article L4231-1. Code de la santé publique.

113. Code de la santé publique - Article L4231-2. Code de la santé publique.

114. Ordre National des Pharmaciens. Gouvernance et conduite du DP - Le Dossier Pharmaceutique - Ordre National des Pharmaciens [Internet]. [cité 5 mars 2018]. Disponible à: http://www.ordre.pharmacien.fr/Le-Dossier-Pharmaceutique/Gouvernance-et-conduite-du-DP

115. Ordre National des Pharmaciens. Evaluation du DP - Le Dossier Pharmaceutique - Ordre National des Pharmaciens [Internet]. [cité 5 mars 2018]. Disponible à: http://www.ordre.pharmacien.fr/Le-Dossier-Pharmaceutique/Evaluation-du-DP

116. Direction des Technologies de Santé - Ordre National des Pharmaciens. Rapport d'activités 2015 - Le Dossier Pharmaceutique. 2015.

117. Décret n° 2015-208 du 24 février 2015 portant sur les durées d'accessibilité et de conservation dans le dossier pharmaceutique des données relatives à la dispensation des vaccins et des médicaments biologiques - Article 1. 2015-208 févr 24, 2015.

118. Délibération n° 2015-452 du 17 décembre 2015 autorisant la modification des traitements nécessaires à la mise en œuvre du dossier pharmaceutique portant allongement de la durée de conservation des données relatives à la dispensation des vaccins et des médicaments biologiques. 2015-452 déc 17, 2015.

119. Ordre National des Pharmaciens. Qu'est-ce que le DP ? - Le Dossier Pharmaceutique - Ordre National des Pharmaciens [Internet]. [cité 23 févr 2018]. Disponible à: http://www.ordre.pharmacien.fr/index.php/Le-Dossier-Pharmaceutique/Qu-est-ce-que-le-DP

120. Délibération n° 2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel. 2010-449 déc 2, 2010.

121. Code de la santé publique - Article R1111-20-12. Code de la santé publique.

122. Ordre National des Pharmaciens. Dossier Pharmaceutique : délivrez la nouvelle brochure patients - Communications - Ordre National des Pharmaciens [Internet]. [cité 9 mars 2018]. Disponible à: http://www.ordre.pharmacien.fr/Communications/Les-actualites/Dossier-Pharmaceutique-delivrez-la-nouvelle-brochure-patients

123. Ordre National des Pharmaciens. Vos droits : respect de la vie privée et confidentialité de vos données - Le Dossier Pharmaceutique - Ordre National des Pharmaciens [Internet]. [cité 9 mars 2018]. Disponible à: http://www.ordre.pharmacien.fr/Le-Dossier-Pharmaceutique/Vos-droits-respect-de-la-vie-privee-et-confidentialite-de-vos-donnees

124. CNOP. Communiqué de presse - Changement d'hébergeur pour le Dossier Pharmaceutique [Internet]. 2013. Disponible à: http://www.ordre.pharmacien.fr/Communications/Communiques-de-presse/Changement-d-hebergeur-pour-le-Dossier-Pharmaceutique

125. CNIL. Dossier pharmaceutique : quels droits pour les personnes ? | CNIL [Internet]. [cité 30 janv 2018]. Disponible à: https://www.cnil.fr/fr/dossier-pharmaceutique-quels-droits-pour-les-personnes

126. Délibération n° 2013-26 du 17 janvier 2013 autorisant les traitements de données personnelles permettant la mise en œuvre généralisée du dossier pharmaceutique dans les pharmacies à usage intérieur. 2013-26 janv 17, 2013.

127. Délibération n° 2017-111 du 13 avril 2017 portant avis sur un projet de décret relatif au dossier pharmaceutique (demande d'avis n° 16021765). 2017-111 avr 13, 2017.

128. Institut National du Cancer (INCa). Parcours de soins d'un patient traité par anticancéreux oraux. Institut National du Cancer (INCa); 2016 oct.

129. Enterprise Estonia. e-Health Records [Internet]. e-Estonia. [cité 20 févr 2018]. Disponible à: https://e-estonia.com/solutions/healthcare/e-health-record/

130. Assemblée nationale - Protection des données personnelles (n° 592) - Amendement n° 128 [Internet]. 592 févr 2, 2018. Disponible à: http://www.assemblee-nationale.fr/15/amendements/0592/AN/128.asp

FACULTE DE PHARMACIE UNIVERSITE DE LORRAINE

DEMANDE D'IMPRIMATUR

Date de soutenance : 05/06/2018

DIPLOME D'ETAT DE DOCTEUR EN PHARMACIE

présenté par : Paul BOLOT

Sujet :

Le cadre juridique des données personnelles et le système de santé en France

Jury :

Président : Mme Francine PAULUS, Maître de Conférences, Pharmacien
Directeurs : Mme Alexandrine LAMBERT, Maître de Conférences
Mme Julie LEONHARD, Maître de Conférences
Juges : M. René PAULUS, Pharmacien

Vu,

Nancy, le 15.05.2018

Le Président du Jury Directeur de Thèse

Mme PAULUS Mme Lambert

Mme LEONHARD

Vu et approuvé,

Nancy, le 16.05.2018

Doyen de la Faculté de Pharmacie
de l'Université de Lorraine,

Francine PAULUS

Vu,

Nancy, le 25 MAI 2018

Le Président de l'Université de Lorraine,

Université de Lorraine Le Président

Pierre MUTZENHARDT

N° d'enregistrement : 10299.

N° d'identification :

TITRE

Le cadre juridique des données personnelles et le système de santé en France

Thèse soutenue le 5 juin 2018

Par M. Paul BOLOT

RESUME :

La protection des données personnelles, ou données à caractère personnel, est un sujet éminemment contemporain et d'actualité, comme en témoigne l'entrée en application récente d'un nouveau règlement européen, le Règlement Général sur la Protection des Données, ou RGPD. Or, cette question juridique, cet enjeu de société touche également à notre système de santé, qui collecte et traite nos données personnelles, et notamment nos données de santé.

Aussi nos travaux ont-ils pour objectif de décrire la protection des données personnelles au sein du système de santé en France. Pour ce faire, et dans une première partie, nous nous attachons à décrire le cadre juridique de la protection des données personnelles. De ce cadre légal, composés de plusieurs textes législatifs, français et européens, émerge un triptyque composé du responsable du traitement, de la personne concernée par le traitement de ses données et de l'autorité de contrôle. Ce triptyque nous a servi de grille de lecture pour la suite de nos travaux.

En effet, dans une seconde partie nous nous sommes intéressés au cœur de notre sujet, à savoir la protection des données personnelles au sein de notre système de santé. Et après avoir décrit les particularités juridiques encadrant les données de santé, catégorie de données personnelles dites sensibles, nous avons observé le système de santé français sous l'angle du triptyque évoqué précédemment.

Enfin, nous avons souhaité consacré notre troisième et dernière partie à une étude de cas, afin d'appréhender de façon plus pratique les principes théoriques évoqués jusqu'à présent. Nous avons donc étudié le cas du dossier pharmaceutique, une nouvelle fois à travers le prisme de ce triptyque.

MOTS CLES : Données personnelles, système de santé, dossier pharmaceutique

Directrices de thèse	Intitulé du laboratoire	Nature
Mme Alexandrine LAMBERT Mme Julie LEONHARD		**Expérimentale** ☐ **Bibliographique** ☑ **Thème** ☐

Thèmes	1 – Sciences fondamentales 3 – Médicament 5 - Biologie	2 – Hygiène/Environnement 4 – Alimentation – Nutrition ⑥ **– Pratique professionnelle**