Les nouveaux cadres de la e-santé à l'ère du Big Data : quels enjeux pour la santé de demain ?

Mathilde Drouin

▶ **To cite this version:**

Mathilde Drouin. Les nouveaux cadres de la e-santé à l'ère du Big Data : quels enjeux pour la santé de demain ?. Sciences pharmaceutiques. 2018. dumas-02303934

HAL Id: dumas-02303934

https://dumas.ccsd.cnrs.fr/dumas-02303934

Submitted on 2 Oct 2019

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

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

UNIVERSITE DE PICARDIE JULES VERNE **U.F.R. de Pharmacie**

THESE
POUR LE DIPLÔME D'ETAT DE DOCTEUR EN PHARMACIE

Soutenue publiquement le jeudi 25 Octobre 2018

Par **Mathilde DROUIN**

Née le 28/01/1993 à Senlis (60)

Les nouveaux cadres de la e-santé à l'ère du Big Data : quels enjeux pour la santé de demain ?

JURY :

Monsieur Pascal SONNET, Président de thèse et Professeur à la Faculté de Pharmacie d'Amiens
Madame Catherine DEMAILLY, Directrice de thèse et Docteur en Pharmacie
Madame Selima ELLOUZE, Pharmacien Affaires Réglementaires spécialisée en Protection des données personnelles
Madame Angélique LEMAIRE-RIQUIER, Docteur en Pharmacie et Pharmacien titulaire

Thèse n°

SERMENT DE GALIEN

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

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

D'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.

De 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.

Listes des enseignants-chercheurs de la faculté des Sciences Pharmaceutiques d'Amiens

Année universitaire 2017 – 2018

Professeurs :

- *Mme Sylvie Baltora*
- *M. Michel Brazier*
- *M. Emmanuel Baudrin*
- *M. Jean-Marc Chillon*
- *M. Guillaume Decocq*
- *M. François Dupradeau*
- *M. Gilles Duverlie*
- *M. Eric Housieaux*
- *M. Saïd Kamel*
- *M. François Mesnard*
- *M. Laurent Metzinger*
- *M. Mickaël Naasila*
- *Mme Théodora Popovici*
- *M. Pascal Sonnet*

Maîtres de Conférences :

- *M. Jean-Charles Ahomadegbe*
- *Mme Judith André*
- *Mme Viviane Antonietti*
- *M. Jean-Paul Becker*
- *M. Christophe Bienaimé*
- *M. Etienne Brochot*
- *Mme Christine Cezard*
- *M. Olivier Chabrerie*
- *Mme Déborah Closset-Kopp*
- *Mme Catherine Demailly*
- *Mme Ophélie Fliniaux*
- *M. Xavier Fontaine*
- *M. Nicolas Guillaume*
- *M. François Helle*
- *Mme Alexandra Klimpt-Dassonville*
- *Mme Liabeuf-Estebanez Sophie*
- *M. Jonathan Lenoir*
- *Mme Elodie Lohou*
- *M. Gilles Mairesse*
- *M. Frédéric Marçon*
- *M. Romuald Mentaverri*
- *M. Roland Molinié*
- *M. Anthony Quero*
- *Mme Viviane Silva Pires*
- *Mme Isabelle Six*
- *Mme Aurélie Terrier-Lenglet*
- *M. Pierre Vanlemmens*
- *Mme Catherine Vilpoux*
- *Mme Patricia Zawadzki*

Remerciements

A **Monsieur Pascal SONNET** et **Madame Catherine DEMAILLY**,

Je vous remercie de l'honneur que vous me faites en ayant accepté d'être, respectivement, président et directrice de ma thèse ; ainsi que pour m'avoir suivi durant toutes mes années d'études de pharmacie au sein de la filière industrie. Pour votre disponibilité, vos connaissances ainsi que votre pédagogie, je tenais à vous exprimer toute ma gratitude. Soyez assurés de ma profonde reconnaissance.

A **Madame Selima ELLOUZE**,

Je vous remercie d'avoir accepté de faire partie de mon jury de thèse, mais surtout d'avoir suscité mon intérêt pour ce sujet cette année. Pour votre temps, votre esprit critique et votre partage de connaissances, je vous adresse mes remerciements les plus sincères et tout mon respect.

A **Madame Angélique LEMAIRE**,

Vous m'avez vu grandir et m'épanouir personnellement et professionnellement. Je ne vous remercierai jamais assez pour m'avoir embauché durant toutes ces années d'études et pour m'avoir transmis votre passion du métier. Je n'oublierai jamais votre pharmacie, toutes ces discussions et tous ces bons moments passés ensemble avec l'équipe. Une nouvelle page s'ouvre, et je suis heureuse que vous aillez accepté de faire partie de mon jury.

A **ma famille,**

Et plus particulièrement à mes parents, ma sœur et mon frère : merci de m'avoir toujours soutenue durant ces sept années d'études, parfois accompagnées de doutes, mais surtout de joie. Vous avez été exemplaires, et sans ce cadre équilibré, je ne serai pas devenue la femme et pharmacienne épanouie que je suis aujourd'hui. Merci de m'avoir encouragée sans cesse sur cette voie, qui aboutit aujourd'hui. Pour avoir toujours cru en mon potentiel, pour votre

patience face à mon caractère « changeant » en période d'examen, pour votre soutien dans toutes les étapes importantes de ma vie et pour tout votre amour au quotidien, merci. Après deux années plus que difficiles, le meilleur reste à venir, je vous aime tant.

A **mes amis et proches,**

Toutes ces années d'études n'auraient pas été les mêmes sans vous, et je ne serai pas la même personne sans chacun de ces précieux instants passés ensemble.

A mes amis de longues dates : Jean-Charles et Hugo, il s'en sera passé des choses depuis le bac à sable... Plus de 20 ans après, toujours les mêmes, ne changez pas. A mon binôme depuis toutes ces années : Sarah, cela n'aura pas toujours été facile, mais on l'a fait. Nina, Jérémy, Arnaud Jean-Baptiste, Antoine, Arthur, Valentin, Nolan, Fabien, Charlotte, Laura, Florian et Florient… c'est un pur bonheur d'avoir des amis exceptionnels comme vous et de se rejoindre « dans le 14^{e} » ou dans notre cher quartier de la muette.

A mes amis de la faculté et à tous les autres rencontrés au cours de soirées folles : Hugo, Chloé, Aymeric, Emma, Eve, Massiva, Cléa, Noëllyne... avec vous j'ai certes partagé les bancs de la fac mais bien plus encore. Merci pour votre bonne humeur quotidienne et tous ces bons moments à vos côtés : la suite reste à écrire. Une pensée toute particulière à mes 2 acolytes de toujours, Alix et « Belgique » : qui aurait dit 7 ans plus tôt que l'on passerait notre thèse le même jour ? Le hasard fait bien les choses.

A ma team ARIS : merci pour cette belle amitié qui s'est créée cette année et tous ces bons moments passés ensemble, que ce soit en cours, dans le RER, en festivals ou au cours de soirées improbables et de « fondues pour les nuls ».

A mes collègues qui sont devenus mes amis : la team Asco et la team Sanof, je suis heureuse de vous avoir rencontré et que vous fassiez partie de ma vie. En route pour de nouvelles vadrouilles et des « week-ends plus que parfaits ».

A **mes collègues de travail passés ou actuels**,

Je n'oublie aucun de ces moments passés à vos côtés. Merci pour tout ce que vous m'avez appris professionnellement et apporté humainement.

Table des matières

Liste des abréviations 10

Liste des Figures 12

Liste des Tableaux 12

Introduction 13

Partie 1 : Les nouvelles technologies au cœur de la santé 15

I- La santé connectée 15

1. La e-santé 15

1.1. Notions associées à la e-santé 15

1.2. Les enjeux de la e-santé 17

2. Les objets connectés et l'intelligence artificielle 19

2.1. Référentiel de bonnes pratiques de la Haute Autorité de Santé 21

2.2. Code de conduite européen Privacy en santé mobile 21

2.3. Référentiels en vigueur sur les objets connectés 23

2.3.1. Qualification des objets connectés 23

2.3.2. Qualification des données 25

2.3.3. Régimes applicables 26

2.3.4. Points de vigilance 27

2.4. L'intelligence artificielle 28

II- Les intervenants de la e-santé 30

1. Les utilisateurs 30

2. Les autorités de contrôle en présence 31

2.1. La CNIL 31

2.1.1. Organisation 32

2.1.2. Missions 33

2.1.2.1. Informer le grand public et les professionnels 34

2.1.2.2. Conseiller et réglementer 34

2.1.2.3. Accompagner la conformité 35

2.1.2.4. Contrôler et sanctionner 35

2.1.2.5. Liens avec les pouvoirs publics 36
2.1.2.6. Protéger les citoyens 37
2.2. L'ASIP Santé (Figure 4) 37
2.3. Les ARS 39
3. Stratégie nationale de santé 39
3.1. Stratégie nationale 2018-2022 39
3.2. Programme Territoire de Soins Numériques ou TSN 43
4. Les dernières avancées réglementaires 45
4.1. Loi pour une république numérique du 07/10/2016 45
4.2. Règlement général sur la protection des données personnelles 46
4.3. L'exemple des accords EU-US Privacy Shield 47
4.4. Règlement européen sur les dispositifs médicaux 47
4.5. Projet de loi relatif à la protection des données 48
III- Les données au cœur de la e-santé 49
1. Le Big Data 49
2. Les sources de ces données en santé 50

Partie 2 : Maitrise du traitement des données de santé sous l'égide du RGPD 52
I- Mettre en œuvre un traitement des données médicales en conformité avec le RGPD 52
1. Textes de références 52
2. Périmètre 53
3. Principes 56
4. Principaux objectifs 57
4.1. Repenser les données en plaçant les personnes concernées au cœur du traitement 58
4.1.1. Renforcer le droit à l'information 59
4.1.2. Renforcer le droit d'accès 59
4.1.3. Renforcer le consentement 59
4.2. Responsabiliser les acteurs 61
4.2.1. Traitement licite 61
4.2.2. Suppression des formalités et nouveaux outils 63
4.2.3. Sécurisation et confidentialité des données 65
4.2.4. Sous-traitance du traitement 67
4.2.5. Violations des données 67
4.2.6. Transfert hors Union Européenne 68
4.3. Crédibiliser les autorités 70

II- Maitriser le partage des données dans le cadre de la sécurisation des systèmes d'information de santé 71
III- Maitriser le cadre législatif et réglementaire de l'hébergement de données de santé..... 73
IV- Premiers résultats depuis l'instauration du RGPD 74

Partie 3 : place de la e-santé et du Big Data dans le système de soins de demain..... 75
I- Big Data et santé publique 75
1. Usage en pharmacovigilance..... 76
2. Usage en prévention et suivi des épidémies..... 78
3. Evaluation et anticipation de l'adhérence à un traitement 79
4. Individualisation de la prévention..... 80
II- Big Data et impact sur les métiers médicaux 81
1. L'ère de la médecine 6P 82
1.1. L'imagerie médicale..... 82
1.2. Le diagnostic, le suivi et la prévention 83
1.2.1. Diminution de l'errance thérapeutique à l'aide de l'intelligence artificielle 84
1.2.2. Amélioration de la prise en charge des cancers à l'aide de l'intelligence artificielle.... 85
1.2.3. Amélioration du suivi médicamenteux grâce à l'intelligence artificielle 87
1.3. La recherche 88
2. L'approche collaborative des professionnels de santé indispensable autours de la e-santé ... 90
3. Big Data et Pharmaciens..... 91
3.1. Digitalisation de l'officine..... 91
3.2. Nouveau business model pour l'industrie pharmaceutique 92
III- Big Data et éthique..... 94

Conclusion 97

Bibliographie..... 98

Liste des abréviations

ALD : Affection Longue Durée

ANAP : Agence Nationale d'Appui à la Performance

ANSM : Agence Nationale de Sécurité du Médicament et des Produits de Santé

ASIP Santé : Agence des Systèmes d'Information Partagées de Santé

CEPD : Comité Européen de la Protection des Données

CIL : Correspondant Informatique et Libertés

CNIL : Commission Nationale de l'Informatique et des Libertés

CNOM : Conseil National de l'Ordre des Médecins

CPS : Carte de Professionnel de Santé

CRPV : Centre Régional de Pharmacovigilance

CSP : Code de la Santé Publique

DGOS : Direction Générale de l'Offre de Soins

DM : Dispositif Médical

DMDIV : Dispositif Médical de Diagnostic In Vitro

DMIA : Dispositif Médical Implantable Actif

DMP : Dossier Médical Personnel (DMP)

DPO : Délégué à la Protection des Données ou Data Protection Officer

GAFA MS : Google, Apple, Facebook, Amazon, Microsoft et Samsung

HAS : Haute Autorité de Santé

IA : Intelligence Artificielle

IoT : Internet of Things

LAD : Logiciels d'Aides à la Dispensation

LAP : Logiciels d'Aides à la Prescription

LIL : Loi Informatique et Libertés

LNE-GMED : Laboratoire National de Métrologie et d'Essais - Groupement pour l'Evaluation des Dispositifs Médicaux

NIR : Numéro d'Inscription au Répertoire

NTIC : Nouvelles Technologies de l'Information et de la Communication

OCDE : Organisation de Coopération et de Développement Economiques

OMS : Organisation Mondiale de la Santé

ON : Organismes notifiés

PGSSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

PIA : Programme Investissement d'Avenir

RGPD : Règlement Général sur la Protection des Données

RT : Responsable de Traitement

SAFARI : Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus

SI : Système d'information

SNIIRAM : Système National d'Information Inter Régimes de l'Assurance Maladie

SNS : Stratégie Nationale de Santé

ST : Sous-traitant

TIC : Technologies de l'Information et de la Communication

Liste des Figures

Figure 1 : notions associées à la e-santé……page 16

Figure 2 : répartition des différentes catégories d'applications grand public……page 20

Figure 3 : Organigramme des directions et services de la CNIL……page 33

Figure 4 : Organigramme des directions et services de l'ASIP Santé en Décembre 2017……page 38

Figure 5 : Types de données recueillies sur le portail Epidémiologie-France……page 50

Figure 6 : Champ d'application du RGPD……page 55

Figure 7 : définition des échanges et partages de données à caractère personnel de santé……page 72

Figure 8 : le machine learning et l'anticipation de l'adhésion à un traitement……page 80

Liste des Tableaux

Tableau 1 : mécanismes d'autorisation de transferts de données à caractère personnel hors Union Européenne sous l'égide du RGPD…… page 69

Tableau 2 : sanctions administratives pouvant impacter le responsable de traitement ou le sous-traitant ne respectant pas les obligations du RGPD pour les données à caractère personnel, d'après les articles 58 et 83 du RGPD……page 70

Tableau 3 : exemples de délégations de tâches possibles……page 90

Introduction

Face aux diverses problématiques de santé publique actuelles, le système de santé français est à la croisée des chemins, et est en train d'être repensé et retravaillé avec les différentes parties prenantes de son système que sont les patients, les professionnels de santé et l'Etat. Imaginé en 1945, avec la création par ordonnance de la Sécurité Sociale, notre système national de santé est un système social solidaire qui repose sur la prise en charge des frais de santé des Français par l'Assurance Maladie. Mais, plus de 70 ans plus tard, le système est malmené et fait face à de nombreuses problématiques : surconsommation médicale pour certains et déserts médicaux pour d'autres, errance thérapeutique et diagnostique pour de nombreux patients, vieillissement de la population et augmentation des maladies chroniques, accentuation de la vétusté des infrastructures de santé suite aux coupes budgétaires à répétition, recrudescence des maladies… Le système s'essouffle, le coût de la santé évolue plus vite que les ressources qui lui sont attribuées. Mais notre système se doit de continuer à être performant tout en restant solidaire. Les patients se sentent davantage concernés par leur santé, et sont de plus en plus informés grâce aux nouveaux moyens technologiques et au développement d'Internet. Pourquoi le système de santé doit-il être repensé ? Les comportements changent, le système de santé doit s'adapter en conséquence à ces nouveaux enjeux, certains diraient se réinventer.

La consommation de soins n'étant pas une consommation comme les autres, les perspectives d'évolutions sont nombreuses et les mutations sont en cours. Et cela passe notamment par la réorganisation du parcours de soins dorénavant centré autour du patient ; par une médecine de parcours pour structurer les soins de ville ; par une meilleure coopération entre professionnels de santé avec le développement des maisons et pôles de santé et par la télémédecine et la santé connectée. Mais cette réorganisation se fait aussi en faisant de l'information et de la transparence sur la qualité des soins un levier fondamental de transformation au service des patients, grâce à l'ouverture des données de santé. Elle doit aussi donner une plus grande place à l'innovation en santé en faisant de la France un leader numérique au service de la santé au travers de trois axes principaux que sont : l'utilisation de la donnée et des approches numériques, l'automatisation de certains processus et la communication et le partage de données entre professionnels.

Les moyens technologiques actuellement en notre possession sont utilisés au service de l'information sur le patient et peuvent permettre de fluidifier la prise en charge de ces derniers et de gagner du temps, en limitant la perte d'informations et en améliorant la communication entre tous les professionnels. Les données de santé, créées via ces nouveaux outils technologiques et faisant partie intégrante de la santé connectée, connaissent une croissance exponentielle en France, et comme dans tous les pays du monde : on parle de « Big Data ». Il est prévu que, d'ici 2020, leur volume atteigne 2,3 milliards de giga-octets et que le volume de données produites dans le monde soit multiplié par 44 (1). Ces données, toujours plus nombreuses et disparates, proviennent de sources très variées (les essais cliniques, les dossiers médicaux partagés entre professionnels, les objets connectés, les bases de données de l'Etat, etc.). Utilisées à bon escient et de manière sécurisée, elles constituent un véritable levier pour assurer la sécurité sanitaire, un parcours de soins efficient et une médecine plus personnalisée. Employées dans le développement de l'intelligence artificielle, les données constituent un réel levier pour repenser la prise en charge des malades.

Dans le cadre de ma thèse d'exercice, j'ai choisi de développer les problématiques associées à la santé connectée et à l'hébergement des données de santé : comment le caractère confidentiel de ces dernières est-il respecté ? Quelles sont les nouvelles réglementations en vigueur afin d'assurer un traitement licite de ces dernières, en vertu du droit des patients ? Quelles sont les perspectives d'évolutions de prise en charge des patients et de leurs pathologies via l'analyse de leurs données de santé et les nouvelles technologies en notre possession à l'ère du numérique ? Actuellement dans une période de transformation et de révolution digitale en santé, le modèle de prise en charge des patients évolue.

Partie 1 : Les nouvelles technologies au cœur de la santé

I- La santé connectée

1. La e-santé

1.1. Notions associées à la e-santé

La « e-Health » ou « e-santé », également appelée « santé numérique » ou « information numérique sur la santé », est un terme utilisé pour désigner les différents domaines de la santé qui utilisent les technologies de l'information et de la communication (ou « TIC ») et nouvelles technologies de l'information et de la communication (ou « NTIC »), via l'utilisation des smartphones, tablettes, ordinateurs, podomètres, ou tout autre appareil connecté ; ainsi que l'ensemble des dispositifs technologiques de pointe qui viennent aider les professionnels de santé à mesurer et analyser nos actes au quotidien.

Terme apparu à la fin des années 90, il s'est désormais banalisé avec l'essor d'internet dans les années 2000. L'Organisation Mondiale de la Santé (OMS) vient la définir en tant que l'ensemble des « services du numérique au service du bien-être de la personne » via « l'utilisation des outils de production, de transmission, de gestion et de partage d'informations numérisées au bénéfice des pratiques tant médicales que médico-sociales ». Cette notion s'est construite autour de la notion de santé définie par l'OMS en 1946 : « la santé est un état de complet bien-être physique, mental et social, et ne consiste pas seulement en une absence de maladie ou d'infirmité ».

Concomitante avec la transformation digitale de notre société (c'est-à-dire ce qui se rapporte au numérique et qui correspond au passage des données analogiques en numérique), la santé numérique est un secteur économique qui a émergé avec l'arrivée massive des nouvelles technologies en santé, ayant permis la production de nouveaux produits, services, techniques et systèmes, permettant de modifier notre façon de travailler. Au sein de la santé numérique, diverses notions sont retrouvées (*cf. Figure 1*) :

- les actes de santé réalisés à distance, via la télémédecine ainsi que la vente de médicaments en ligne via les pharmacies en ligne ;

- les dossiers médicaux numériques, qui correspondent à l'ensemble des informations de santé pour chaque patient disponible sous forme dématérialisée (via le numérique) ;
- la démocratisation de la santé mobile ou « m-santé », qui correspond d'après la définition apportée par l'OMS, aux « pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que les téléphones portables, systèmes de surveillance des patients, assistants numériques personnels et autres appareils sans fil » ;
- les logiciels d'aides à la prescription (LAP) et les logiciels d'aides à la dispensation (LAD), qui sont des programmes d'ordinateurs qui permettent de proposer aux professionnels de santé des recommandations en termes de santé. De nos jours, ces logiciels ont également une composante d'intelligence artificielle (ou « IA »), c'est-à-dire une capacité à apprendre par expérience ;
- la sécurisation, certification des identités et des échanges de données de santé.

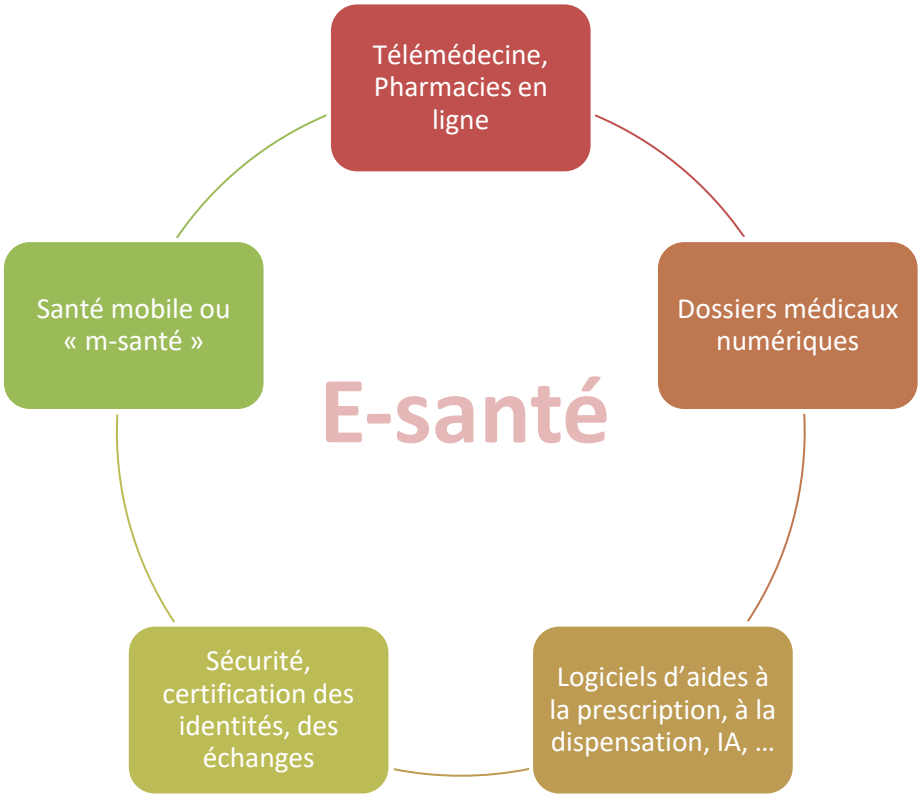

Figure 1 : notions associées à la e-santé

1.2. Les enjeux de la e-santé

La e-santé semble être une solution de plus en plus pertinente pour répondre aux nombreux défis que doit relever le système de santé français, mais a demeuré longtemps sous-exploitée, et ce pour l'ensemble des pays de l'OCDE (Organisation de Coopération et de Développement Economiques) (2). Le rapport 2016 de l'OMS sur la e-santé vient démontrer que l'Europe réalise de gros progrès dans ce secteur, mais qu'il persiste toutefois un écart entre la capacité de faire des nouveaux outils technologiques de plus en plus perfectionnés, le cadre juridique qui tend à s'harmoniser et l'adhésion des consommateurs plutôt lente : la technologie a dépassé la demande des consommateurs.

Dans ce contexte, il est attendu du développement de la e-santé des répercussions notables sur l'organisation de notre système de santé, la qualité des soins proposés, le coût des pratiques professionnelles, ainsi que sur le comportement des patients. Les objectifs de la santé numérique résultent d'un impératif de soins et de santé publique. Il est nécessaire de :

- modifier la manière de travailler en santé, en utilisant la dématérialisation des supports. Il faut permettre l'accès en ligne par les patients à leurs données via l'open data sécurisé. Les nouvelles technologies permettent d'atteindre une plus grande égalité d'accès aux soins, en atteignant des zones éloignées et des personnes ayant des difficultés pour se soigner et/ou se déplacer ;
- permettre aux professionnels de santé de mutualiser leurs activités et de partager les informations, en utilisant les différents canaux numériques existants afin d'être le plus efficient possible et d'assurer la durabilité du système de santé français. Cela se fait déjà à petite échelle, avec les centres antipoison et de toxicovigilance : ils sont à l'heure actuelle très peu nombreux mais très efficaces, via le réseau hôpital/centre antipoison très connecté ;
- faire de l'information et de la transparence sur la qualité des soins un levier fondamental de transformation : l'objectif de l'ouverture des données de santé et de faire des patients des acteurs éclairés sur leur pathologie et sur le choix de leur propre parcours de santé, et donc donner aux patients les outils pour prendre le contrôle de leur santé ;

- promouvoir la prévention sanitaire, via le maximum de canaux de communications possibles : la e-santé permet d'augmenter la portée des actions et des messages diffusés auprès des patients. De plus, la mise à disposition de certaines applications ou d'outils technologiques d'auto-évaluation et de télédiagnostic, permettrait de dépister des maladies chroniques à un stade plus précoce et d'en limiter la gravité.

Repenser l'organisation des soins autours du numérique va permettre de faire face à la transformation des besoins médicaux. Avant les années 50, les décès étaient principalement dus aux maladies aiguës. Dorénavant, en raison de l'allongement de l'espérance de vie, les patients sont davantage atteints de maladies chroniques, qu'il faut prendre en compte dans la prise en charge médicale. Il faut davantage réaliser une prise en charge personnalisée et optimale, avec des professionnels de santé qui travaillent de manière coordonnée autour du patient. Les différentes données de santé collectées via la e-santé permettent une adaptation de cette prise en charge, car prenant en considération l'ensemble des informations sur le patient, et non plus uniquement ce qu'il peut indiquer en consultation.

Mais, au-delà des avancées techniques et technologiques, le développement du numérique et de la e-santé posent la question du contrat social. Pour être efficaces, les professionnels de santé doivent être formés aux TIC et aux nouveaux modes d'exercice de leur métier, et se préparer à leur nouvelle relation avec les patients. La disruption numérique, ajoutée aux inégalités territoriales en termes de couverture sanitaire et d'infrastructures, produit de fortes discriminations : l'usage de la e-santé est en lui-même un enjeu sociétal. Il faut donc construire et penser la e-santé autour et avec le patient, en fonction de ses besoins, de son adhésion aux nouveaux moyens et méthodes de santé et de son éducation thérapeutique. Les solutions de e-santé contribuent à davantage impliquer le patient dans son parcours de soin, auparavant plus passif, et le rendre plus responsable de sa santé.

2. Les objets connectés et l'intelligence artificielle

Le développement des outils issus de la technologie digitale s'est fortement accentué ces dernières années, et a révolutionné notre approche en santé. L'utilisation massive des smartphones et des appareils connectés tels que les tablettes, montres connectées, ordinateurs etc. a donné naissance à un nouveau concept qu'est la santé mobile, plus connue sous le nom de « m-santé ».

Elle est définie par l'OMS comme recouvrant « les pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, systèmes de surveillance des patients, assistants numériques personnels et autres appareils sans fil ». La m-santé regroupe un grand nombre de produits et services très variés : y sont retrouvés par exemple les lecteurs de glycémie connectés (considérés comme dispositifs médicaux), les applications sur les interactions médicamenteuses, mais également les applications bien-être et celles à vocation médicale. Ces dernières ont connu un essor majeur durant les années 2010 : le volume mondial des applis de m-santé est passé de 6 000 en 2010 à 100 000 en 2013, et 165 000 en 2015 (3).

Le développement de cette m-santé s'explique et s'articule autour de plusieurs raisons : elle permet l'amélioration de la qualité des soins, tout en facilitant son accès dans les zones de désertification médicale, et permet également de prévenir certaines maladies, tout en permettant une diminution notable des coûts liés à la prise en charge des patients (4). Les applications en santé sont utilisées à la fois par les patients, mais également par les professionnels de santé. Depuis 4 ans, un renforcement de l'utilisation professionnelle du smartphone est ainsi observé et 65% des médecins interrogés s'en servent pour prescrire, s'informer sur un médicament ou encore une stratégie thérapeutique (5). Pour le grand public, 2 types d'applications sont principalement utilisées : les applications dédiées au bien-être et celles dédiées aux pathologies et traitements (*cf. Figure 2*).

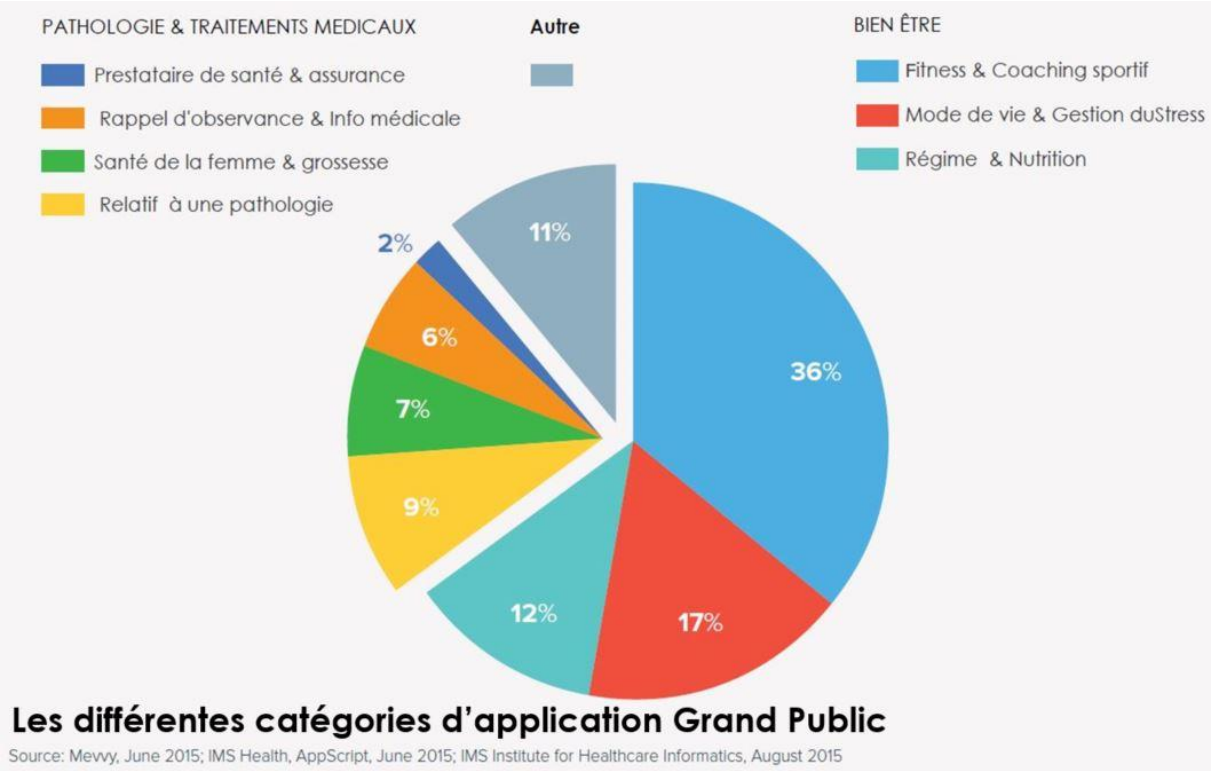

Figure 2 : répartition des différentes catégories d'applications grand public

Il existe une multitude d'applications mobiles dans différents domaines, mais l'un des secteurs où le développement a été le plus marquant est celui de la santé. En effet, la santé mobile permet d'avoir à portée de main de nombreuses solutions technologiques, et notamment de pouvoir réaliser soi-même la mesure des paramètres vitaux tels que le rythme cardiaque, la glycémie, la pression artérielle, l'activité cérébrale ou encore la température corporelle. D'autres vont analyser la qualité du sommeil, ou proposer des recommandations en termes d'alimentation ou de forme physique. La grande majorité de ces applications mobiles prodigue des informations, des messages de prévention et d'accompagnement (6).

Mais ces objets connectés ont parfois été développés dans un cadre international non réglementé, et certaines questions éthiques sont soulevées, notamment sur la gestion des données personnelles accumulées et collectées via ces nouvelles technologies de santé. Comment être sûr que ces données soient conservées de manière confidentielle ? De par leur caractère sensible, il apparait évident qu'un dysfonctionnement ou qu'une vulnérabilité d'un de ces appareils soit péjoratif pour le patient utilisateur de cet outil. C'est dans ce contexte

que certaines réglementations plus spécifiques à la santé connectée et à la m-santé ont récemment été développées.

2.1. Référentiel de bonnes pratiques de la Haute Autorité de Santé

La Haute Autorité de Santé ou « HAS » a publié dans son référentiel en Octobre 2016 ses recommandations d'usage et de bonnes pratiques des applications et objets connectés en santé. Ce référentiel, ayant pour but de promouvoir l'usage et de renforcer la confiance des utilisateurs dans la e-santé et les objets connectés, s'adresse aux patients et aux industriels développeurs des applications. Il vise les objets et applications connectés étant à la frontière des objets connectés considérés comme ayant un effet potentiel sur la santé, sans pour autant avoir le statut de dispositif médical (7). Ce référentiel est articulé autour de 5 domaines (informations utilisateurs, contenu de santé, contenant technique, sécurité/fiabilité, utilisation/usage) et rassemble 101 recommandations de bonnes pratiques. Les industriels créateurs d'applications mobiles ou d'objets connectés peuvent ainsi se baser sur ce référentiel à tous les stades de conception et de développement de leurs applications ou objets connectés, et s'assurer ainsi que leur innovation s'inscrit bien dans le respect de la règlementation relative aux données personnelles.

Ce référentiel vient définir et différencier 3 niveaux pour les applications santé, et indique qu'il faut prendre en compte :

- le contenu « initial », avec la qualité de l'information, des bases de données etc. ;
- le contenu « généré », avec les réponses aux questionnaires, les collectes de données via les différents capteurs, etc. ;
- le contenu « interprété », par un professionnel et/ou par un algorithme informatique.

2.2. Code de conduite européen Privacy en santé mobile

Un autre code relatif à la santé mobile et au respect de la vie privée est actuellement en cours d'élaboration par la Commission européenne, afin de promouvoir la confiance des

utilisateurs dans les applications de santé ; et également de permettre aux différents développeurs d'applications ainsi qu'à l'ensemble des acteurs économiques intervenant dans la santé mobile de bénéficier d'un support. Le but est de s'assurer de la conformité du produit développé au regard du règlement général sur la protection des données (RGPD). Toujours en cours d'élaboration (8), ce code vient détailler les principales lignes directrices à destination des développeurs d'applications et s'articule autour du RGPD en prenant en compte (9) :

- le consentement de l'utilisateur ;
- la limitation des finalités et minimisation des données ;
- la protection des données dès la conception et par défaut ;
- les droits des personnes concernées et les exigences en matière d'information ;
- la conservation des données ;
- la publicité dans les applications mHealth ;
- l'utilisation des données personnelles à des fins secondaires ;
- la divulgation de données à des tiers ;
- les transferts hors Union européenne (UE) ;
- les violations de données et les failles de sécurité ;
- les données recueillies auprès des enfants.

Ce projet de code a été commenté par le G29 dans sa lettre du 10-4-2017. Le G29 est le Groupe de Travail Article 29 sur la protection des données, et rassemble l'ensemble des autorités de contrôle européennes, afin d'élaborer les normes européennes relatives aux données à caractère personnel et d'émettre des avis sur les niveaux de protections octroyés. Ce dernier juge qu'en l'état, le projet ne remplit pas encore les niveaux d'exigences requis pour obtenir son accord, et vient ajouter que ce projet de code doit :

- préciser le rôle des différents acteurs concernés dans le traitement des données ;
- apporter plus de références ;
- faire plus de lien entre le RGPD et les législations nationales ;
- prendre davantage en considération d'autres éléments de réglementation, tels que la « directive ePrivacy » (10) s'agissant des cookies sur les sites de navigations, le règlement « eIDAS » (11) s'agissant d'une matière d'identification électronique, ou encore la directive 93/42/CE (12) relative aux dispositifs médicaux.

2.3. Référentiels en vigueur sur les objets connectés

2.3.1. Qualification des objets connectés

Lorsque l'on parle de e-santé, il faut définir ce que sont les objets connectés, qui se démocratisent de plus en plus. A l'heure actuelle, il y a un réel engouement pour le sujet et différentes instances en parlent régulièrement telles que la Commission Européenne, la Commission nationale de l'informatique et des libertés (CNIL), la HAS, le G29, le CNOM (Conseil National de l'Ordre des Médecins) ou encore la Food and Drug Administration (FDA). Mais une définition légale n'existe pas, en raison de l'absence de consensus sur une définition technique, tant les objets connectés peuvent être différents les uns des autres. Pourrait être défini en tant qu'objet connecté tout instrument, appareil, équipement, matière, produit ou autre article utilisé seul ou en association, y compris les accessoires et logiciels, doté de capteurs et de système de connectivité, et communiquant via un réseau.

Leur nombre ne cesse de grandir (6) : il était recensé 15 milliards d'objets connectés dans le monde en 2015, il en est attendu 80 à 100 milliards d'ici 2020 ; 23% des Français déclarent utiliser un objet connecté et 11% en auraient déjà adopté un dans le contexte santé/bien-être.

Les établissements de santé utilisent également ces objets connectés et l'Internet des objets ou « Internet of Things » (IoT). L'étude internationale Aruba sur l'usage fait des objets connectés indique même que l'IoT est couramment utilisé par 6 établissements de santé sur 10 (13). Les appareils connectés étant les plus utilisés dans ces établissements sont les moniteurs de patients et les appareils de rayons X et d'imagerie. Les appareils connectés ayant une forte plus-value étant les capteurs destinés à surveiller et à maintenir les appareils médicaux. Dans cette étude, plus de 70% des participants affirment que l'IoT permet de réaliser de réelles économies.

Les objets connectés doivent être différentiés des Dispositifs Médicaux. Ces derniers sont définis dans l'article L.5211-1 du CSP comme « tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action

principale voulue n'est obtenue pas par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Constitue également un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques ».

L'article R.5211-1 du CSP vient préciser que « ces dispositifs sont destinés à être utilisés à des fins de diagnostic, de prévention, de contrôle, de traitement ou d'atténuation d'une maladie ; de diagnostic, de contrôle, de traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap ; d'étude ou de remplacement ou de modification de l'anatomie ou d'un processus physiologique ; et de maitrise de la conception ». Ainsi, les DM autres que les DMIA (Dispositif Médical Implantable Actif) et DMDIV (Dispositif Médical de Diagnostic In Vitro), sont classés en 4 classes par ordre de criticité d'après les articles R.5221-6 et 5221-7 du CSP : classe I, classe IIa, classe IIb et classe III. La criticité est évaluée en fonction du risque potentiel pour le patient, le professionnel de santé ou toute autre personne intervenant lors de l'utilisation des DM (invasivité, caractère actif, durée d'utilisation, destination chirurgicale, etc.).

La question se pose de la définition des dispositifs dits « frontières » bien-être/santé, tel que le pilulier électronique. La Cour de Justice de l'Union européenne (CJUE) vient préciser dans un arrêt du 22 Novembre 2012 suite à l'affaire C-219-11 Brain Products GmBH contre BioSemi VOF, qu'il faut également regarder si le dispositif est « destiné à un but médical » (14). Ainsi est précisé :

- dans l'article 30 : « Dès lors, dans des situations dans lesquelles un produit n'est pas conçu par son fabricant pour être utilisé à des fins médicales, la certification de celui-ci en tant que dispositif médical ne saurait être exigée » ;
- dans l'article 31 : « Tel est notamment le cas de nombreux articles de sport qui permettent de mesurer, en dehors de toute utilisation médicale, le fonctionnement de certains organes du corps humain. Si de tels articles devaient être qualifiés de dispositifs médicaux, ils seraient soumis à une procédure de certification sans que cette exigence soit justifiée. »

L'ANSM (Agence Nationale de Sécurité du Médicament et des Produits de Santé) vient préciser que, pour définir si un dispositif est un objet connecté ou un dispositif médical, il faut regarder

la « destination d'usage » revendiquée par le fabricant. D'après ses principes directeurs, il faut regarder :

- si le logiciel doit avoir une finalité médicale : par exemple permettre un diagnostic, une aide au diagnostic, un traitement ou une aide au traitement ;
- si le logiciel donne un résultat propre à un patient sur la base de ses données individuelles ;
- si le logiciel pilote ou influence un DM, auquel cas les conditions de mise sur le marché sont identiques.

Pour l'ANSM, certaines fonctions de logiciels utilisées en santé ne correspondent pas à des finalités médicales, comme c'est le cas pour les fonctions de gestion administrative (archivage, communication, etc.), de réalisation d'actes à distance, de validation ou de gestion automatisée de la prescription (à l'exception des fonctions de calcul de doses propres à un individu). Certaines applications ne sont pas considérées comme des DM, comme par exemple les applications pour prescrire la pratique d'entrainements sportifs ou encore les applications d'observance.

Un réel travail de définition et d'analyse des applications et objets connectés est actuellement réalisé par les autorités compétentes, afin de différencier les dispositifs médicaux des objets connectés, et parfois la frontière est extrêmement mince.

2.3.2. Qualification des données

Pour les objets connectés, qu'il s'agisse d'un DM ou non, cela n'impacte pas la nature des données traitées, qui sont relatives à la santé ou au bien-être de l'utilisateur du dispositif. L'ASIP Santé et le RGPD viennent préciser que ces dernières doivent être collectées et traitées après en avoir correctement informé la personne concernée et être conservées de manière sécurisée.

2.3.3. Régimes applicables

Pour être mis sur le marché, un DM doit avoir le marquage CE. A cela s'ajoute la certification de conformité du dispositif, assurée par des organismes dit notifiés ou « ON » désignés auprès de la Commission européenne par les Etats Membres. En France, l'organisme notifié qui a été désigné par l'ANSM est le LNE-GMED (Laboratoire National de Métrologie et d'Essais - Groupement pour l'Evaluation des Dispositifs Médicaux). Il est chargé de vérifier que certaines exigences de sécurité sont respectées :

- pour les DM : qu'ils sont bien classés et ont le marquage CE ainsi que la certification adéquate ;
- pour les données de santé : que l'authentification est forte et que l'hébergeur de données de santé est agréé ou certifié.

La CNIL élabore également des programmes de contrôles portant notamment sur les objets connectés « bien-être et santé », et son activité de labélisation se transforme en activité de certification des objets connectés.

En parallèle, un nouveau règlement sur les DM et DMDIV a été adopté par le Conseil et le Parlement européens en mai 2017 et devra être appliqué obligatoirement dans un délai de 3 ans pour les DM et dans un délai de 5 ans pour les DMDIV. L'objectif de ce règlement est d'harmoniser l'interprétation des directives DM, de lever les lacunes et incertitudes règlementaires, et de renforcer la sécurité des dispositifs, notamment après le scandale de l'affaire PIP. Ce règlement vient ainsi :

- étendre le champ d'application de la réglementation ;
- classer de manière plus sévère les DM ;
- remplacer les exigences essentielles des directives par des exigences générales sur la sécurité et la performance des DM ;
- obliger d'établir un plan de surveillance (matériovigilance) ;
- définir de nouvelles obligations à la charge des distributeurs DM ;
- mettre en place un système d'identification des DM (traçabilité) ;
- désigner une personne chargée de veiller au respect de la réglementation (justifiant de diplômes ou qualifications) ;

- renforcer les exigences et contrôle des organismes notifiés ;
- préciser la possibilité de retraitement de certains dispositifs à usage unique.

2.3.4. Points de vigilance

Les objets connectés sont de plus en plus utilisés, ce qui augmente la probabilité d'avoir des failles ou autres incidents de sécurité sur leur usage. Malgré leurs nombreux avantages, il ne faut pas oublier de considérer l'objet dans sa globalité et ne pas oublier que les données générées par les différents capteurs ou renseignements complétés par les utilisateurs peuvent potentiellement transiter sur internet et sont stockées sur différents serveurs, plus ou moins sécurisés.

Le fait que les données soient stockées sur différents serveurs peut entrainer des cyber-attaques, et la question de la qualité et de la sécurité des systèmes se pose. Cela a été le cas en février 2016 dans l'hôpital Hollywood Prebyterian Medical Center de Los Angeles, où, durant 12 jours, l'hôpital a été paralysé (15). Toutes les machines, que ce soit les ordinateurs, les scanners, les logiciels de gestion des médicaments, étaient bloqués par un virus informatique qui chiffrait et rendait illisible les données des patients, tant qu'un code de déblocage n'était pas saisi (appelé ramsomware ou rançongiciel). La rançon de 17 000 dollars a été payée par l'hôpital rapidement car, sans données et sans historique des patients, ces derniers ne peuvent être soignés. En Angleterre, trois hôpitaux du nord-est ont également été touchés par une attaque informatique fin 2016 (16). Les systèmes de gestion des analyses, l'accès aux dossiers patients, les fichiers de banque du sang etc. étaient inaccessibles. Les hôpitaux ont dû couper l'intégralité de leur système informatique le temps de trouver une solution.

Partout dans le monde, les systèmes d'informations de santé sont régulièrement la cible de cyber-attaques ; et l'utilisation de plus en plus forte du numérique dans les infrastructures de santé augmente le risque de défaillance et de dysfonctionnement. A cela s'ajoute la connexion des systèmes de plus en plus présente. La sécurité des données de santé est donc devenue une pierre angulaire de la e-santé. Pour l'instant, le système français n'a pas été la cible d'attaques. Mais ce genre d'actes paralyserait potentiellement les infrastructures

et les soins prodigués, comme cela a été le cas aux Etats-Unis et en Angleterre. Sécuriser les systèmes informatiques et les données de santé est l'un des plus gros enjeux de notre siècle. L'ASIP santé a mis en place un portail de cyberveille (17) afin d'aider les structures hospitalières, aux maturités numériques peu homogènes, à détecter et contrer les éléments de vulnérabilité éventuels.

La sécurisation des données de santé et des infrastructures hospitalières, qu'elle soit physique, logistique ou numérique, est primordiale, et passera également par la responsabilisation des acteurs (18). A cette responsabilisation s'ajoute le respect de la propriété intellectuelle, les objets connectés pouvant faire intervenir différents types de droits, tels que le droit d'auteur (pour les logiciels), le droit des marques (pour les noms et logos), le droit des dessins et modèles (pour les noms et design), le droit des brevets (pour les innovations techniques) ou encore les droits voisins (pour les bases de données). A ces différents droits s'ajoutent l'encadrement contractuel, tels que les contrats de sous-traitance, les contrats de cession, ou encore les contrats de licence. Pour les objets connectés, il faut prendre en considération l'ensemble de ces droits et obligations contractuelles.

2.4. L'intelligence artificielle

Tout comme les objets connectés, l'intelligence artificielle se développe dans le domaine de la santé, et son déploiement va s'accentuer de plus en plus dans les années à venir. La notion d'Intelligence Artificielle ou « IA » est une notion très ancienne. Cette notion mouvante, qui renvoie à une multitude de technologies créées durant la deuxième moitié du XX^{e} siècle, repose sur l'utilisation des algorithmes. L'algorithme est la description d'une suite finie et non ambiguë d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée. L'IA est novatrice dans le sens où elle combine l'utilisation de différents algorithmes, afin d'en potentialiser les résultats et de créer des « machines à penser », semblables dans leur fonctionnement aux Hommes. Marvin Minsky en donne la définition dans les années 50 : il s'agit de la « science qui consiste à faire faire aux machines ce que l'homme ferait moyennant une certaine intelligence » (19). La difficulté à la définir précisément vient du fait

que cette dernière évolue très rapidement. Les algorithmes sont créés en fonction des données recueillies.

Lorsque l'on parle d'IA, il faut également parler de Machine Learning et de Deep Learning. Le Machine Learning, ou apprentissage automatique, consiste à alimenter la machine par des exemples de tâches qu'on lui propose d'accomplir : elle est ainsi entrainée, via les données qui lui sont fournies, à apprendre et à déterminer d'elle-même les opérations à mettre en œuvre pour effectuer ladite tache. C'est la data ici qui alimente l'IA pour qu'elle fasse du machine learning. Le Deep Learning ou apprentissage profond est, quant à lui, un système d'apprentissage basé sur des « réseaux de neurones artificiels » numériques. La différence entre le machine learning et le deep learning est que, lorsqu'il y a des analyses complexes à réaliser, les caractéristiques essentielles de l'opération ne sont plus identifiées par l'Homme dans l'algorithme préalable, mais directement par l'algorithme de deep learning. L'IA s'est particulièrement développée dans les années 2010 grâce à ces deux outils et à l'explosion du Big Data. Intégrée dans notre quotidien, l'IA modifie notre approche en santé et permet d'envisager de réels progrès, notamment dans le domaine médical. L'IA présente de réelles promesses et participe déjà à :

- générer de la connaissance, en tirant profit et en tirant des tendances de la quantité immense des publications scientifiques ;
- faire du « matching », par exemple en répartissant les patients dans les essais cliniques les plus appropriés pour leur pathologie. Il est de plus en plus évoqué de pratiquer une médecine personnalisée avec des schémas thérapeutiques adaptés aux patients, via le croisement des données du patient à celles de cohortes gigantesques ;
- prédire des épidémies, ou encore repérer certaines prédispositions pour des pathologies et en éviter le développement ;
- aider à la décision les médecins, en leur suggérant des solutions thérapeutiques adaptées.

II- Les intervenants de la e-santé

1. Les utilisateurs

Le développement de la e-santé concerne tous les acteurs en santé, ainsi que toutes les personnes ayant un lien, direct ou indirect, avec ces professionnels de santé. Qu'il s'agisse des patients, premiers concernés, ou bien des médecins, des pharmaciens, des établissements de santé, des laboratoires pharmaceutiques ; ou encore des start-ups, des GAFA MS (Google, Apple, Facebook, Amazon, Microsoft et Samsung), des politiques ou des institutionnels : tous sont concernés de près ou de loin par cette nouvelle manière d'appréhender la santé, et tous viennent d'horizons très variés. Les patients peuvent par exemple utiliser certaines applications pouvant les aider à maintenir leur santé, disposer d'informations en ligne sur leurs pathologies ou les traitements existants. Les professionnels de santé quant à eux s'en servent, plus ou moins régulièrement en fonction de leurs pratiques médicales ou paramédicales, tout comme les instances de santé, avec notamment les chercheurs et épidémiologistes qui publient leurs résultats sur certaines bases de données accessibles de tous. Enfin, il faut aussi noter que les organismes complémentaires que sont les mutuelles de santé ainsi que l'Assurance Maladie développent des bases de données en rapport avec leurs activités, mais aussi pour apporter un support aux patients et aux professionnels de santé. Certaines instances telles que l'ANSM ou la HAS publient régulièrement et en libre accès des connaissances sur les médicaments, ainsi que des guides de bonnes pratiques cliniques.

Les industriels y voient un réel marché, les professionnels de santé y voient de nouvelles opportunités d'efficacité et de qualité des soins, mais les deux ont un point en commun : leur approche collaborative pour concrétiser des solutions innovantes pour la santé de demain. Bien sûr, il faut préciser que les acteurs du numérique ne sont pas forcément tous égaux. Pour les patients, cet outil devient vital, alors que, pour les laboratoires par exemple, la motivation est différente, car ils seront davantage intéressés par le médecin potentiel prescripteur de médicaments que par le patient. La difficulté consiste donc à évoluer en transparence, et de trouver pour tous les acteurs des intérêts communs.

2. Les autorités de contrôle en présence

2.1. La CNIL

La CNIL, ou Commission Nationale de l'Informatique et des Libertés, est une agence française autonome ayant été créée par la loi du 6 janvier 1978, également connue sous le nom de « Loi Informatique et Libertés ». En effet, l'essor des premiers réseaux connectés et l'apparition d'Internet dans les années 1960-1970 a conduit à se poser la question de la protection des données recueillies via et/ou stockées sur les réseaux informatiques.

Historiquement, tout a débuté suite à la création d'un projet nommé « SAFARI » (ou Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) au début des années 1970 (20). Ce projet émanant du gouvernement avait pour objectif d'identifier chaque citoyen par des numéros et de relier entre eux tous les fichiers administratifs concernant les personnes.

Devant les dangers potentiels de cette pratique informatique, est créée en France en 1974 une « Commission Informatique et Libertés », présidée à l'époque par Mr. Bernard Chenot, qui s'est penchée sur la création d'une institution indépendante chargée de veiller à l'application de la loi et du respect de la vie privée, et ce même sur les réseaux connectés. Durant 6 mois de consultations et de débats, plusieurs propositions ont été formulées ; et sur le fondement de ces dernières, le gouvernement a déposé fin 1977 un projet de loi devant le Parlement, projet de loi qui par la suite sera voté et donnera naissance à la loi du 6 Janvier 1978. C'est cette loi et les décrets qui la constituent qui permettent à la CNIL d'agir pour la protection de la vie privée des citoyens contre toutes pratiques illégales quant au traitement de leurs données à caractère personnel. De nos jours, la CNIL a de nombreuses missions pour permettre à tout citoyen d'avoir l'assurance du respect de ses droits fondamentaux et du respect de ses libertés individuelles, ainsi que d'assurer les intérêts économiques et les impératifs de santé publique (21).

2.1.1. Organisation

La Commission est composée 198 agents et de 18 membres (22), dont :

- 6 représentants des hautes juridictions ;
- 5 personnes qualifiées ;
- 4 parlementaires ;
- 2 membres du Conseil économique, social et environnemental ;
- 1 membre de la Commission d'accès aux documents administratifs.

Ils se réunissent en formation plénière une fois par semaine, afin notamment d'analyser les conséquences des nouvelles technologies sur la vie des citoyens.

La Commission peut également se réunir en formation restreinte, composée alors de 5 membres, et prononce diverses sanctions, notamment à l'égard des responsables de traitements ne respectant pas la loi. Son organigramme est présenté dans la Figure 3.

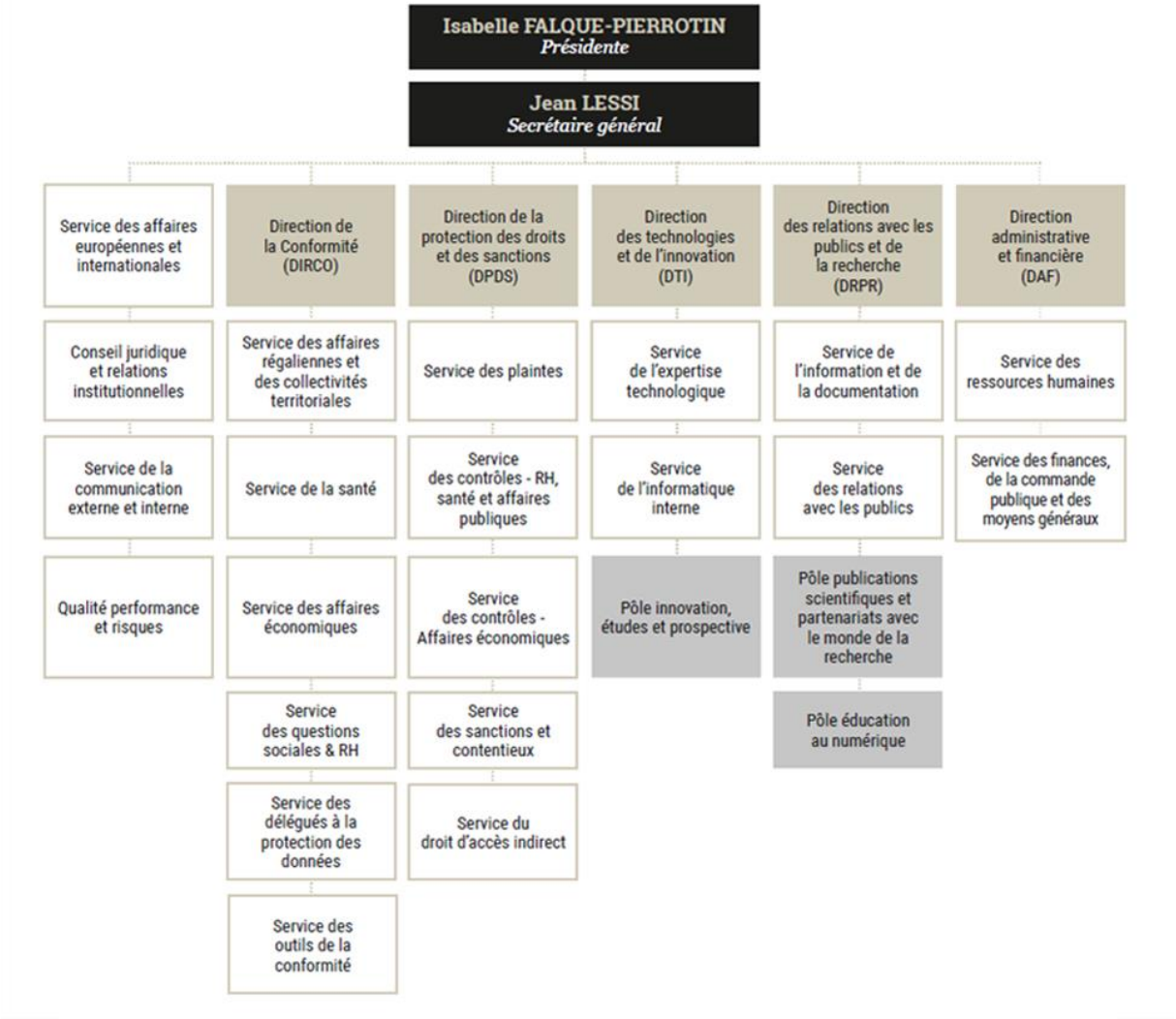

Figure 3 : Organigramme des directions et services de la CNIL

2.1.2. Missions

A l'ère des données et du numérique, la CNIL doit s'assurer que ces dernières soient correctement utilisées. Parmi ses nombreuses missions, se retrouvent celles d'informer le grand public et les professionnels, de conseiller et de réglementer les pratiques, d'accompagner la conformité, de contrôler et de sanctionner en cas de pratiques illégales, d'être en lien avec les pouvoirs publics et enfin et surtout : d'assurer la protection des citoyens (23). Nous allons maintenant brièvement les détailler.

2.1.2.1. Informer le grand public et les professionnels

Au regard du RGPD et de la Loi Informatique et Libertés (LIL), la CNIL se doit d'informer le grand public sur ses droits et ses obligations, mais également d'informer plus personnellement les petites et moyennes entreprises (*cf.* loi n°2018-493 du 20 juin 2018 modifiant la Loi Informatique et Libertés (24)), ainsi que de répondre à leurs demandes. Elle s'acquitte de cette mission via la mise en place régulière d'actions de communications, au cours de colloques, conférences, salons, etc. Elle assure également des actions de sensibilisation auprès de médiateurs de la consommation et de médiateurs publics, afin de s'assurer du respect et de l'application de la loi.

2.1.2.2. Conseiller et réglementer

Réglementer les données à caractère personnel se fait via différents instruments et méthodes, cherchant tous à atteindre le même objectif : assurer la mise en conformité des organismes. Ainsi, la CNIL va :

- émettre des avis sur les traitements pour le compte de l'Etat, pour la sureté de l'Etat (*cf. art. 26 et 27 de la LIL*) ;
- établir et publier les lignes directrices, les recommandations et les référentiels destinés à faciliter la mise en conformité des traitements des données à caractère personnel et de mettre en place l'évaluation préalable des risques par les responsables de traitement et les sous-traitants ;
- homologuer et publier les méthodologies de référence ;
- établir et publier, et ce en concertation avec les organismes publics et privés acteurs du système, des règlements types afin d'assurer la sécurité des systèmes de traitements des données et de régir les traitements de données biométriques, génétiques et de santé ;
- établir une liste de traitements pouvant potentiellement créer un risque élevé devant faire l'objet d'une consultation préalable.

2.1.2.3. Accompagner la conformité

La CNIL accompagne la conformité en encourageant notamment l'élaboration de Codes de Conduite, tel que celui de l'Union Française du Marketing Direct (UFMD) (25), visant à définir des règles déontologiques en matière de collecte et d'utilisation de données électroniques à des fins de prospection directe. La CNIL va également certifier des personnes, des organismes, des produits, des systèmes de données ou encore des procédures afin de s'assurer qu'ils soient conformes au RGPD. Enfin, elle a également pour missions d'assurer la conformité des processus d'anonymisation des données via la certification ou l'homologation, la publication de référentiels ou de méthodologies générales aux fins de certification.

2.1.2.4. Contrôler et sanctionner

Afin d'assurer la conformité des pratiques au regard de la réglementation, la CNIL reçoit les réclamations, pétitions et plaintes des parties prenantes et réalise un contrôle *a posteriori*. Elle peut charger ses agents de procéder ou faire procéder à des vérifications portant sur tous les traitements, et lors d'un contrôle, elle peut :

- accéder aux locaux professionnels ;
- demander tout document nécessaire et en garder une copie ;
- recueillir tout type de renseignement jugé utile ;
- accéder aux programmes informatiques et aux données.

Des programmes de contrôles sont élaborés en fonction des thématiques d'actualité, des problématiques identifiées et des plaintes envoyées à la CNIL. En 2017, la CNIL a réalisé 341 contrôles sur place, sur audition, sur pièces et en ligne (26). En comparaison, il n'y avait eu que 34 contrôles de réalisés en 1990.

A l'issue des contrôles, diverses sanctions peuvent être prononcées par la formation restreinte de la CNIL : une sanction pécuniaire d'un montant maximal de 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, une publication de la décision dans la presse, ou encore ordonner que les fautifs informent individuellement les personnes concernées par un

traitement abusif de leurs données. Le RGPD vient détailler les différentes sanctions applicables dans l'art. 58.2 (27), qui sont par ordre croissant de gravité:

- un avertissement du responsable de traitement et/ou du sous-traitant que les opérations envisagées sont susceptibles de violer les dispositions du RGPD ;
- un rappel à l'ordre du responsable de traitement et/ou du sous-traitant que les opérations réalisées ont entraîné une violation du RGPD ;
- un ordre donné au responsable de traitement et/ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée exerçant ses droits en application du RGPD ;
- un ordre donné au responsable de traitement et/ou au sous-traitant de mettre en conformité les diverses opérations concernées avec les dispositions du RGPD ;
- un ordre donné au responsable de traitement et/ou au sous-traitant de communiquer à la personne concernée la violation de ses données à caractère personnel ;
- d'imposer une limitation temporaire ou définitive d'effectuer un traitement ;
- d'ordonner une rectification, une limitation ou un effacement des données à caractère personnel et d'en notifier les personnes concernées ;
- de retirer une certification ;
- d'imposer une amende administrative ;
- d'ordonner la suspension des flux de données adressés à un destinataire dans un pays tiers.

A noter que le montant des amendes est perçu par le Trésor Public et que les sanctions peuvent être cumulatives. En 2017, la CNIL a ainsi réalisé 79 mises en demeures et prononcé 14 sanctions, dont 9 sanctions financières et 5 avertissements (26).

2.1.2.5. Liens avec les pouvoirs publics

La CNIL a également pour missions de répondre aux demandes des pouvoirs publics et d'informer l'Etat des infractions dont elle a connaissance. Son avis est requis sur tout projet de loi ou décret ou toute disposition de projet de loi ou de décret relatif à la protection des

données et, à la demande de certaines institutions, sur toute proposition de loi. Elle peut présenter ses observations devant toute juridiction à l'occasion d'un litige relatif à l'application du RGPD et de la LIL.

2.1.2.6. Protéger les citoyens

La CNIL s'assure de d'accompagner et de protéger les citoyens, via :

- la gestion et le suivi des réclamations et plaintes de ces derniers ;
- une information sur la protection de leurs données ;
- la réponse aux demandes d'exercice des droits d'accès concernant les traitements liés à la sûreté de l'Etat, à la défense ou la sécurité publique.

2.2. L'ASIP Santé (Figure 4)

Dans le cadre de la e-santé, d'autres agences existent en France, et notamment l'Agence des Systèmes d'Information Partagées de Santé, ou « ASIP Santé ». Il s'agit d'un groupement d'intérêt public créé en 2009, ayant pour objectif d'assurer trois missions complémentaires (28) :

- créer les conditions propices à l'essor de la e-santé, via la maitrise d'ouvrage des projets de systèmes d'information en santé ; ou encore la définition, la promotion et l'homologation de référentiels, standards, produits ou services contribuant à l'interopérabilité, la sécurité et l'usage des Systèmes d'Information (SI) de santé et de télésanté ;
- conduire des projets d'envergure nationale, via notamment la maitrise d'ouvrage et la gestion, dans le cadre des missions déléguées, des annuaires et référentiels nationaux ; ainsi que la certification, la production, la gestion et le déploiement de la Carte de Professionnel de Santé (CPS) ;
- déployer les usages en soutenant l'innovation, via l'accompagnement et l'encadrement des initiatives publiques et privées concourant à son objet ; et via la

participation aux préparations et aux applications des accords aux projets internationaux dans les domaines des systèmes de partage d'information de santé.

L'ASIP Santé participe également aux politiques de santé actuelles avec, depuis avril 2018, la création d'une nouvelle mission « e-santé » installée auprès du ministère de la santé. Cette mission unique a pour objectif de regrouper l'ensemble des instances existantes au sein du ministère de la santé, et est chargée des projets numériques. Cette mission a pour objectif d'assurer « la coordination stratégique des chantiers de transformation numérique du système de santé », notamment pour atteindre les objectifs fixés par le gouvernement avec l'interopérabilité des systèmes d'information (SI), le développement des échanges sécurisés des données et l'appropriation des différents outils par les acteurs (professionnels de santé, patients, structures d'accueil, etc.) (29).

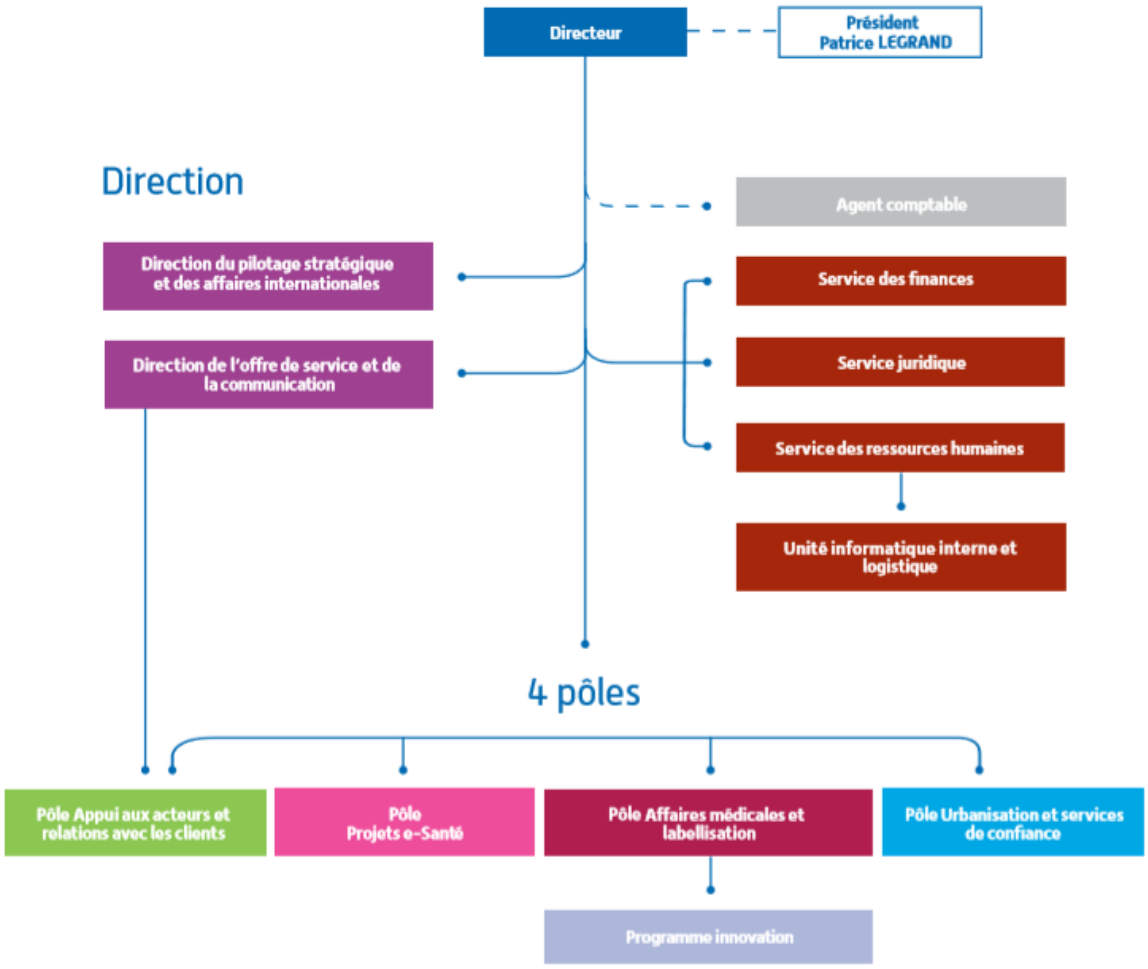

Figure 4 : Organigramme des directions et services de l'ASIP Santé en Décembre 2017

2.3. Les ARS

Aujourd'hui au nombre de 17, les Agences Régionales de Santé ou « ARS » sont des établissements créés à la suite de la loi n°2009-879 du 21 juillet 2009 dite « Hôpital, patients, santé et territoire » (30). Ces agences ont permis d'inscrire la gouvernance du système de santé dans un cadre global, impliquant l'ensemble des acteurs de santé, et ayant pour principales missions de piloter la politique de santé publique et de réguler l'offre de santé en région (31).

Ces ARS sont représentées dans chaque département par une délégation départementale, qui va décliner localement la stratégie régionale de santé, via :

- «la veille et la sécurité sanitaire, ainsi que l'observance en santé ;
- la définition, le financement et l'évaluation des actions de prévention et de promotion de la santé ;
- l'anticipation, la préparation et la gestion des crises sanitaires ».

Les ARS mettent en place leurs actions au niveau régional via les Projets Régionaux de Santé, élaborés après concertation avec l'ensemble des acteurs de santé. Est définie à la suite de ces concertations la stratégie nationale de santé, que les ARS organisent et mettent en œuvre. Dans ce contexte, la stratégie nationale de santé pour 2018-2022 a été mise en place et devra être appliquée, entre autres via les ARS.

3. Stratégie nationale de santé

En raison de l'avancée des nouvelles technologies et des différentes problématiques sanitaires toujours présentes, tels que les déserts médicaux, l'Etat français adapte sa politique en santé, notamment en élaborant divers programmes de e-santé.

3.1. Stratégie nationale 2018-2022

La Stratégie Nationale (SN) de e-santé 2020 a pour objectif « d'accompagner les acteurs du système de soins dans le virage numérique et de permettre à la France de rester à la pointe en matière d'innovation. En tant que régulateurs et financeurs du système de santé

en région, les agences régionales de santé sont étroitement impliquées dans sa mise en œuvre » (32).

Il faut savoir que certaines actions sont engagées depuis plusieurs années, et impliquent diverses agences régionales de santé à plusieurs niveaux, avec notamment le Dossier Médical Personnel (DMP) depuis 2016, les objets connectés et applications mobiles en santé se développant depuis les années 2000, les différents systèmes d'information en santé ou encore les programmes Hôpital numérique ou territoire de soins numériques. Afin de prendre en compte l'avis des citoyens et/ou d'experts dans le domaine et d'orienter ainsi la politique e-santé nationale, diverses concertations citoyennes ont été mises en place, via le gouvernement ou des organismes habilités : 17 experts se sont ainsi réunis en mars 2017 pour proposer une politique de e-santé numérique ambitieuse (33), et la CNIL a également organisé plusieurs débats publics en 2017 dans le cadre de la réflexion éthique qui lui a été confiée par la loi pour une république numérique (34). La SN de e-santé 2020 a pris en compte ses avis et s'articule ainsi autours de 4 axes principaux.

Le 1er axe de cette SN vise à remettre les citoyens au cœur de la e-santé, via notamment :

- le renforcement et la simplification de l'accès aux soins pour tous, en facilitant l'accès à la télémédecine et surtout en simplifiant les démarches administratives ;
- le développement des services aux patients pour favoriser leur autonomie, via une information plus claire sur l'offre de soins, ainsi qu'en leur facilitant l'accès à leurs informations médicales (initié par le DMP) et leur suivi des indicateurs de santé ;
- la démocratie sanitaire, en favorisant l'usage du numérique par les associations de patients, en permettant la contribution individuelle à l'amélioration de notre système de santé et en promulguant l'expression collective des patients et citoyens.

Le 2e axe abordé vise à apporter tout le soutien nécessaire pour favoriser l'innovation par les professionnels de santé, avec :

- le développement des cursus de formation des professionnels de santé autour du numérique : en France, la formation des médecins aux technologies numériques

doit prendre une place accrue et contribuer ainsi à lever les freins au dynamisme de la e-santé ;

- le soutien aux professionnels de santé qui s'engagent en faveur de l'innovation numérique. Cela passe par le renforcement de la cohérence et de la visibilité des programmes d'appui aux professionnels porteurs de projets numériques innovants ; et aussi par l'appui et la sécurisation des initiatives de professionnels de santé dans le recours aux objets connectés ;
- l'accompagnement du développement des systèmes d'aide à la décision médicale, afin de faciliter l'exploitation numérique des connaissances médicales ; et une meilleure utilisation des outils numériques pour simplifier l'utilisation des recommandations de pratique clinique par les professionnels de santé ;
- le soutien de la co-innovation avec les patients et les industriels, en favorisant la co-construction des solutions numériques entre start-ups professionnelles de santé et citoyens-patients. Cela passe aussi par l'accompagnement de la professionnalisation et de la mutualisation, avec le développement depuis plusieurs années des « living labs en santé » (laboratoires de rencontre entre entrepreneurs et utilisateurs) (35).

Le 3e axe majeur vise à simplifier l'action de l'ensemble des acteurs économiques en santé, en :

- établissant une gouvernance plus lisible et ouverte de la e-santé, via l'optimisation de la répartition des rôles entre les acteurs de la régulation. A cet effet, le ministère va adapter son organisation interne ;
- favorisant le partage de priorités entre acteurs publics et économiques en matière de SI, avec le déploiement d'outils d'aide à la coordination des soins comme priorité. D'autres investissements pourront être financés si les acteurs sont organisés pour garantir leur utilité ;
- clarifiant davantage les voies d'accès au marché des solutions de e-santé, via une instance publique ;
- déployant un cadre d'interopérabilité facilitant l'intégration des innovations, avec une définition d'alternatives à la CPS en tant qu'outil d'authentification ; ainsi qu'une définition de normes pour structurer les documents échangés par les professionnels.

Enfin, le 4e axe développé vise à limiter les scandales sanitaires, en favorisant la modernisation des outils de régulation de notre système de santé. Cela passe par :

- une sécurité des SI assurée : face à la montée des menaces en matière de cyber-sécurité, le ministère chargé de la santé fait de la sécurité de ces systèmes une priorité et accompagnera par un plan d'action à court terme la mise en œuvre de la PGSSI-S, ou « Politique Générale de Sécurité des Systèmes d'Information de Santé » (36) ;
- une accélération du développement de méthodes d'évaluation adaptées aux solutions multi-technologiques : cela passe par un soutien des pouvoirs publics, avec le concours de la HAS (Haute Autorité de Santé), du développement des méthodologies d'évaluation adaptées à la e-santé (notamment pour les dispositifs innovants), en y impliquant les professionnels et les patients ;
- le numérique au service de la veille et de la surveillance sanitaire, avec le développement de nouveaux outils :
    - de modélisation facilitant l'anticipation des menaces épidémiques ;
    - d'imagerie et de représentation des données environnementales pour faciliter les interventions en santé ;
- lever les freins au développement du Big Data au service de la santé :
    - la loi de modernisation de notre système de santé simplifie le cadre juridique lié à la circulation de l'information de santé ;
    - l'ouverture des données est devenue une mission officielle du ministère chargé de la santé.

Ces grands axes font partie intégrante des objectifs de l'actuel gouvernement. Le 13 février 2018, les actuels premier ministre et ministre des solidarités et de la santé ont lancé une « stratégie de transformation du système de santé » dont le chapitre 3 vise à « accélérer le virage numérique » du secteur de la santé (37). Dans le chapitre dédié au « numérique en santé », l'exécutif place parmi ses objectifs pour 2022 : l'accessibilité en ligne, et ce pour chaque individu, de l'ensemble de ses données médicales ; la dématérialisation de l'intégralité des prescriptions et la simplification effective du partage de l'information entre toutes les parties prenantes en santé.

3.2. Programme Territoire de Soins Numériques ou TSN

Face à l'augmentation des pathologies chroniques et à l'évolution de la prise en charge des patients, davantage orienté « parcours patient », il est nécessaire de chercher à moderniser le système de santé. Pour ce faire, divers programmes sont élaborés, ainsi que des actions menées localement via les ARS.

Lancé en 2014 dans le cadre des investissements d'avenir avec un budget de 80 millions d'euros, le programme Territoire de soins numériques vise à moderniser le système de soins en expérimentant, dans certaines zones pilotes, les services et les technologies les plus innovants en matière de e-santé (38). Cinq grands projets ont été sélectionnés par les ARS de différentes régions pour être testés en 2014 :

- la Nouvelle Aquitaine : le projet XL ENS (Landes espace numérique de santé) qui vise à réduire les distances et délais de prise en charge des patients ;
- la Bourgogne Franche-Comté : le projet E_TICSS (Territoire Innovant Coordonné Santé Social), qui regroupe un panel d'outils numériques incluant des répertoires professionnels, une messagerie sécurisée, des dossiers coordonnés ;
- l'Ile-de-France : le projet TerriS@nté (« Le numérique au service de la santé en métropole du Grand-Paris »), qui regroupe entre autres des services incluant un service d'information, un compte patient, des offres de formation, des outils de coordination ;
- l'Auvergne - Rhône Alpes : le projet PASCALINE, qui regroupe des outils communicants pour « passer de parcours par pathologie à une approche territoriale décloisonnée » ;
- l'océan Indien : le projet OIIS (Océan Indien Innovation Santé), qui vise à améliorer le parcours de prise en charge de maladies chroniques.

Ces TSN sont financés par le commissariat général à l'investissement dans le cadre du Programme Investissement d'Avenir (PIA) et piloté au niveau national par la Direction Générale de l'Offre de Soins (DGOS). L'Agence Nationale d'Appui à la Performance (ANAP) est chargée d'accompagner la DGOS dans le pilotage du programme, et d'autres instances interviennent parfois sur certains axes, telles que l'ASIP Santé et la HAS.

Deux ans après la mise en place de ces TSN, les résultats dans ces régions pilotes sont positifs et les TSN sont tous poursuivis. Ils sont en cours de capitalisation pour être diffusés et appliqués à l'ensemble du territoire. L'ANAP travaille également pour les acteurs de santé, en préparant des documents sur les SI, l'organisation autour de la coordination, la mobilisation des acteurs, l'achat des services numériques complexes et d'interface avec les industriels.

Dans le prolongement des TSN, les programmes « e-parcours » et « e-Hôp 2.0 » ont été lancés en 2017 avec pour objectifs de développer les SI des établissements et de proposer des solutions numériques pour améliorer la prise en charge des patients (39).

Le programme « e-parcours » doit permettre de faciliter les échanges entre les professionnels de santé. Les solutions numériques issues de TSN ont vocation à être proposées aux professionnels médico-sociaux et sociaux dans toute la France pour 2021 : 150 millions d'euros ont été débloqués sur cinq ans à destination des ARS, chargées de piloter le déploiement de ce programme dans chaque région.

Le programme « e-Hôp 2.0 », lié aux SI des hôpitaux, vise à soutenir financièrement le développement de solutions numériques pour faciliter les relations entre les établissements et leurs patients ainsi que les établissements partenaires : 400 millions d'euros seront investis jusqu'en 2021.

L'ensemble de ces programmes a pour vocation d'améliorer la santé des populations, en utilisant les moyens technologiques actuellement en notre possession. Comme l'indiquait Marisol Touraine, ministre de la santé du précédent gouvernement, « la rencontre entre le numérique et la santé est une promesse pour les patients, les professionnels et le système dans son ensemble ! Aujourd'hui, il faut innover dans l'organisation territoriale, innover dans les techniques de soins, c'est une exigence. En reconduisant ces programmes, en les généralisant, le Gouvernement accompagne les établissements dans ce virage numérique » (40).

4. Les dernières avancées réglementaires

Bien avant l'essor d'internet et des plateformes numériques, et bien avant la connaissance des risques associés pour la vie privée, le législateur avait perçu la nécessité d'encadrer le traitement des données à caractère personnel, ces dernières pouvant être collectées, conservées et/ou traitées de manière disproportionnée et injustifiée. C'est dans ce contexte qu'avait été adoptée la loi du 6 Janvier 1978, qui a créé la CNIL (41).

A l'ère du numérique, diverses mesures sont prises par le gouvernement, ainsi que par les autorités compétentes afin d'adopter une politique en santé innovante incluant les nouveaux moyens technologiques en notre possession. A ces mesures prises s'ajoutent les nouvelles réglementations en vigueur pour encadrer ces nouvelles technologies.

4.1. Loi pour une république numérique du 07/10/2016

La Loi française pour une République numérique a été initialement déposée à l'Assemblée Nationale en procédure accélérée par le ministre de l'économie en Décembre 2015, suite à une concertation nationale ayant débuté en 2014 sur les enjeux du numérique, et notamment en santé. Suite à différentes lectures, le texte a été adopté définitivement par le Sénat le 28 Septembre 2016 et promulgué le 7 octobre 2016 sous le nom de Loi n°2016-1321 du 7 octobre 2016 pour une République numérique (42). Ce texte a différentes finalités :

- ouvrir les données publiques à tous, également appelé « l'Open Data » afin de favoriser la circulation des données et du savoir. Cela devient obligatoire pour les administrations de publier en ligne des standards de leurs documents principaux ;
- renforcer les droits des personnes (via le droit de déréférencement, le droit à l'oubli des mineurs, le droit à la portabilité des données, etc.) afin que l'ouverture de l'accès aux données reste compatible avec la protection de la vie privée ;
- renforcer les pouvoirs de la CNIL, via notamment l'autorisation de certification de processus d'anonymisation des données par la CNIL ; ainsi que l'augmentation du montant des sanctions prononcées par la CNIL.

4.2. Règlement général sur la protection des données personnelles

Le Règlement Général sur la Protection des Données n°2016/679 du 27 avril 2016 (43), également appelé « RGPD », vient préciser l'encadrement et les traitements autorisés pour les données à caractère à personnel, tout en précisant qu'il est possible d'avoir des dispositions nationales relatives à la protection de ces données à caractère personnel. En France, la loi pour une République numérique avait déjà anticipé ces dispositions dès 1978. Suite au RGPD, les dispositions de cette loi ont été complétées, en allant davantage dans le sens de la protection des données personnelles et une plus grande responsabilisation des individus, qui se retrouvent au cœur du dispositif de protection des données. Les articles n'étant dorénavant plus applicables ont été supprimés. Le règlement, adopté par l'ensemble des Etats membres de l'Union Européenne le 27 avril 2016 et applicable depuis le 25 mai 2018, est relatif à la protection des données à caractère personnel et à la libre circulation de ces données. Il abroge la directive 95/46/CE et :

- renforce les droits des citoyens au respect de leur vie privée (également inscrits à l'art. 8 de la Convention Européenne des Droits de l'Homme) ;
- simplifie les formalités préalables pour les entreprises ;
- affirme les compétences et pouvoirs des autorités de contrôle et renforce la coopération des différentes parties prenantes.

Cette réglementation unique et harmonisée au sein de l'Union Européenne a eu un délai de 2 ans pour être applicable, afin que les entreprises se préparent à son entrée en application. Dorénavant, les données à caractère personnel doivent être (44):

- traitées de manière licite, loyale et transparente ;
- collectées selon des finalités déterminées, explicites et légitimes ;
- adéquates, pertinentes et limitées par rapport à la finalité poursuivie ;
- exactes et régulièrement mises à jour ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de manière sécurisée.

L'Europe est actuellement, via le RGPD, le modèle offrant la plus grande sécurité pour les données de santé des patients.

4.3. L'exemple des accords EU-US Privacy Shield

Au niveau international, d'autres réglementations existent afin d'assurer le respect de la protection des données à caractère personnel des membres de l'Union Européenne. C'est notamment le cas de l'accord EU-US Privacy Shield (45), entré en vigueur le 1er août 2016, qui est un accord réalisé entre l'Union Européenne et les Etats-Unis, afin de s'assurer que le transfert de données à caractère personnel vers les Etats-Unis soit encadré. Il s'agit d'un mécanisme d'auto-certification pour les entreprises installées aux Etats-Unis, qui est reconnu par la Commission européenne comme assurant un niveau de protection adéquat, et permet de transférer à une entreprise américaine des données collectées au sein de l'Union européenne.

4.4. Règlement européen sur les dispositifs médicaux

De par l'essor des applications mobiles et des objets connectés dans le domaine de la santé, il apparaît indispensable de réglementer leur utilisation et leur classification. En fonction de leur finalité, certaines applications et/ou objets connectés seront considérés comme des DM ou non. Les DM sont des produits très hétérogènes, le marché comporte donc des produits très variés et très nombreux. L'une des autres innovations en matière de réglementation concerne donc les dispositifs médicaux, avec le nouveau règlement européen sur les dispositifs médicaux (DM) n° 2017/45 (46) et le nouveau règlement sur les dispositifs médicaux de diagnostic in vitro (DMDIV) n°2017/746 (47). Entrés en vigueur le 26 mai 2017, ils devront être applicables dans un délai maximal de 3 ans pour les DM et de 5 ans pour les DMDIV.

L'objectif de ces règlements est d'harmoniser l'interprétation des directives DM, de renforcer la sécurité sanitaire des DM (suite au scandale de l'affaire PIP notamment), et surtout de lever les incertitudes règlementaires. Cela passe ainsi par :

- une extension du champ d'application de la réglementation ;
- une classification plus sévère des DM ;
- le remplacement des exigences essentielles des directives par des exigences plus générales, portant sur la sécurité et la performance des DM ;
- l'obligation d'établir un plan de surveillance, via la matériovigilance ;
- les nouvelles obligations que devront respecter les distributeurs des DMs ;
- la mise en place d'un système d'identification unique des DMs, afin d'assurer la traçabilité de ces derniers ;
- la désignation d'une personne chargée de veiller au respect de la réglementation ;
- le renforcement des exigences et contrôle des organismes notifiés ;
- la possibilité de retraitement de certains dispositifs à usage unique.

Ces règlements conservent les fondamentaux du marquage CE (marquage traduisant le fait qu'un dispositif est conforme aux exigences applicables au sein de l'UE et qu'il a été évalué), mais il détaille et renforce de nombreuses exigences.

4.5. Projet de loi relatif à la protection des données

Un autre projet de loi a été examiné en France en procédure accélérée : il s'agit de la loi n°2018-493 du 20 juin 2018, qui vient modifier la Loi Informatique et Libertés de 1978 afin de mettre en conformité le droit national avec le RGPD (48). Ce texte vient mettre à jour les dispositions qui entraient en contradiction avec l'actuel RGPD. Ce nouveau texte permet de conserver l'architecture de la Loi Informatique et Libertés, historiquement le premier texte français prévoyant des dispositions nationales pour assurer la protection des données à caractère personnel, mais vient préciser les marges de manœuvre laissées par le RGPD aux Etats membres. Il vient également élargir l'action de groupe aux fins de l'arrêt d'un traitement illicite et vient structurer davantage les pouvoirs de la CNIL, en lui permettant un alourdissement des sanctions.

III- Les données au cœur de la e-santé

Les données générées en santé sont extrêmement nombreuses et proviennent de sources très variées : on parle de Big Data en santé.

1. Le Big Data

Depuis une vingtaine d'années, le terme « Big Data », qui signifie « données massives », est utilisé. Il s'agit de l'ensemble des données générées et échangées de par le monde. Ces données sont extrêmement nombreuses, et cela s'explique par l'avènement des nouvelles technologies, d'internet et des réseaux sociaux, concomitamment aux capacités accrues de stockage sur les serveurs spécialisés. L'analyse et la collecte des données sont bouleversées par le Big Data.

Le Big Data est défini par 5 caractéristiques (ou « les 5V ») que sont le Volume, la Vélocité, la Variété, la Véracité et la Valeur :

- le volume renvoie aux quantités énormes de données créées à chaque instant. D'après IBM, 90% des données mondiales ont été créées au cours des deux dernières années (49). Les capacités actuelles de stockage permettent de les conserver, même si elles ne sont pas toutes exploitées. En effet, il est estimé que 88% des données actuellement disponibles ne sont pas analysées ;
- la vélocité renvoie à la vitesse avec laquelle une donnée est créée et se transmet. Le Big Data rend possible l'analyse en temps réel des données, en même temps qu'elles sont générées, sans avoir nécessairement besoin d'analyser soi-même des bases de données ;
- la variété renvoie aux différents types de données existantes et utilisables. De nos jours, les capacités actuelles des nouvelles technologies rendent possible l'analyse de cette grande variété de données, et qu'importe le type de donnée dont il s'agit ;
- la véracité renvoie à l'exactitude des données recueillies, et à leur fiabilité ;
- la valeur consiste à apporter une plus-value à ces données en masse.

En santé, le Big Data fait référence à l'ensemble des données socio-démographiques et de santé. Le Big Data bouleverse la manière d'aborder les patients en santé. Par exemple, il a fallu 10 ans pour séquencer un génome humain, alors qu'aujourd'hui grâce à ces nouvelles technologies et à cette quantité immense de données recueillies, cela se fait en une journée à peine. Identifier des facteurs de risques de maladies devient plus aisé, l'aide au diagnostic se développe, la pharmacovigilance s'adapte… Les capacités qu'offrent les technologies actuelles vont faire augmenter encore le volume de données disponibles. Ce qui représente une réelle opportunité pour prendre en charge les patients différemment, le Big Data étant synonyme d'innovation, de connaissance et de progrès médical.

2. Les sources de ces données en santé

Il existe en France plus de 260 bases de données publiques en santé (50). Le site internet Epidémiologie-France (https://epidemiologie-france.aviesan.fr/) recense à lui seul plus de 500 bases de données de référence dans différents domaines de la santé (médico-économie, cohortes, registres et études cliniques) (Figure 5).

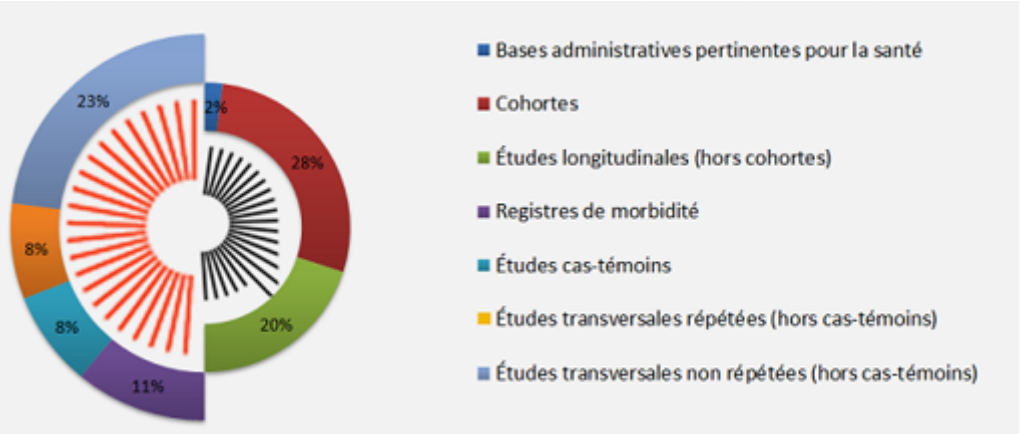

Figure 5 : Types de données recueillies sur le portail Epidémiologie-France (51)

Ces bases publiques mettent à disposition des agences sanitaires et organismes publics à but non lucratif des données fiables et représentatives de grandes populations. L'une des plus importantes bases de données médico-administratives permettant un suivi à long termes est celle du Système National d'Information Inter Régimes de l'Assurance Maladie (52) (SNIIRAM), qui contient l'ensemble des informations relatives aux remboursements réalisés par

l'Assurance Maladie, tout au long de la vie des assurés sociaux, qu'il s'agisse des données biologiques, des médicaments consommés, des consultations faites, etc.

Mais les données de santé sont également recueillies via les objets connectés, et sont également stockées par des organismes autres que des institutions de santé, tels que les GAFAM. D'où l'importance du respect de la confidentialité de ces données de santé sensibles.

C'est dans ce contexte que les législateurs se sont penchés sur la protection des données à caractère personnel et données de santé, afin de protéger les citoyens de l'usage pouvant en être fait et de leur permettre de pouvoir agir contre les mésusages potentiels. Le Règlement Général sur le Protection des données va en ce sens.

Partie 2 : Maitrise du traitement des données de santé sous l'égide du RGPD

I- Mettre en œuvre un traitement des données médicales en conformité avec le RGPD

1. Textes de références

Qui dit e-santé, dit utilisation et génération de Big-Data. Au nom du droit des patients, il est nécessaire que ces dernières soient correctement traitées et sécurisées. En France, il existe trois principaux textes de lois applicables pour assurer la protection des données :

- le Code de la Santé Publique ou « CSP », dans lequel lois et décrets sont codifiés. Les deux grandes dernières réformes le touchant sont la loi n° 2016-41 du 26 Janvier 2016 ainsi que la Loi pour une République numérique n°2016-1321 du 7 Octobre 2016 ;
- d'autres lois sont applicables : la Loi Informatique et Libertés n°78-17 du 6 Janvier 1978 telle que modifiée par la loi relative à la protection des données personnelles;
- enfin, le Règlement général sur la protection des données n° 2016/679 du 27 avril 2016, ou « RGPD ».

L'autorité compétente pour contrôler l'application de ces textes et le respect des données personnelles est la CNIL. Cette dernière vient accompagner les professionnels dans leur mise en conformité avec le nouveau RGPD, applicable depuis mai 2018, et vient également aider les particuliers à maitriser leurs données personnelles, en leur permettant de comprendre et d'exercer leurs droits.

Un des autres acteurs majeurs veillant au respect de l'application du RGPD et de sa conformité est le délégué à la protection des données, également appelé Data Protection Officer ou « DPO », qui vient assurer, et ce de manière indépendante, le respect des obligations prévues par la réglementation.

2. Périmètre

Afin de définir le périmètre et le champ d'application du RGPD, il faut en définir certaines notions.

Le terme de **donnée à caractère personnel** était défini par la LIL art. 2. al. 2 comme « *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* ». Le RGPD vient préciser dans l'art 4. 1) qu'il s'agit de « *toute information se rapportant à une personne physique identifiée ou identifiable* », c'est-à-dire la personne concernée. Il faut distinguer différents types de données à caractère personnel :

- les données directement identifiantes, telles que les noms, prénoms, les photos, les adresses mails nominatives, le numéro de sécurité sociale (également appelé Numéro d'Inscription au Répertoire ou « NIR », étant un code à 13 chiffres attribué par l'INSEE dès la naissance et permettant d'identifier de manière unique une personne), ou encore l'ADN ;
- les données indirectement identifiantes telles que des initiales, un numéro de téléphone, ou encore une plaque d'immatriculation.

Le **traitement des données à caractère personnel**, autrefois défini par la LIL art. 2 al. 3 en tant que « *toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* » ; est dorénavant davantage encadré par le RGPD art. 4. 2) en tant que : « *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* ».

Avant le RGPD, **la donnée de santé** n'était pas clairement définie en France. L'ASIP Santé indiquait qu'il s'agissait d'une *« donnée susceptible de révéler l'état pathologique de la personne* ». Dans l'art. 4. 15) du RGPD, est officiellement définie une donnée de santé, en tant que « *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* ».

Afin de savoir si une entreprise ou une personne est soumise aux obligations du RGPD ou d'une loi Nationale, elle doit vérifier si elle est :

- **responsable d'un traitement** (ou RT) : il s'agit de la personne, l'autorité publique, le service ou l'organisme qui détermine la finalité et les moyens du traitement mis en œuvre ;
- **un sous-traitant** (ou ST) : il s'agit de toute personne qui traite des données à caractère personnel pour le compte, pour le compte et sur instructions du responsable du traitement.

Ces personnes, physiques ou morales, sont soumises aux obligations du RGPD lorsqu'elles effectuent un traitement. En pratique, tout organisme, indépendamment de sa taille, de sa structure, de son activité ou de son pays d'origine ou d'implantation, peut potentiellement être concerné par le RGPD, qui s'applique :

- à toute entité traitant des données personnelles, dès lors que celle-ci est établie au sein de l'UE

- à toute entité située hors de l'Union européenne et traitant des données personnelles ciblant des personnes se trouvant au sein de l'UE.

Le RGPD s'applique également au traitement de données à caractère personnel par un responsable de traitement qui n'est pas établi au sein de l'UE mais dans un lieu où le droit d'un des Etats membres s'applique, et ce en vertu du droit international public.

Le RGPD entraîne ainsi une application territoriale élargie et s'applique :

- aux traitements effectués dans le cadre des activités de RT ou de ST, établis sur le territoire européen : il s'agit du critère de l'établissement ;

- également aux traitements qui sont effectués pour le compte de RT ou ST non établis sur territoire de l'UE dès lors qu'ils visent des personnes se trouvant sur le territoire de l'UE, via :
    - des offres de bien ou de services à ces derniers ;
    - le suivi d'un comportement au sein de l'UE.

La Figure 6 reprend le logigramme permettant de définir si une personne/entreprise est soumise au RGPD.

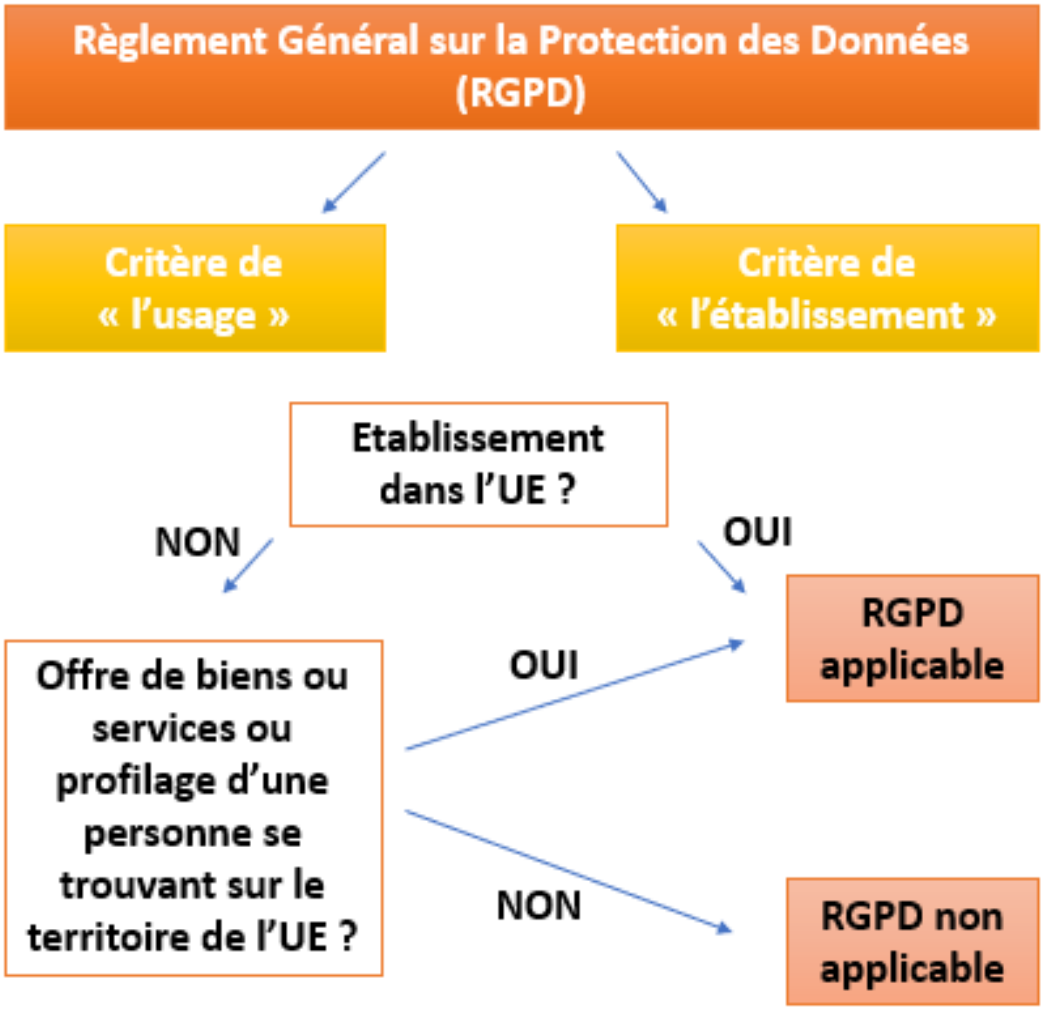

Figure 6 : Champ d'application du RGPD

3. Principes

En raison de la nature des données concernées par un éventuel traitement, le RGPD est venu détailler les principes auxquels chaque entité, physique ou morale, est soumise. Le respect de ces principes, « l'accountability », est de la responsabilité du responsable de traitement, qui est responsable d'agir au sein d'un processus dynamique et permanent de mise en conformité à la réglementation, et ce grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques adaptées.

Le traitement d'une donnée à caractère personnel, et donc d'une donnée de santé, doit respecter six grands principes :

- les données à caractère personnel doivent être traitées de manière licite, loyale, transparente ;
- les finalités doivent être limitées, déterminées, explicites et légitimes ;
- minimisation des données : la minimisation implique que les données à caractère personnel collectées doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Ce principe de minimisation des données est à mettre en œuvre au moment de la détermination des moyens du traitement et lors du traitement lui-même ;
- les données à caractère personnel se doivent d'être exactes et, dans la mesure du possible, tenues à jour. Toutes les mesures doivent être prises pour que les données inexactes soient effacées ou rectifiées ;
- limitation de la conservation des données à caractère personnel, pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- Intégrité et confidentialité : les données à caractère personnel doivent être traitées de manière 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 ou volontaire, à l'aide de moyens techniques et organisationnels appropriés.

La protection de la vie privée dès la conception de nouvelles technologies, ou « *privacy by design* » est un autre concept que le RGPD prend en compte dans son art. 25. Toute technologie qui traite des données à caractère personnel ou qui permet d'en traiter doit garantir, et ce dès sa conception et ensuite au cours de chaque utilisation (même si elle n'a pas été prévue à l'origine), un niveau de protection des données maximal. Ce principe vise à agir de manière proactive et préventive afin de limiter la violation de la protection des données.

L'article 25 du RGPD vient également introduire un autre concept : la protection de la vie privée par défaut, ou « *privacy by default* », qui vient préciser que quiconque réalise un traitement des données à caractère personnel doit permettre aux personnes dont sont issues ces données d'obtenir rapidement et aisément le plus haut niveau de protection possible. Cela correspond à l'ensemble des mesures techniques et organisationnelles appropriées pour garantir, par défaut, que seules les données à caractère personnel nécessaires au regard de chaque finalité du traitement seront traitées.

D'autres mécanismes apparaissent avec le RGPD (art. 42), avec dorénavant les mécanismes de certification, de marques et de labels au niveau européen, normes fixées et encouragées par la Commission et à destination des personnes concernées. Des codes de conduite sont également élaborés (art. 40 du RGPD) et sont « destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises » et élaborés par des associations ou organisations représentant des catégories de responsables de traitement ou de sous-traitants. Ces codes de conduites sont approuvés par l'autorité de contrôle du pays européen concerné (en France : la CNIL) et, le cas échéant, au Comité Européen de la Protection des Données (CEPD).

4. Principaux objectifs

Les principaux buts du RGPD s'inscrivent dans la politique e-santé 2020, avec le patient qui est mis au cœur du traitement de ses données, la responsabilisation des acteurs et la crédibilisation des autorités.

4.1. Repenser les données en plaçant les personnes concernées au cœur du traitement

Lorsque l'on parle de virage numérique et de transformation du système de santé, il ne faut pas oublier que le premier acteur concerné est le patient. Il est l'élément central de la transformation numérique. Le RGPD vient repréciser et renforcer les droits existants, avec :

- une obligation générale de faciliter l'exercice de leurs droits, en favorisant la communication d'informations précises, concises, transparentes, compréhensibles et accessibles facilement. Avec le RGPD, les RT et leurs ST doivent dorénavant être capables de fournir les données réclamées par les patients « dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande », tout en sachant que ce délai peut être prolongé de 2 mois sous certaines conditions (notamment si les données sont difficilement accessibles en raison de leur ancienneté) ;
- une information renforcée, que ce soit sur les coordonnées du délégué ou encore sur la durée de conservation de leurs données personnelles ;
- un droit d'accès aux données personnelles précisé et un droit de rectification maintenu ;
- un droit d'être informé en cas de violation de leurs données personnelles ;
- un droit d'opposition renforcé : le RT ou son ST doivent désormais justifier d'un intérêt légitime supérieur à celui de la personne concernée ;
- un droit d'effacement des données et un droit à l'oubli renforcé : les RT et leurs ST sont obligés de notifier à tout destinataire ses données rectifiées ou effacées.

Le RGPD vient également ajouter de nouveaux droits pour protéger les patients :

- le droit à la limitation du traitement, qui permet aux personnes de contester l'exactitude de leurs données utilisées par l'organisme en question et de s'opposer au traitement de ces données erronées (53) ;
- le droit à la portabilité des données, c'est-à-dire la possibilité de pouvoir récupérer l'ensemble de ses données, et de manière lisible (54).

En ce qui concerne le droit de la santé numérique, le RGPD doit également être en accord avec les règles générales du Code de la Santé Publique concernant le droit des personnes : le droit au respect de la vie privée (art. L. 1110-4), le droit des personnes (art. L. 1111-7) et le principe du secret médical partagé (art. L. 1110-4). Le RGPD vient compléter ces dispositions.

4.1.1. Renforcer le droit à l'information

Tout patient doit être mis au courant du traitement qui va lui être prodigué : c'est l'information préalable aux soins (art. L. 1111-2 du CSP), qui incombe à tout professionnel de santé et qui porte sur les différentes investigations, traitements ou actions de préventions proposées au patient, leur utilité, leur urgence éventuelle, leur conséquence, les risques fréquents ou graves prévisibles qu'ils comportent (55). Dans le cadre des données à caractère personnel, tout patient doit être informé du traitement qui lui sera fait.

4.1.2. Renforcer le droit d'accès

A cette obligation d'information s'ajoute pour tout patient le droit d'accès à son dossier médical (art. L. 1111-7 du CSP), c'est-à-dire à « l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit, par des professionnels et établissements de santé, qui sont formalisés ou ont fait l'objet d'échanges écrits entre professionnels de santé ». En ce qui concerne les données à caractère personnel, toute personne doit avoir accès à ses données.

4.1.3. Renforcer le consentement

Enfin, il est obligatoire de recueillir le consentement du patient (art. L. 1111-4 du CSP) : la décision médicale doit être prise conjointement par le patient dûment informé et par le professionnel de santé qui le prend en charge. Aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne. Des cas dérogatoires

existent toutefois : en cas d'urgence vitale pour le patient, d'impossibilité d'informer la personne, ou encore la volonté de la personne d'être tenue dans l'ignorance d'un diagnostic.

Il existe différents types de consentement : le consentement aux soins (Code de la Santé Publique), le consentement au partage de données médicales en dehors de l'équipe de soins (Code de la Santé Publique), le consentement au traitement des données à caractère personnel (Loi Informatique et Libertés et RGPD), ainsi que d'autres consentements (ex : dans les cas des cookies sur les sites internet, ou encore de géolocalisation).

Pour le traitement des données à caractère personnel, le consentement est défini comme « 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 caractères personnel la concernant fassent l'obligation d'un traitement » (56). Pour recueillir le consentement d'une personne sur ses données personnelles, via une application ou des sites web, il faut que lorsque cette dernière l'utilise elle :

- coche une case spécifique pour un site web ;
- opte pour certains paramètres techniques pour certains types de services ;
- mette en place une déclaration de consentement (possible par voie électronique) ;
- indique clairement par son comportement qu'elle accepte le traitement de ses données, sauf exigence de consentement exprès comme c'est le cas pour les données de santé.

Un consentement ne sera pas considéré comme valide si la personne a émis un consentement tacite et/ou passif, ou si certaines cases sont cochées par défaut.

Pour les mineurs, suite au débat parlementaire de l'Assemblée Nationale des 6 et 7 février 2018 sur le RGPD, il est prévu un « double consentement », de la part de l'enfant et de ses parents. D'après l'art. 7-1 du RGPD « *en application du 1 de l'article 8 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans. Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de la responsabilité*

parentale à l'égard de ce mineur (issu de l'amendement n°103). Le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne ».

Enfin, il faut également préciser que toute personne a le droit de retirer simplement, et à tout moment, son consentement. Le RGPD vient préciser cela, et également que la personne concernée doit être informée obligatoirement de cette faculté de retrait, et ce avant de donner son consentement.

4.2. Responsabiliser les acteurs

Comme indiqué précédemment, les données de santé font l'objet d'une protection spécifique par les textes, et le RGPD vient renforcer le droit des patients en ce sens. Mais il vient également responsabiliser les différents acteurs intervenant dans un contexte d'hyperconnexion et de multiplication du partage et d'échanges des données. Le RGPD s'appliquant à toute personne traitant des données à caractère personnel, il vient donc préciser les différentes responsabilités de chacun.

4.2.1. Traitement licite

Le RGPD vient détailler dans quels cas le traitement d'une donnée à caractère personnel est licite ou non. Pour être licite, le traitement doit respecter au moins l'une des mesures suivantes (57) :

- la personne concernée a émis son consentement libre et éclairé, sur une ou plusieurs finalités spécifiques. Par exemple, dans le cadre d'une application mobile en santé de « bien-être », tels qu'une application pour améliorer la qualité du sommeil ou encore pour assurer le suivi de son activité physique, il est indispensable de recueillir le consentement express de la personne, après qu'elle ait été dument informée que ses données de santé seront recueillies au niveau de cette application mobile téléchargée. A noter que si l'application mobile

téléchargée est utilisée en tant qu'outil de prise en charge sanitaire (comme c'est notamment le cas pour les applications utilisées dans le cadre de télésurveillance médicale), l'accord préalable de la personne n'est pas obligatoire (58) ;

- le traitement est nécessaire à l'obligation d'un contrat ou dans l'intention d'établir un contrat ;
- il en est de l'obligation légale pesant sur le RT ou dans le cadre de l'exécution d'une mission d'intérêt public, c'est-à-dire que le traitement est effectué dans le cadre d'une obligation légale ou encore dans le cas où il est indispensable à l'exécution d'une mission d'intérêt public ;
- il en est de l'intérêt vital de la personne concernée, ou d'une autre personne physique en jeu. C'est notamment le cas pour le traitement des données à finalité humanitaire ;
- il en est de l'intérêt légitime poursuivi par le RT ou par un tiers : cela s'apprécie au cas par cas, il faut évaluer si l'intérêt du RT prévaut ou non à l'intérêt et aux droit et libertés fondamentaux individuels. C'est le cas par exemple pour les campagnes d'e-mailing, qui doivent se conformer au RGPD via l'obtention explicite des consentements des abonnés concernés. De par le caractère personnel des données et informations échangées par email, le RGPD vient préciser les nouvelles obligations pour le RT et le ST.

Evoquées dans l'art 8-I de la LIL, le RGPD vient compléter dans son art. 9 le principe d'interdiction de traitement dans le cas des données dites « sensibles », c'est-à-dire des « données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». Si une personne physique ou morale traite des données sensibles, il ne s'agira pas d'un traitement licite, sauf si ce traitement fait partie des exceptions annoncées à l'art. 9 du RGPD.

4.2.2. Suppression des formalités et nouveaux outils

L'objectif du RGPD est de supprimer les formalités préalables au traitement des données à caractère personnel, et de laisser des « marges de manœuvre » aux personnes pouvant traiter des données, si elles ont respecté certaines dispositions initiales. En contrepartie, le RT doit être :

- en conformité avec les dispositions du RGPD ;
- et en mesure de le démontrer.

Pour ce faire, de nouveaux outils sont donc mis en place. Dorénavant, il est obligatoire de tenir un registre des activités de traitements (art. 30 RGPD), pour le RT mais également pour le ST.

Les entreprises réalisant des traitements doivent également nécessairement réaliser des analyses d'impact, pour :

- les traitements présentant des risques particuliers du fait de leur nature, de leur portée et/ou de leur finalité ;
- les traitements présentant des risques particuliers tels que la surveillance à grande échelle d'une zone accessible à tous ou encore le traitement à grande échelle d'informations sensibles ;
- les traitements considérés par l'autorité de contrôle comme étant susceptibles de présenter des risques spécifiques pour les droits et libertés des personnes concernées.

L'analyse d'impact doit prendre en compte le contexte général du traitement (la description fonctionnelle de la méthodologie, le type de données traitées, quels supports sont utilisés, etc.) ; évaluer si les principes fondamentaux sont respectés (proportionnalité et nécessité du traitement, quelles sont les mesures protectrices pour assurer le respect des droits des personnes) ; mesurer les risques liés à la sécurisation des données (déterminer les mesures existantes ou prévues et apprécier les risques) ; et valider le plan PIA ou « Privacy Impact Assessment », qui regroupe les différentes portées du traitement et mesures prises pour en limiter les risques.

Le Correspondant Informatique et Libertés (ou « CIL ») est supprimé pour être remplacé par le Data Protection Officer, dont la désignation dans les entreprises est obligatoire dans trois cas :

- lorsqu'il s'agit d'organismes ou d'autorités publiques, tels que les hôpitaux ;
- lorsque les activités de base de l'organisme, du fait de leur nature, de leur portée ou de leurs finalités, exigent un suivi systématique et régulier des personnes concernées, et ce à grande échelle ;
- lorsque les activités de bases du RT ou de son ST correspondent à un traitement de données sensibles et de données à caractère personnel relatives à des condamnations pénales et/ou à des infractions, et ce à grande échelle.

Il est choisi en fonction de ses connaissances et qualités professionnelles, en particulier en droit des nouvelles technologies. Pour les groupes d'entreprises, le RGPD vient également préciser qu'il peut y avoir un DPO mutualisé, sous réserve qu'il soit joignable et accessible aisément pour chacune des entreprises. Il doit s'assurer que son employeur et/ou ses clients respectent la législation pour l'utilisation des données à caractère personnel. Agissant en toute indépendance et confidentialité dans l'accomplissement de ses missions, il doit, d'après l'art. 39 du RGPD :

- informer et conseiller sur les obligations du responsable de traitement et/ou du sous-traitant ; mais également sur l'analyse d'impact ;
- contrôler la mise en œuvre de l'application du RGPD en interne, le respect des procédures et des politiques d'entreprises en matière de protection des données à caractère personnel ;
- vérifier la mise en place de l'analyse d'impact et répondre aux demandes de l'autorité de contrôle et/ou des personnes concernées ;
- être l'intermédiaire entre l'autorité de contrôle et les personnes concernées ;
- veiller à la bonne tenue des registres de traitement.

Le RGPD vient également apporter des spécificités pour le traitement des données de santé : l'art. 9.4 du RGPD prévoit en effet que « les Etats membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la

santé ». Ainsi, dans le projet de loi français relatif à la protection des données personnelles, il est précisé que les traitements concernant les données de santé des personnes sont soumis à un nouveau chapitre IX « Traitement de données à caractère personnel dans le domaine de la santé » ; et qu'ils ne peuvent être mis en œuvre que si :

- des référentiels et des règlements types sont établis par la CNIL ;
- les traitements étant conformes aux référentiels peuvent être mis en œuvre si les RT et/ou leur ST ont adressé une attestation préalable de conformité auprès de la CNIL ;
- qu'en cas de traitement non conforme aux référentiels, ces derniers pourront éventuellement être mis en œuvre si autorisation de la CNIL après évaluation individuelle.

L'ensemble de ces nouveautés vient responsabiliser les entreprises et permet une internalisation de la conformité des entreprises avec le nouveau RGPD.

4.2.3. Sécurisation et confidentialité des données

Afin d'assurer une sécurisation optimale des données à caractère personnel, la CNIL émet des recommandations (à adapter en fonction de chaque utilisation) telles que l'adoption de « mesures physiques » (ex : l'accès aux locaux réglementé, la protection des données via des supports d'archivages présentant une garantie suffisante) ainsi que de « mesures logistiques » telles qu'une authentification forte et un chiffrement des sauvegardes. Le RGPD vient préciser dans son article 32 que « *compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».

En concertation avec l'ensemble des acteurs du domaine de la santé et du médico-social, , il a été décidé dans l'art. L. 1110-4-1 du CSP que pour les données personnelles de

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

- le chiffrement, qui est un procédé cryptographique permettant de garantir la confidentialité d'une information (59);
- l'identification des opérateurs qui devient essentielle, afin de mettre en place des mesures harmonisées au sein de l'UE et d'assurer un niveau commun de sécurité des réseaux et SI. La directive NIS n°2016/1148, transposée en droit français par la loi n° 2018-133 le 26 février 2018 vient préciser que « *les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services sont soumis aux dispositions du présent chapitre. Ces opérateurs sont désignés par le Premier ministre. La liste de ces opérateurs est actualisée à intervalles réguliers et au moins tous les deux ans*. » ;
- l'anonymisation des données qui est « le résultat du traitement de données personnelles afin d'empêcher de façon irréversible, toute identification » (60). La CNIL doit dorénavant certifier la conformité des processus d'anonymisation ;
- La pseudonymisation qui correspond au « traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » art. 4.5° du

RGPD. L'objectif est d'empêcher que les données à caractère personnel pseudonymisées puissent être attribuées à une personne précise, sans avoir à recourir à d'autres informations détenues de manière sécurisée et séparée. La différence entre l'anonymisation et la pseudonymisation des données à caractère personnel est que l'anonymisation est faite de manière irréversible.

L'ensemble de ces moyens doit être appliqué afin d'assurer une sécurisation optimale des données à caractère personnel de santé.

4.2.4. Sous-traitance du traitement

Il existe une grande variété de ST, et leurs activités peuvent concerner une tâche précise ou plus étendue. Avec le RGPD, le ST devient lui aussi soumis à des règles, dans la logique de responsabilisation des acteurs impliqués dans le traitement des données à caractère personnel. Ils doivent ainsi :

- conserver une trace de toutes leurs activités de traitement (art. 30 du RGPD) ;
- coopérer avec l'autorité de contrôle (art. 31 du RGPD) ;
- mettre en place les mesures techniques et organisationnelles afin de garantir un traitement conforme des données (art. 32 du RGPD) ;
- informer le RT, dans les meilleurs délais à compter de la connaissance du fait, d'un cas de violation de données (art. 33 du RDPG) ;
- désigner un DPO (art. 37 du RGPD) ;
- respecter les règles inhérentes au transfert de données vers un pays tiers (art. 44 du RGPD) ou des organisations internationales (art. 45 du RGPD).

4.2.5. Violations des données

En cas de violation des données, le RT doit le notifier auprès de l'autorité de contrôle, et ce dans les meilleurs délais (au plus tard 72h après la connaissance du fait) d'après l'art. 33 du RGPD. La notification doit décrire :

- la nature de la violation des données, le nombre de personnes concernées, le nombre de données concernées ;
- l'identité et les coordonnées du DPO ;
- la description des conséquences de la violation ;
- la description des mesures prises par le RT pour remédier à cette violation des données et en atténuer les conséquences.

Après avoir informé l'autorité de contrôle, ils doivent également en informer les personnes concernées (art. 34 du RGPD), car cela entraine un risque élevé pour leurs droits et libertés fondamentales. Enfin, le RT doit établir un registre de violation des données (art.33 du RGPD) pour documenter tous les types de violation de données à caractère personnel, leurs effets et les mesures prises pour y remédier. Cela permet ainsi d'assurer une traçabilité en interne ; de démontrer à la CNIL et le RT un niveau optimal de sécurisation des traitements des données ; et de participer au respect du principe d'accountability. A ces obligations s'ajoute celle, depuis le 1er octobre 2017, du signalement des incidents de sécurités des SI numériques de santé sur une plateforme dédiée (art. L. 1111-8-2 du CSP et décret du 12 octobre 2016) : signalement.social-sante.gouv.fr (61). Toute action de suspicion ou encore de malveillance, pouvant entraîner des contraintes partielles ou totales des SI, une altération ou encore une perte potentielle de données doit y être signalée obligatoirement par :

- les établissements de santé ;
- les hôpitaux des armées ;
- les laboratoires de biologie médicale ;
- les centres de radiothérapie.

Il faut ainsi déclarer tous les incidents de sécurité graves ayant potentiellement des conséquences sur la sécurité des soins ; sur la disponibilité, la confidentialité ou encore l'intégrité des soins ; ou encore sur le bon fonctionnement de l'établissement (62).

4.2.6. Transfert hors Union Européenne

Il faut également assurer un niveau de sécurisation des données suffisant lors de transfert de données à caractère personnel. Deux cas sont à distinguer : les pays destinataires disposant

d'un niveau suffisant de sécurité (ex : la Suisse, le Canada ou encore les Etats-Unis avec le Privacy Shield) où les obligations du RT/ST sont bien précisées et à respecter ; et les pays ne disposant pas d'un niveau suffisant de protection adéquat.

Le RGPD a introduit de nouveaux outils juridiques pour encadrer les transferts de données à caractère personnel hors UE, pour ces pays ne disposant pas d'un niveau suffisant de protection. Il peut ainsi s'agir :

- d'une décision d'adéquation (art. 45 du RGPD) sur l'encadrement des données. Cette décision est prise suite à un examen global de la législation en vigueur de l'Etat ou du territoire au sein duquel seront stockées ces données ;
- dans le cas où aucune décision d'adéquation n'est prise, l'art. 46 du RGPD introduit des « garanties appropriées » correspondant pour la majorité de décisions des autorités de contrôle en présence, et étant prises via des engagements des organismes concernés.

Si aucune garantie appropriée n'est prise, le transfert peut toutefois se faire « par dérogation » aux outils d'encadrement, en cas de situation particulière et spécifique. Les mécanismes d'autorisation des transferts sous le RGPD sont détaillés dans le tableau 1 ci-dessous.

Tableau 1 : mécanismes d'autorisation de transferts de données à caractère personnel hors Union Européenne sous l'égide du RGPD.

Mécanismes actuels d'encadrement des transferts restant valables	**Nouveaux mécanismes d'encadrement des transferts autorisés**
- décision d'adéquation de la Commission européenne pour les pays permettant un niveau de protection suffisant ; - délivrance par la Commission européenne de clauses contractuelles types (CCT) ; - des règles internes d'entreprises ; - des clauses contractuelles spécifiques, jugées conformes aux clauses de la Commission européenne.	- des clauses contractuelles types ayant été adopté par une autorité de contrôle et approuvée par la Commission européenne ; - un code de conduite approuvé ; - un mécanisme de certification approuvé ; - un arrangement administratif ou un texte juridique contraignant et exécutoire pour permettre une coopération avec les autorités publiques.

4.3. Crédibiliser les autorités

Afin d'assurer la crédibilité des autorités de contrôle, il faut qu'elles aient la possibilité d'appliquer des contrôles et des sanctions pour les personnes ne respectant pas le nouveau RGPD. Dans ce dernier, il est ainsi précisé que les RT et/ou ST ne respectant pas les obligations liées au traitement des données à caractère personnel peuvent être soumis à des sanctions administratives qui sont dans l'ordre crescendo de gravité : un avertissement ; un rappel à l'ordre ; l'ordre de satisfaire aux demandes d'une personne concernée ; l'ordre de se conformer avec injonction ou non ; l'ordre de communiquer à la personne concernée une violation ; l'ordre de rectifier et/ou effacer des données ou limiter le traitement ; le retrait de la certification ; la suspension des flux hors-UE ; ou encore une amende administrative dont le montant peut varier (63). Les sanctions pécuniaires en regard de ces infractions sont présentées dans le tableau 2.

Tableau 2 : sanctions administratives pouvant impacter le responsable de traitement ou le sous-traitant ne respectant pas les obligations du RGPD pour les données à caractère personnel, d'après les art. 58 et 83 du RGPD.

Activité sanctionnée	Montant maximal de la sanction administrative
1) Absence de protection des données dès la conception et protection des données par défaut 2) Absence de représentant établi au sein de l'UE 3) Absence de registre des activités de traitement 4) Absence de coopération avec l'autorité de contrôle 5) Absence de notification à l'autorité de contrôle ou à la personne concernée d'une violation de ses données 6) Absence d'analyse d'impact	10 000 000€ ou 2% du chiffre d'affaire annuel mondial
1) Non-respect des principes de base d'un traitement d'une donnée à caractère personnel (licéité, loyauté, légitimité, adéquation et pertinence des données, consentement, données sensibles, etc.) 2) Non- respect du droit des personnes 3) Non-respect des règles relatives au transfert de données à caractère personnel hors UE - Non-respect d'une injonction d'une autorité, d'une limitation du traitement, etc.	20 000 000€ ou 4% du chiffre d'affaire annuel mondial

Sont pris en compte différents facteurs dans la sanction, tels que : la nature, la gravité et la durée de la violation ; le nombre de personnes concernées et le niveau de dommages subis ; les mesures prises pour atténuer ces dommages ; le type de donnés à caractère personnel

concernées ; le degré de coopération avec l'autorité de contrôle etc. D'après l'art. 82 du RGPD, toute personne qui a subi un dommage, qu'il soit matériel ou moral, du fait d'une violation du règlement pour exiger réparation dans sa totalité auprès du RT ou du ST responsable.

Le cas d'un praticien hospitalier qui avait créé une plateforme afin de permettre la prise en charge de patients mais sur un site hébergeur ne disposant pas de la certification pour être hébergeur de données de santé, peut par exemple être cité (64). Un patient avait porté plainte contre l'hôpital pour violation du secret professionnel, car il avait pu retrouver sur internet ses données médicales ainsi que celles de son fils. Après enquête, le praticien hospitalier a été condamné en Juin 2017 à payer 5 000€ d'amende pour avoir mis en place un traitement de données à caractère personnel illicite ; et le ST n'a pas été condamné, car le RGPD n'était pas encore entré en vigueur. Dorénavant, en raison de la responsabilisation des acteurs, il aurait également pu être condamné en tant que ST de données à caractère personnel.

II- Maitriser le partage des données dans le cadre de la sécurisation des systèmes d'information de santé

Lorsque les données à caractère personnel de santé sont traitées, elles peuvent l'être par différents intervenants, et le secret professionnel peut être partagé. Il est alors important de définir qui est soumis au dit secret professionnel. L'art. L.1110-4 du CSP vient définir les personnes tenues au secret professionnel (« tout professionnel (…) tous les professionnels intervenant dans le système de santé ») ainsi que les règles d'échange et de partage de données de santé.

L'échange de données de santé est réalisé entre professionnels identifiés, participant à la coordination, la continuité des soins et le suivi social et médico-social d'un même patient. Le patient doit être informé au préalable et a un droit d'opposition sur l'échange de ses données à caractère personnel. Le partage de données de santé est réalisé entre professionnels participant à la coordination, la continué des soins et le suivi social et médico-social d'un même patient au sein de la même équipe de soins (auquel cas le consentement du patient est requis et il peut toujours exercer son droit d'opposition) ou en dehors de la même équipe de soins (le patient doit alors fournir un consentement exprès).

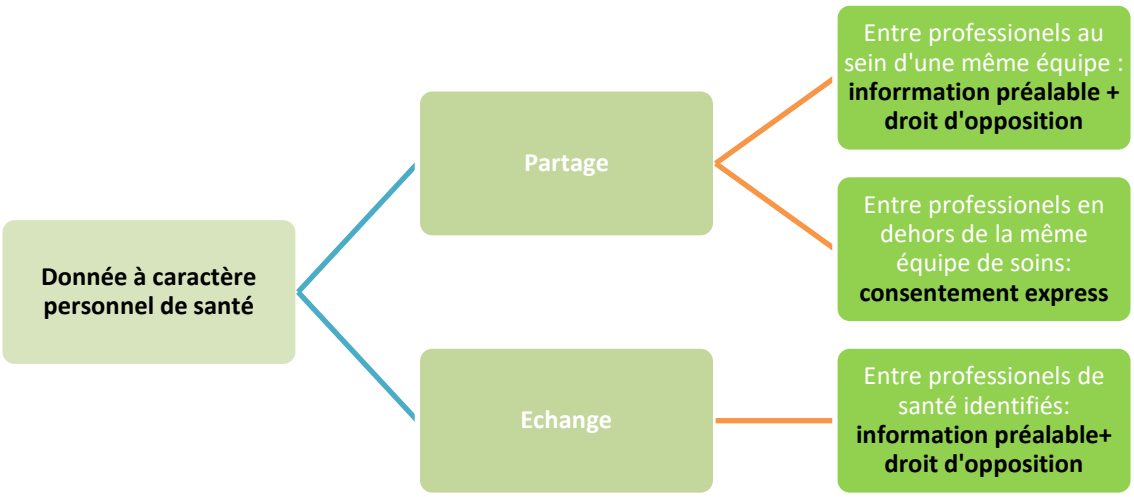

Figure 7 : définition des échanges et partages de données à caractère personnel de santé

D'après l'art. L. 1110-12 du CSP, le régime d'échange et de partage de données de santé est dorénavant fondé sur la notion d'équipe de soins, c'est-à-dire sur « *l'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 actes* » et qui :

- exercent dans la même structure : les établissements de santé, les établissements de service sociaux et médico-sociaux, les structures de coopération, etc. ;
- ou se sont vu reconnaitre cette qualité par le patient ;
- ou encore qui exercent dans un ensemble comprenant au moins un établissement de santé et qui respectent un cahier des charges.

Lorsque l'on parle d'échange et de partage de données, il faut donc prendre en compte cette dimension d'équipe de soins dans sa globalité, et s'assurer de la maitrise du partage des informations à caractère personnel (Figure 7). Les dossiers partagés de données à caractère personnel de santé existant à l'heure actuelle sont : le Dossier Médical Partagé ou « DMP » ; le Dossier Pharmaceutique ou « DP » ; le Dossier Communiquant de Cancérologie ou « DCC » ; ainsi que les dossiers de partage entre professionnels de santé (exemple : le programme TERR-eSANTE (65) d'île de France).

Il faut également informer le patient pris en charge par cette équipe de soins qu'il a le droit de s'opposer au partage des données de santé le concernant, et de l'informer sur son consentement. En effet, les conditions dans lesquelles ce dernier est recueilli font l'objet d'un décret qui stipule que le consentement doit être recueilli par le professionnel de santé qui prend en charge le patient ; doit être strictement limité à la durée de la prise en charge du patient ; et qu'il doit être recueilli par tous moyens, y compris de manière dématérialisée.

III- Maitriser le cadre législatif et réglementaire de l'hébergement de données de santé

Afin d'assurer un hébergement licite des données de santé, il faut s'assurer que l'hébergeur est correctement habilité à héberger des données à caractère personnel. Le RGPD fait évoluer la labellisation vers la certification. Concomitant au RGPD, le mécanisme d'agrément des hébergeurs a été remplacé par le principe de certification des hébergeurs de données, définit à l'art. L.1111-8 du CSP (66), c'est-à-dire que « *Toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article. L'hébergement, quel qu'en soit le support, papier ou numérique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime. La prestation d'hébergement de données de santé à caractère personnel fait l'objet d'un contrat* ».

Cette certification est effectuée par un organisme certificateur, lui-même accrédité par le COFRAC (Comité Français d'Accréditation) après examen et évaluation de l'aptitude à héberger des données de santé en toute sécurité et avec respect des réglementations en vigueur. La certification est attribuée pour 5 ans. Toujours dans un souci de responsabilisation des acteurs, la certification doit être partagée par l'ensemble des acteurs participant à l'hébergement des données de santé.

IV- Premiers résultats depuis l'instauration du RGPD

Le RGPD est entré en application depuis le 25 mai 2018. L'Europe est depuis le nouveau modèle à suivre en matière de protection des données à caractère personnel, car elle offre le niveau de protection le plus élevé. L'ensemble des entreprises et des collectivités doivent se mettre en conformité avec le RGPD, sous peine de subir des sanctions pouvant aller jusque 4% du chiffre d'affaires mondial ou 20 millions d'euros (le montant le plus élevé étant retenu).

Une centaine de jours après la mise en place du nouveau règlement, la CNIL révèle avoir été saisie de 3767 plaintes contre 2294 sur la même période en 2017, soit une hausse de 64% (67). Cette augmentation du nombre de plaintes déposées est concomitante à la médiatisation de l'affaire Cambridge Analytica en mars 2018, où Facebook a été accusé de partager massivement les informations de ses utilisateurs pour les revendre (68).

Cela ne fait aucun doute : cette évolution du nombre de plaintes déposées fait suite à la prise de conscience des citoyens sur le caractère personnel de leurs données, et qu'ils sont plus à même de les contrôler grâce au nouveau RGPD, afin d'en limiter les utilisations illicites par des tiers. Ils ne sont plus passifs face à cette collecte massive de données, ils peuvent devenir acteurs et récupérer leurs données à tout moment. Les usages illicites sont dorénavant sanctionnables, et des moyens de recours existent pour le faire savoir. Ce règlement vient offrir ce droit légitime à tout citoyen de maitriser l'usage fait de ses données à caractère personnel. Et cela s'applique également pour les données à caractère personnel de santé, collectées via les objets connectés ou via les circuits plus « classiques » tels que les études cliniques ou encore les données recueillies en établissements de santé. Chacun doit voir sa liberté et ses droits respectés. Comme le disait Julien Green « être libre, ce n'est pas seulement ne rien posséder, c'est n'être possédé par rien », et donc ne pas voir ses données utilisées par des tiers sans consentement donné de manière explicite et éclairée.

Partie 3 : place de la e-santé et du Big Data dans le système de soins de demain

Avec le développement du Big Data et l'obtention exponentielle de données de santé, il apparait évident que la prise en charge des patients est en cours de modification, voire de révolution. L'accélération de l'avancée technologique fait croître encore davantage le volume de données disponibles. Cette source intarissable de connaissances est une réelle avancée pour favoriser l'innovation et les progrès médicaux. L'exploitation de ces données est un réel avantage pour identifier des facteurs de risques de maladie, aider au diagnostic ou encore au choix des traitements. L'exploitation de ces données massives constitue donc un réel levier pour comprendre les maladies, assurer le développement des médicaments et de la prise en charge des patients. Le Big Data génère beaucoup d'attentes en santé, et répond à de réels enjeux économiques pour le système de santé, mais également éthiques.

I- Big Data et santé publique

L'analyse et l'exploitation des données de santé venant de sources très disparates constitue un réel avantage en santé publique et permet d'envisager de réels progrès en matière d'avancée scientifique, de prévention de la santé des populations et de diminution des risques sanitaires.

L'OMS définit la prévention en santé publique comme « la science et l'art de favoriser la santé, de prévenir les maladies et de prolonger la vie grâce aux efforts organisés de la société » (69). La prévention consiste donc à prendre l'ensemble des moyens nécessaires pour diminuer la survenue de maladies, d'empêcher leur gravité et leurs conséquences. L'utilisation du Big Data joue donc un rôle indispensable en prévention, car il permet de collecter, de stocker et de traiter un grand nombre de données en temps réel sur l'état de santé des populations. La rapidité de traitement de ces données rendue possible par les nouvelles technologies et la diffusion des objets connectés révolutionne les approches plus traditionnelles en matière de prévention.

La compréhension des problèmes sanitaires repose sur l'analyse des données recueillies en temps réel. L'épidémiologie, qui consiste à mesurer, analyser et expliquer des évènements sanitaires sur une population donnée, se base également sur l'analyse de données recueillies en temps réel. De nos jours, avec le Big Data, les données obtenues de sources différentes et traitées très rapidement sont bien plus nombreuses et permettent d'envisager un nouvel usage en santé publique. Encore sous-utilisées, ces données massives offrent de réelles perspectives de connaissances et de prévention des maladies, de surveillance et de veille sanitaire, afin de mieux comprendre et de détecter plus rapidement les évènements de santé inhabituels, pouvant potentiellement engendrer des crises sanitaires. Correctement analysées, elles peuvent également permettre de personnaliser les actions de préventions vers les personnes les plus ciblées, et ainsi renforcer les messages de prévention. Enfin, l'analyse des data permet de participer au suivi et à l'analyse d'actions en santé publique. Le RGPD parle de « finalité compatible », c'est-à-dire la possibilité d'utiliser en toute légalité des données de santé, si ces dernières sont utilisées à des fins compatibles avec un intérêt général tout en respectant le droit des personnes. La finalité compatible s'applique quand on veut traiter les données pour une nouvelle finalité, qui doit donc être compatible par rapport à la finalité initiale. Il est donc question soit de finalité légitime pour l'utilisation des données, soit de finalité compatible pour une réutilisation des données.

1. Usage en pharmacovigilance

Discipline de la pharmacoépidémiologie, la pharmacovigilance se base sur l'analyse de données et est définie comme « la surveillance des médicaments et la prévention du risque d'effet indésirable résultant de leur utilisation, que ce risque soit avéré ou non » (70).

Auparavant, les données de santé étaient recueillies via des collectes de données « ad hoc », sur la base de certains critères et sur des durées très longues. Elles étaient également recueillies via les actes de soins ou lors de la demande de remboursements de certains médicaments ou actes médicaux, où encore lors de la déclaration d'évènements indésirables liés à des prises médicamenteuses. Dorénavant, les data peuvent être recueillies directement par les patients, via les objets connectés, l'internet et ses réseaux, et permettent de constituer

une source inépuisable de données pour identifier certains facteurs de risques sanitaires. A cette source de données supplémentaires plus exactes (car obtenues davantage en temps réel) s'ajoute la rapidité de leur analyse, rendue possible grâce à l'IA.

Le système de pharmacovigilance français fait partie intégrante du système européen de pharmacovigilance, ce qui permet une identification et un échange d'informations plus rapide et efficace sur les problèmes de pharmacovigilance, et d'envisager des mesures harmonisées et synchronisées pour répondre aux problèmes sanitaires. Mais, malgré cette volonté communautaire européenne de détecter les signaux d'alertes, certaines crises sanitaires n'ont été détectées que trop tardivement, notamment en raison de l'absence ou de l'insuffisance de données précises sur les médicaments et leur mésusage (71). Les scandales sanitaires du Médiator, des pilules de 3^{e} et 4^{e} générations ou encore de la Dépakine auraient peut-être pu être évités si les données recueillies par les Centre Régionaux de Pharmacovigilance (CRPV) avaient été plus nombreuses et analysées plus rapidement. Pendant des années, il y a eu mésusage de médicaments entrainant des effets dramatiques en santé publique et très couteux pour l'Etat. Au niveau européen, il est estimé que 197 000 morts par an sont liés à un mésusage des médicaments ; et l'impact économique est estimé à 79 milliards d'euros par an (72). La France étant l'un des pays européens ayant la plus forte consommation de médicaments, s'assurer du bon usage de ces derniers et de la bonne détection des effets indésirables associés à leur consommation s'impose comme étant l'un des plus gros sujets de santé publique.

La pharmacovigilance repose principalement sur des actions d'évaluation mises en place après la commercialisation des médicaments. Les données collectées durant les études cliniques vont être complétées par celles recueillies par les CRPV après la mise sur le marché des médicaments. L'analyse des données recueillies sur ce long terme peut permettre de détecter les signaux et déclencher des alertes sur de possibles effets indésirables ou sur des cas de mésusages.

Une multitude de facteurs et de données sont à prendre en compte et à analyser dans la gestion de ces crises : le Big Data et l'analyse rapide réalisée par l'IA peuvent permettre d'en améliorer le système. Plus l'évènement est connu précocement, plus la connaissance associée et le plan d'actions en santé publique pourront être élaborés.

2. Usage en prévention et suivi des épidémies

Combiné aux nouvelles technologies, l'utilisation de données recueillies en temps réel et en grandes quantité et variété peut permettre d'évaluer et de déterminer l'état de santé des populations à un temps t et sur une zone géographique déterminée. Les modèles épidémiologiques se développent, orientés dans le suivi de la propagation des évènements sanitaires tels que les épidémies, à partir de l'analyse des données recueillies en masse mais également des analyses plus traditionnelles de recueil de données, tels que le réseau sentinelle français (73).

L'usage du Big Data en épidémiologie n'est pas nouveau, et a démarré depuis plus de 10 ans au sein de plusieurs entités, telles que l'InVS (Institut National de Veille Sanitaire), l'INPES (Institut National de Prévention et d'Education pour la Santé) ou encore l'EPRUS (Etablissement de Préparation et de Réponse aux Urgences Sanitaires). La variété des données recueillies via des sources intarissables et stables telles que le PMSI (Programme de Médicalisation des Systèmes d'Information), le SNIIRAM, le CepiDC (Centre d'Epidémiologie sur les Causes Médicales de Décès) ; mais également via d'autres bases de données telles que le registre des cancers permettent d'élaborer des analyses épidémiologiques plus poussées et de développer des systèmes de surveillance épidémiologique. Le logiciel Sursaud (Surveillance Sanitaire des Urgences et des Décès) qui a été élaboré suite à la canicule des années 2000 en France et analyse les données de diverses sources en temps réel, peut ainsi être cité en exemple. Tous ces éléments permettent d'élaborer le BQA (Bulletin Quotidien des Alertes), à destination de l'Etat français, qui va ensuite élaborer des stratégies sanitaires adaptées aux informations recueillies. Ce genre de système permet de détecter précocement des évènements sanitaires non prévisibles ou prévisibles (tels que la grippe saisonnière), d'en estimer l'impact potentiel et de surveiller des maladies.

Ces modèles n'ont pas encore révélé l'ensemble de leur potentiel, mais leur utilisation est de plus en plus courante et pertinente. Par exemple, certains signaux sont couramment utilisés, tels que l'analyse de la fréquence de consultation de diverses pages internet où l'utilisation de mots-clés, afin de déterminer, plus ou moins précisément, l'apparition de maladies saisonnières. L'utilisation des données recueillies via les smartphones peuvent

également permettent de décrire précisément la propagation de maladies via les mouvements de foule et l'analyse de leurs recherches sur smartphones (74). La société HealthMap, spécialisée dans le Big Data en santé, affirme avoir détecté une épidémie de fièvre hémorragique Ebola 9 jours avant que l'OMS n'en fasse l'annonce officielle (75), via l'analyse des réseaux sociaux, des informations locales africaines et d'autres bases de données. Ce logiciel a été développé afin de détecter les épidémies naissantes de par le monde, afin de les prendre en charge le plus rapidement et d'en diminuer la sévérité.

Lorsque l'on sait à quel point le délai de prise en charge doit être le plus court possible pour contenir les épidémies, l'utilisation des Big Data prend tout son sens en santé. L'amélioration continue des algorithmes et l'obtention exponentielle de données de santé pourront permettre de prédire et/ou de détecter, in fine, la majorité des événements sanitaires, tout en gardant un délai suffisant d'analyse de ces données afin d'utiliser uniquement celles pertinentes.

3. Evaluation et anticipation de l'adhérence à un traitement

Il apparait également intéressant d'utiliser le machine learning pour combiner les données socio-économiques et géographiques (pour une majorité non utilisées dans le domaine de la santé) aux données médicales classiquement utilisées, afin d'anticiper l'adhérence à un traitement donné (Figure 8). La prise en charge des patients pourrait ainsi être optimisée et personnalisée, en privilégiant par exemple l'utilisation de certains moyens pour les patients les plus exposés à des risques identifiés, et dont les données actuelles révèlent qu'ils pourraient être réfractaires à certains types de traitements et pas à d'autres. Cette approche prédictive, encore peu utilisée en santé publique mais très courante pour analyser les comportements d'achats, pourrait améliorer la prise en charge des patients en en proposant une qui soit la plus adaptée en fonction de l'historique et des antécédents en santé. L'utilisation de données de santé des patients doit être néanmoins anonymisée, même si dans certains pays tels que les Etats-Unis, ces dernières sont accessibles à tous. Les données comportementales des populations et leur analyse peuvent permettre d'adapter le traitement et d'anticiper les bénéfices attendus sur leur état de santé, ainsi que leur adhérence à un type de traitement donné.

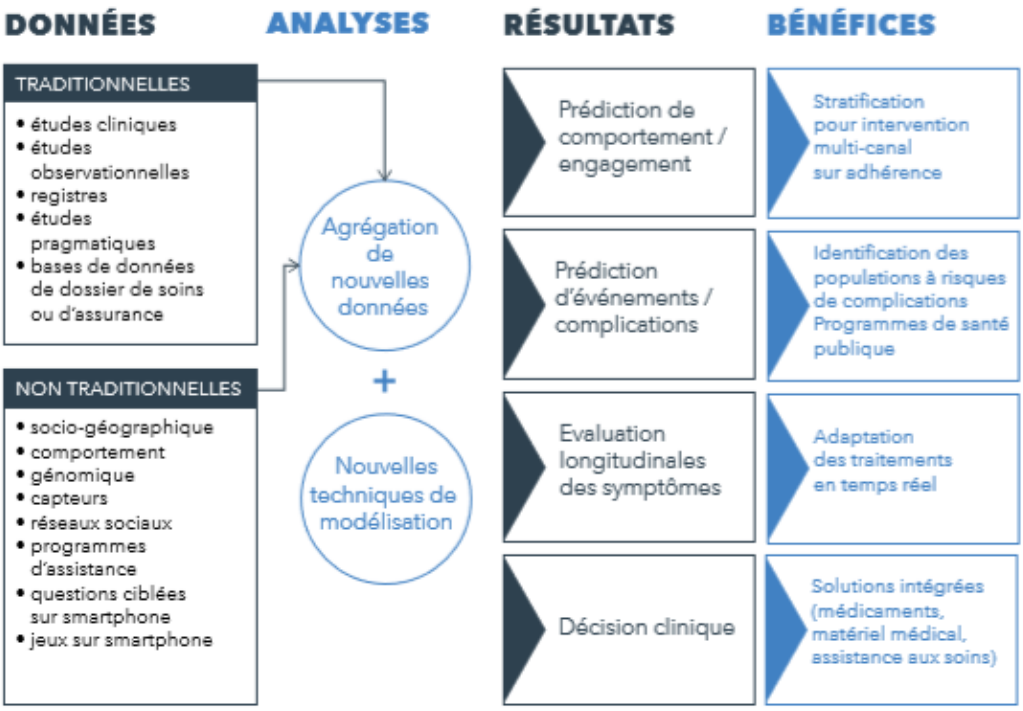

Figure 8 : le machine learning et l'anticipation de l'adhésion à un traitement (76)

4. Individualisation de la prévention

Traditionnellement, les actions de prévention s'adressent à tous et passent par des actions collectives (telles que les campagnes de vaccination, de dépistage ou de sensibilisation face à certains risques) et individuelles (telles que la prévention des comportements à risque avec l'alcool et le tabac, la promotion d'une bonne condition physique et de conseils nutritionnels tels que « 5 fruits et légumes par jour » ou « manger bouger »). Touchant une grande partie de la population, les bénéfices personnels constatés en sont une conséquence directe. Les populations sont peu ciblées spécifiquement par les messages de prévention, pensés pour impacter le plus grand nombre.

Avec le Big Data et l'intelligence artificielle, le ciblage sera plus précis et les actions de prévention plus adaptées, en prenant en compte diverses informations propres à chacun, tels que les antécédents personnels, la consommation médicamenteuse, les données comportementales ou génétiques. L'INCa (Institut National du Cancer) est par exemple en train d'adapter sa campagne de prévention contre le cancer du sein : auparavant, était

proposé une mammographie systématique tous les 2 ans chez toutes les femmes âgées de 50 à74 ans ; dorénavant l'institut se penche sur un programme de prévention plus adapté et individualisé en utilisant les données génétiques des femmes ayant une prédisposition héréditaire à ce type de cancers (77).

Le Big Data offre une réelle promesse d'amélioration de la santé publique et d'économies, et cela a bien été compris par les différentes parties prenantes en e-santé. Dans certains pays tel que le Royaume-Uni, le « bon comportement » individuel des populations est récompensé financièrement par des mutuelles, via des avoirs ou une diminution du montant à payer mensuellement, et permet une réelle amélioration de la santé publique. En France, le programme « santé active » a été mis en place récemment par l'Assurance Maladie pour promouvoir des actions individuelles de prévention plus ciblée. La promotion des bons comportements individuels est primordiale dans un système de mutualisation des risques, mais les rôles et responsabilités de chacun doivent être clairement définis en amont afin d'éviter les dérives associées à la récompense des « bons comportements », et donc l'exclusion des personnes en adoptant de mauvais.

II- Big Data et impact sur les métiers médicaux

Il est de nos jours acquis que le numérique est une réelle opportunité pour révolutionner le système de santé. Présent dans une grande majorité des filières, il s'avère être de plus en plus nécessaire dans les technologies médicales, et ce à différents stades de la prise en charge des patients. Qu'il s'agisse du diagnostic ou encore du suivi de pathologies chroniques, le numérique et le développement de l'IA trouvent leur place dans de nombreux domaines en santé.

Les capacités qu'offrent le digital et le Big Data en santé permettent dorénavant de passer à une nouvelle médecine, plus algorithmique et prédictive. En dépit des progrès thérapeutiques continus, de plus en plus de patients sont atteints de maladies chroniques, et la prise en charge de ces patients coûte cher au système de santé français. En effet, il est estimé que 20% de la population française en Affection Longue Durée (ALD) consomme 80%

de l'offre de soins (78). Dans un bon nombre de cas, les maladies chroniques ou leurs complications pourraient être évitées, en adoptant les comportements adéquats. Il ne faut plus avoir une logique curative mais une logique préventive pour ces maladies. Le digital a longtemps été hors de portée de nombreuses personnes, mais les coûts ayant diminué, il permet de passer à une autre médecine.

1. L'ère de la médecine 6P

La médecine s'oriente de plus en plus vers une médecine dite « 6P », c'est-à-dire une médecine personnalisée, précise, participative, préventive, prédictive et orientée vers le patient. Cette médecine se fonde sur les dernières avancées technologiques, permettant d'avoir de plus amples connaissances génétiques et moléculaires sur les patients et leurs prédispositions, permettant ainsi de (76) :

- comprendre davantage les mécanismes pathologiques ;
- d'identifier les nouvelles cibles thérapeutiques ;
- d'identifier les facteurs de risques ;
- d'accompagner le diagnostic pathologique et la décision médicale ;
- de personnaliser le traitement.

De nombreux domaines médicaux sont concernés, et les gains de temps de prise en charge des malades et de diminution des coûts sont nombreux.

1.1. L'imagerie médicale

Les données actuelles indiquent clairement que l'IA constitue un réel avantage dans le domaine de l'imagerie médicale, permettant d'accompagner le professionnel de santé pour réaliser certaines tâches. Certains actes d'imagerie, tels que les mammographies, les prises d'images en dermatologie, ou encore la recherche de rétinopathie diabétique sont réalisés plus rapidement grâce à l'IA, qui permet également de fournir des résultats plus précis que ceux apportés uniquement par « l'œil » du médecin. Le développement des outils d'analyse

automatisés s'accroit : chaque jour, de nouveaux algorithmes sont développés pour accompagner la détection de pathologies. Ces analyses poussées d'imagerie représentent une avancée prometteuse pour traiter les maladies et les prévenir. Ayant accès à des banques d'images, les algorithmes peuvent déceler des maladies par « expérience », en comparant les nouvelles images obtenues à celles déjà collectées et analysées.

De nombreux algorithmes existent, et tous cherchent à orienter le médecin dans son acte d'imagerie et dans son diagnostic médical. En radiologie, le logiciel Aidoc Medical (79), qui permet de déceler sur les radiographies les anomalies en utilisant l'ensemble des résultats des études cliniques et des diagnostics réalisés pour le même type d'images collectées chez d'autres patients, peut être cité. Google a également développé un logiciel, DreamUp Vision, permettant de détecter les maladies de l'œil touchant les diabétiques.

Cette nouvelle pratique en médecine va au-delà d'une meilleure prise en charge des malades et de l'accroissement d'efficacité des médecins. Elle cherche également à améliorer la prévention des maladies, en diminuant les coûts associés aux actes médicaux réalisés via une assistance de plus en plus fiable : l'IA et la corrélation avec les données déjà recueillies au préalable.

1.2. Le diagnostic, le suivi et la prévention

Analyser des données de santé à un temps donné permet de faciliter les détections en temps réel de pathologies, et de réaliser des diagnostics de plus en plus précis, mais également de suivre les patients de manière exhaustive, et notamment les patients atteints de maladies chroniques.

Divers logiciels existent, pour aider les professionnels de santé dans leur diagnostic ou suivi médical. Le logiciel Implicity, qui permet de gérer à distance les pacemakers des patients atteints de pathologies cardiaques ; ou encore le logiciel WinterLight Labs, qui permet via l'analyse d'extraits de conversations de patients, d'émettre des recommandations diagnostiques sur certaines maladies mentales telles qu'Alzheimer peuvent être pris en exemples. L'IA peut également être utilisée pour prévenir l'évolution de maladies, telles que la sarcopénie ; la société Insilico Medicine a en effet développé un modèle qui se base sur

l'apprentissage profond permettant de prédire l'âge biologique d'un muscle, et de prédire comment il va vieillir (la sarcopénie étant une maladie accélérant le vieillissement des muscles). D'autres logiciels se développent également pour accompagner les médecins généralistes dans leur diagnostic tels que le logiciel CardioLogs, qui permet d'obtenir un rapport personnalisé en temps réel sur un électrocardiogramme (ou ECG), d'analyser et d'associer les signaux de l'ECG à des troubles cardiaques correspondants. Cette aide au diagnostic permet d'améliorer la prise en charge rapide des patients atteints de pathologies cardiaques et permettrait de réduire les décès imputables aux maladies cardiovasculaires, représentant plus de 30% de la mortalité mondiale totale.

1.2.1. Diminution de l'errance thérapeutique à l'aide de l'intelligence artificielle

L'IA et l'analyse des data offrent donc de réelles perspectives d'aide au diagnostic. Elles permettent de « mémoriser » des millions d'informations, d'analyser les variables et de dresser un diagnostic, là où parfois la mémoire humaine flanche. Un médecin peut n'être confronté à une pathologie qu'une seule fois durant son exercice, en oublier certaines caractéristiques et/ou ne plus la diagnostiquer lors d'une autre consultation. L'IA, en accumulant toutes ces informations, ne l'oubliera pas et saura la détecter plus précocement : cette dernière représente donc une aide indispensable au diagnostic, et peut permettre de faire gagner du temps et des examens à des patients en errance diagnostique et thérapeutique.

En effet, réduire le délai entre les premiers symptômes et le diagnostic est primordial pour prendre en charge les patients atteints de maladies rares. Plus de 7 000 maladies rares existent, il est difficile voire impossible en soins primaires de les détecter rapidement, et les patients restent souvent des années sans diagnostic, en errant de service en service. S'appuyer sur le numérique pour les détecter plus rapidement est indispensable pour les prendre en charge : via l'accumulation des données recueillies sur ces maladies, l'IA est pleinement capable d'aider au diagnostic. Le laboratoire Sanofi a pris une initiative afin de lutter contre cette errance et a réuni 23 acteurs français afin d'entreprendre une démarche collective, et cherchant à trouver des solutions en lien avec les nouvelles technologies (80).

Parmi ces acteurs étaient présents des associations de malades, l'Institut National de la Recherche dédiée au numérique, des médecins spécialisés dans les maladies rares ainsi que des start-up.

L'errance diagnostique est responsable d'une aggravation possible de l'état des malades, d'un retard sur les possibilités de conseil génétique et d'un gaspillage de ressources médicales (81). La démocratisation des analyses diagnostiques génétiques et leur diminution de coûts concomitante à l'essor des nouvelles technologies devrait permettre de mieux diagnostiquer les patients. A cela s'ajoute un enjeu primordial pour assurer l'efficience des soins : partager les données de santé de qualité et recueillies par les différents centres existants pour accélérer encore davantage la compréhension des maladies rares, leur diagnostic et leur prise en charge.

1.2.2. Amélioration de la prise en charge des cancers à l'aide de l'intelligence artificielle

L'immense quantité d'informations et de données recueillies peut permettre de développer des algorithmes spécialisés, et notamment dans le diagnostic de cancers. Les techniques plus classiques de détection sont souvent longues et couteuses. Utiliser les données déjà collectées sur ces pathologies peut permettre de les diagnostiquer plus rapidement et d'adapter l'arsenal thérapeutique qui sera utilisé pour le malade.

Le cancer est un défi en lui-même, du fait qu'il ne s'agit pas d'une maladie unique mais de centaines de maladies différentes pluri-caractéristiques : chaque tumeur sera différente, chacune se développera plus ou moins rapidement, chaque patient atteint réagira plus ou moins bien aux traitements. On le sait, une cellule cancéreuse unique est capable d'avoir des milliards de mutations génétiques à chaque division cellulaire. Ce qui rend le diagnostic et le traitement extrêmement compliqués, du fait de cette hétérogénéité des données recueillies.

Un patient malade peut générer un téraoctet de données médicales, qu'il s'agisse du diagnostic, des antécédents ou des données cliniques. Cela équivaut à stocker plus de 100 000 livres. Utiliser les données génétiques devient donc essentiel pour comprendre et traiter les

cancers. Les coûts d'analyses génomiques diminuant chaque année grâce à l'avancée des nouvelles technologies, cela permet d'établir le profil d'un patient et de le comparer à ceux d'autres patients.

La nature complexe et hétérogène des cancers contraint donc à adopter une autre approche pour les traiter, et analyser l'immense quantité de données recueillies. Parfois, il y aura des milliers de données communes pour un type de cancer chez plusieurs patients, et parfois il n'y en aura que quelques-unes de similaires. Analyser toutes ces données avec des moyens humains est chronophage et fastidieux. Utiliser les nouvelles technologies et l'IA pour les traiter représente un réel gain de temps, indispensable surtout lorsque l'on sait que plus les cancers sont détectés et traités tôt, et plus les chances de survie sont élevées. L'objectif de cette analyse de masse de données est d'apporter aux patients malades le traitement le plus ciblé, tout en limitant les effets secondaires. Le défi consiste à analyser tous les éléments correctement. Du fait de l'hétérogénéité des cancers, il n'existe pas d'outil unique pour analyser les données, et les chercheurs et informaticiens ont sans cesse besoin de s'adapter.

Des chercheurs français ont développé en ce sens un algorithme d'intelligence artificielle capable de détecter seul, si un patient va bien réagir ou non à un traitement immunosuppresseur. Le logiciel est capable de réaliser cette analyse grâce à des millions de données recueillies et interprétées sur des tumeurs cancéreuses (82). Cette technique prometteuse d'imagerie médicale laisse à penser qu'il sera permis à l'avenir de s'exempter d'une analyse génétique nécessitant des actes médicaux invasifs (tels que les biopsies), d'éviter un acte douloureux et risqué en fonction de la localisation des tumeurs pour le patient et de s'abstenir de solliciter un chirurgien expérimenté. Encore à l'étude, cet algorithme est néanmoins capable de déterminer si le patient répondra bien au traitement immunosuppresseur dans 60% des cas. Le potentiel de ce genre de logiciel est majeur et confirme l'intérêt de l'usage de la data en santé.

D'autres chercheurs français se sont intéressés à l'IA pour la prise en charge des patients atteints de cancers colorectaux, afin d'en prédire les chances de guérison et d'éviter potentiellement des actes chirurgicaux. Cette maladie concerne plus de 40 000 personnes par an, et nécessite dans la plupart des cas des radio-chimiothérapies ainsi qu'une ablation totale du rectum. Seulement, dans 20 à 30% des cas, cet acte chirurgical n'est pas nécessaire, mais

cela ne peut être confirmé qu'après l'opération (83). Ces chercheurs ont souhaité développer un logiciel capable de détecter si l'acte chirurgical était indispensable ou non, afin d'éviter des douleurs inutiles au patient et d'améliorer son quotidien. Ce logiciel évalue les chances de survie chez les patients à l'aide des data collectées au préalable et va déterminer s'il faut traiter par acte chirurgical ou par radio-chimiothérapie, et ce qu'importe la taille des tumeurs. Les résultats sont probants : dans 80% des cas, le logiciel a vu juste et a orienté le patient vers la thérapie la plus adaptée à son état de santé. L'étude vient préciser que dorénavant, « les images ne sont plus de simples photos que l'on interprète visuellement, elles sont maintenant traitées comme des données ». L'IA permet donc d'analyser de plus en plus d'images et de données, et selon l'auteur de cette étude, « l'intelligence artificielle sera le stéthoscope du XXIe siècle ».

1.2.3. Amélioration du suivi médicamenteux grâce à l'intelligence artificielle

L'usage de l'IA en santé ne va cesser de s'accroitre dans les années à venir, tant les applications sont nombreuses. Améliorer l'observance médicamenteuse fait partie de ces dernières.

A Amiens, la start-up Posos l'utilise pour développer un algorithme capable de prévenir et d'éviter les erreurs médicamenteuses (84). Les professionnels de santé le savent mieux que quiconque, les erreurs et confusions lors de la prise de médicament sont extrêmement nombreuses. En France, il est estimé qu'un évènement indésirable grave sur deux est lié à une erreur médicamenteuse (85). L'OMS rappelle également que ces erreurs entrainent 1% des dépenses de santé au niveau mondial. Cette start-up amiénoise a ainsi développé un algorithme destiné à la fois aux professionnels de santé et aux patients, et répond aux questions posées grâce à l'analyse des précédentes questions émises et réponses apportées. Ce logiciel renvoie vers les réponses les plus pertinentes, et la base de données est de plus en plus efficiente au fur et à mesure qu'elle est utilisée.

Améliorer le suivi médicamenteux passe par une meilleure diffusion de l'information. Le patient est parfois perdu dans des explications complexes et nouvelles lorsqu'il débute un nouveau traitement. Les informations transmises par son médecin, son pharmacien et/ou tout

autre professionnel de santé peuvent parfois être mal comprises ou oubliées. Les notices des médicaments ne sont pas toujours aisées à assimiler. Les laboratoires pharmaceutiques l'ont compris et adaptent leurs matériels informatifs (notice, étiquetage, Résumé des Caractéristiques du Produit ou RCP) afin d'obtenir la meilleure compréhension et observance possible du traitement. L'usage du QR (Quick Response) code se démocratise et s'implémente de plus en plus sur les étiquetages, et principalement sur les dispositifs médicaux combinés aux médicaments, souvent plus complexes à utiliser. Il s'agit d'un code barre en 2 dimensions permettant d'être redirigé vers un contenu multimédia, afin de promouvoir le bon usage en renvoyant vers des informations utiles et pratiques (86). En téléchargeant une application sur son téléphone, le patient scanne le QR code de la boite du médicament, ce qui l'amène vers des sites explicatifs. Des vidéos d'utilisation du DM peuvent également être utilisées, afin de montrer au patient une nouvelle fois comment se servir de ce dernier.

La démocratisation de l'usage du Big Data et de l'IA représente donc une avancée réelle pour envisager de diminuer les erreurs médicamenteuses.

1.3. La recherche

Les progrès réalisés dans la prise en charge des patients sont considérables, et cela est rendu possible grâce au développement des nouvelles technologies concomitant aux activités de recherches. Les cancers sont de mieux en mieux diagnostiqués et pris en charge, l'analyse génomique se développe et coûte de moins en moins cher : chaque année, 70 000 nouveaux patients ont la possibilité de séquencer leur génome à l'Institut National du Cancer, afin d'améliorer leur prise en charge. D'ici quelques années, il est juste de penser que le séquençage génomique sera un acte réalisé en routine. La recherche évolue aussi dans les essais cliniques, où les patients sont dorénavant sélectionnés en fonction de leur génome et de leur compatibilité au traitement. Certaines études sont même ré-évaluées suite à la découverte de nouveaux biomarqueurs spécifiques à certains gènes, afin d'apporter la réponse thérapeutique la plus appropriée en fonction du profil génomique. L'objectif est d'utiliser les données actuelles afin d'orienter le traitement des patients au sein des études cliniques.

Actuellement, l'usage du Big Data en routine n'est que peu développé en génomique parmi toutes les méthodes classiques de recherches, car le séquençage n'est pas encore universalisé. Pourtant, il existe de réelles applications, à la frontière entre le digital, l'IA et les biotechnologies. A l'aide d'algorithmes spécialisés, de plus en plus d'hôpitaux se servent de ces outils d'analyse génomique et d'interprétation pour aider les médecins dans leurs décisions et rendre le diagnostic plus rapide. Le Big Data offre la possibilité d'améliorer et d'accélérer les travaux de recherches en croisant des millions d'informations de sources diverses (revues scientifiques, colloques, études cliniques, données génétiques, résultats des recherches existantes, etc.). Là où l'Homme mettrait des mois ou des années, l'IA permet en quelques jours, via ce croisement d'informations, de révéler les premiers résultats, de déceler des pathologies à des stades précoces, de proposer la thérapeutique la plus adaptée et de détecter des anomalies médicamenteuses. Aujourd'hui, les chercheurs utilisent le Big Data sur trois niveaux principaux en recherche :

- cellulaire : afin de détecter les profils types des cellules malades et de déterminer quels sont les biomarqueurs génétiques. Etablir quelles sont les caractéristiques cellulaires communes aux maladies permettrait de mieux prédire la manière dont les cellules individuelles peuvent muter et d'adapter ensuite l'arsenal thérapeutique ;
- patient : les antécédents médicaux ainsi que les données recueillies via le séquençage génomique permettent encore une fois d'adapter les combinaisons thérapeutiques, et de proposer celles les plus adaptées en fonction du type de tumeur, des gène retrouvés etc. en basant le choix sur les effets obtenus chez d'autres patients aux pathologies et gènes similaires ;
- population : les données recueillies sur une large population permettent d'orienter les stratégies de traitement des malades en fonction de leur mode de vie, de leurs habitudes socio-démographiques ou encore de leur pathologie.

2. L'approche collaborative des professionnels de santé indispensable autours de la e-santé

L'histoire nous montre que les rôles et responsabilités entre spécialités médicales et professionnels de santé évoluent sans cesse. Les métiers sont repensés en fonction des problèmes de santé publique, des avancées de la science et également des mutations de la société. Les nouvelles technologies permettent d'envisager une nouvelle médecine, plus orientée vers la délégation des tâches en santé, vers des professionnels moins qualifiés initialement pour réaliser certains actes en routine. Cette délégation de tâches, en plus de fournir à ces professionnels de nouvelles compétences, peut permettre de combler en partie les déserts médicaux et d'améliorer la qualité des soins. Celle-ci a été expérimentée dans plusieurs hôpitaux durant les années 2000 afin d'évaluer la faisabilité de cette interopérabilité (Tableau 3).

Tableau 3 : exemples de délégations de tâches possibles. (87)

Expérimentation	Site d'expérimentation	Période d'expérimentation
Acte technique : pratique d'échocardiographie par un acteur paramédical	CHU la Timone – Hôpital Louis Pradel à Lyon	Janvier 2007
Expérimentation du rôle d'infirmière spécialisée en hépato-gastro-entérologie pour le suivi de patients atteints d'hépatite C	CHU Henri Mondor à Créteil	Mars 2007
Expérimentation de nouveaux services de soins en cabinet de ville	18 cabinets des Deux-Sèvres	Début 2006

Les nouvelles technologies rendent possible cette délégation. Cela se fait déjà couramment dans de nombreux pays membres de l'OCDE (Finlande, Royaume-Uni, Etats-Unis, etc.). Des infirmiers et autres professionnels paramédicaux, une fois formés via les nouvelles technologies, sont à même de réaliser des missions autrefois réservées aux médecins. Le développement de l'IA en santé laisse à penser que le rôle du médecin est à redéfinir : il pourrait ainsi réaliser les missions les moins automatisables dans son exercice médical et accroitre son rôle d'écoute et de conseil ; et déléguer des tâches médicales à d'autres professionnels.

L'IA et le digital bouleversent la prise en charge des patients, en s'adressant à tous. Les nouvelles technologies développées permettent un gain de temps réel dans le diagnostic et dans la prévention des maladies. Elles sont utilisables facilement et permettent de diminuer les coûts financiers et de temps associés aux formations des professionnels, rendant le déploiement de la e-santé plus rapide et aisé. Ce déploiement de la e-santé est nécessaire pour coordonner le parcours de soins autour et avec le patient. Bien souvent, les patients en consultation omettent des détails sur leurs antécédents, leurs autres consultations médicales ou leurs traitements actuels. Cela peut compromettre un diagnostic et orienter vers un traitement moins adapté à leur réel état de santé. La dématérialisation des données de santé peut permettre d'améliorer l'échange entre le patient et son médecin, et améliorer le traitement en conséquence. Les SI en santé et dans les domaines médico-sociaux doivent permettre une communication optimale, afin de favoriser l'interopérabilité entre les professionnels et les patients. L'instauration de standards européens de communication sur les données de santé est primordiale, et le RGPD vient le rappeler.

Diverses approches collaboratives se développent, et les nouvelles technologies permettent de mettre en commun des professionnels de santé sur toute la planète, afin de trouver des solutions thérapeutiques ensemble pour les patients. Le Project Data Sphere (88), où les chercheurs du monde entier collectent, partagent et analysent en un endroit unique des données sur le cancer peut être cité en exemple. Analyser toutes ces données nécessite une réelle collaboration, chacun doit partager au mieux son expertise afin d'apporter la meilleure prise en charge possible des patients. Si la médecine du XX^{e} siècle était celle de la recherche de données, celle du XXI^{e} siècle sera celle de la collaboration autour des données et de leur traitement.

3. Big Data et Pharmaciens

3.1. Digitalisation de l'officine

Les patients sont de plus en plus connectés. Afin de répondre au mieux aux nouvelles attentes des patients, de rester concurrentiel mais également pour faire face aux divers plans

gouvernementaux de maitrise des coûts, les pharmaciens s'engagent également dans la transformation numérique. Ils doivent repenser leur exercice et s'adapter aux nouvelles mœurs. « La transformation numérique de la pharmacie d'officine suit les mouvements sociétaux » affirme Jacques Perche, directeur général de la société Sterling Pharma (89). Le pharmacien d'officine devient à juste titre le premier interlocuteur santé pour faire face aux déserts médicaux, lutter contre l'automédication dangereuse préconisée sur certains sites internet, et dispenser des entretiens santé personnalisés.

A l'heure du tout connecté, il apparait judicieux d'avoir un site internet par pharmacie afin de donner le plus de visibilité possible sur les activités officinales et de proposer des services et conseils touchant le plus grand nombre. Les patients seraient ainsi plus à même de s'orienter vers les officines répondant à leurs besoins. Le digital modifie dans tous les secteurs l'approche qu'ont les utilisateurs face aux entreprises : en officine par exemple, posséder un site internet permet de prolonger le lien entretenu avec les patients. Tout en conservant le lien unique créé avec les patients au comptoir, les officinaux doivent continuer d'évoluer en proposant de nouveaux services apportant une réelle valeur ajoutée. Le digital permet d'appréhender davantage les attentes des patients.

La data intelligence peut également renforcer l'exercice officinal, en croisant les données santé des patients et des médicaments, et permettre ainsi d'apporter un support supplémentaire aux officinaux et de conforter leurs connaissances et compétences, en vue de proposer une thérapeutique adaptée, tout en conservant le degré de proximité avec les patients. La e-santé n'en est qu'à ses débuts, et le pharmacien joue le rôle central de connecteur entre les différentes professions médicales.

3.2. Nouveau business model pour l'industrie pharmaceutique

Le Big Data a bouleversé l'approche en santé pour tous les acteurs, et également pour les industriels pharmaceutiques. En 2017, l'industrie pharmaceutique avait un chiffre d'affaires (CA) de plus de 53 milliards d'euros (90). Mais la crise de 2008 a entrainé une réelle diminution de ce dernier, et les industriels ont dû repenser leur R&D en conséquence. Dans ce contexte, l'industrie pharmaceutique propose de nouveaux services aux patients ainsi qu'aux

professionnels, afin de répondre à leurs attentes ; et la transformation digitale constitue une réelle opportunité d'améliorer la qualité des soins proposés.

La contrainte réglementaire en santé n'empêche en rien l'innovation que porte en lui le digital. Les laboratoires pharmaceutiques repensent leur business model, pour passer de fabricant de médicaments à fournisseur de produits et services en santé. La transformation digitale des industries pharmaceutiques est nécessaire car cela permet aux entreprises de rester compétitives et innovantes tout en offrant de nouveaux moyens de diffusions de l'information, permettant l'interopérabilité entre les professionnels de santé, autour du patient. Le Big Data permet un renouvellement de l'industrie pharmaceutique, car il est constitué d'une immense quantité de données issues des objets connectés, des smartphones et d'autres réseaux connectés. Associé aux nouvelles technologies, il permet d'envisager une nouvelle prise en charge des patients, au plus proche de ses réels besoins. Le Big Data fait partie intégrante de l'arsenal thérapeutique que doivent développer les industriels pour rester compétitifs.

Le laboratoire Sanofi l'a bien compris et a ouvert fin 2017 « le premier laboratoire consacré à la santé numérique en France » : le 39bis (91). L'objectif est d'accompagner les start-ups afin de créer des projets de cocréation et d'industrialiser des process ou solutions, en vue d'améliorer le suivi et la prise en charge des patients, tout en créant des nouveaux outils pour les professionnels de santé. Le laboratoire cherche à accompagner les start-ups en e-santé, en leur offrant un lieu d'échanges, d'information et de travail pour développer des projets de e-santé. L'objectif est d'aller au-delà du médicament et de proposer une prise en charge globale.

En parallèle, le laboratoire développe ses activités de recherches en s'appuyant sur l'IA pour améliorer ses vaccins contre la grippe. Sanofi utilise une plateforme d'IA pour analyser des échantillons de patients atteints de grippe, afin de générer des milliards de données et d'identifier les biomarqueurs spécifiques de la maladie. L'objectif est d'anticiper les mutations du virus et de cibler davantage les populations à vacciner. L'usage des datas en santé modifie donc la stratégie de R&D des laboratoires.

Sanofi développe également de nouvelles plateformes pour proposer une meilleure prise en charge des patients atteints de maladies chroniques, et notamment dans le diabète. En partenariat avec Google, le laboratoire va lancer des essais cliniques en 2018, à l'aide d'une

plateforme appelée Onduo, s'appuyant sur des algorithmes afin de « conseiller sur les prises en charge et les traitements les mieux adaptés – insulines notamment – pour la pathologie », et ce « en prenant en compte de nombreux paramètres nécessaires, comme la démographie des patients, les caractéristiques de leur pathologie, l'épidémiologie, le mode de vie » déclare Joshua Riff, médecin urgentiste de formation et directeur général annoncé pour cette plateforme.

Plus que jamais, les industries pharmaceutiques investissent le marché de la e-santé. L'objectif est d'apporter une solution thérapeutique innovante et adaptée aux patients, et de rester compétitif sur un marché pharmaceutique où la pression concurrentielle est très forte.

III- Big Data et éthique

Il existe de nombreuses applications possibles à l'utilisation de nos données de santé numérisées. Mais les algorithmes développés doivent permettre de garantir une confidentialité et le respect des droits des personnes sur leur utilisation. Les enjeux sont majeurs, car parmi les risques associés est retrouvée la divulgation de la vie privée, avec des conséquences sociétales telles que le harcèlement, le chantage et le non-respect du principe de confidentialité. Toutes les pratiques et tous les traitements sur les données à caractère personnel ne sont pas acceptables au nom du plus grand bien. Elles doivent être encadrées et limitées. Il en va de la confiance des utilisateurs.

Il y a quelques années encore, la majorité de nos données de santé étaient recueillies au format papier : bilans sanguins, radiographies, comptes-rendus opératoires… elles sont désormais pour la majorité stockées sur des serveurs, qui ne sont pas forcément en France ou en Europe. Les règles applicables ne sont pas forcément les mêmes, le RGPD n'est pas toujours adapté. A ces données recueillies par les circuits médicaux « classiques » s'ajoutent celles recueillies via les objets connectés ou les applications mobiles, qu'il s'agisse de la fréquence cardiaque, de données de masse corporelle, de données recueillies sur la qualité du sommeil etc. Ces données sont des informations très sensibles, d'autant plus du fait qu'elles se retrouvent entre les mains des organismes privés qui développent ces applications, qui ne sont pas nécessairement contraints au secret professionnel.

Dans le domaine médical, le risque principal associé à ce Big Data est le manque d'encadrement de ces données, associé au non-respect du secret médical. Les états généraux de Bioéthique abordent la problématique d'utilisation à mauvais escient de ces datas. La principale difficulté réside en effet dans leur utilisation à des fins de recherches médicales afin d'en tirer le plus grand profit, sans par ailleurs porter atteinte au droit des patients et à leur vie privée.

A cette problématique s'ajoute celle associée à « la révélation d'une pathologie qui pourrait avoir des conséquences catastrophiques pour l'individu concerné, vis-à-vis d'un employeur ou d'un organisme de crédit par exemple » affirme Hélène Guimiot-Bréaut, chef du service de la santé à la CNIL (92). En effet, à partir du moment où des informations confidentielles sont révélées, le secret médical n'est plus assuré. En France, une stricte codification du stockage des données à caractère personnel et leur accès est donc implémentée par la loi. Les données sont pseudonymisées. Le RGPD vient renforcer ces pratiques. Mais, en réalité, certains manquements de sécurité sont notifiés à la CNIL. La question de la bonne gestion des données se pose donc.

En France, les données à caractère personnel de santé sont très protégées. Mais les données dites de « santé bien-être » (c'est-à-dire celles recueillies par le biais d'applications mobiles ou d'objets connectés) sont encore trop peu protégées, en raison d'un régime juridique encore à définir. Les organismes privés détenteurs des applications ne sont en rien contraints à anonymiser les données, sous-entendant la possibilité de la vente à des tiers. Leur seule obligation consiste à informer les utilisateurs de l'usage futur réalisé sur leurs données à caractère personnel via la nécessité « d'accepter les conditions générales d'utilisation ». Dans l'immense majorité des cas, ces conditions générales ne sont pas lues, et les utilisateurs n'ont pas pleinement conscience de l'usage potentiel qui sera fait de leurs données. Dans un souci éthique, la CNIL se penche actuellement sur la question de définition d'un label incitatif pour informer davantage les utilisateurs de l'utilisation future de leurs données.

Cette numérisation systématique des données s'inscrit dans les mœurs, et sera encore plus forte dans les années à venir. Il est légitime de se poser la question de l'usage futur qui en sera fait. Par exemple, en fonction des habitudes comportementales d'une personne recueillies via ces data, il est possible d'envisager une individualisation du système assurantiel,

et d'une modulation des tarifs en fonction des personnes. Ces pratiques ne sont pas autorisées en France grâce à la loi du 26 janvier 2016, mais certains pays penchent vers cette solution. Le numérique et l'IA constituent un réel outil efficace dans la coordination du parcours de santé de chacun ; mais, en parallèle, ils offrent à l'Assurance Maladie un réel outil de contrôle des malades, plus connu sous le nom de « télé observance », ou de surveillance de masse. Il est primordial de veiller à conserver un système de santé ne sélectionnant pas à grande échelle les populations à risques pour les faire payer davantage.

Le système de santé est en train d'être repensé, les pratiques médicales évoluent avec l'utilisation de ces Big Data : la vigilance s'impose donc, car derrière ces données il y a des Hommes.

Conclusion

En santé, les données sont présentes partout et proviennent de sources multiples. Dès lors qu'elles sont disponibles et utilisées à bon escient, elles constituent une réelle avancée pour la prise en charge des patients. Permettant de détecter des signaux, de suivre des épidémies, d'anticiper des crises sanitaires et d'individualiser les messages de prévention, elles permettent de réelles améliorations en santé publique. Leur analyse et leur suivi en temps réel permettent de mesurer l'efficacité des actions sanitaires prises, et de les adapter. Les professions médicales sont repensées grâce à l'apport des algorithmes basés sur l'IA. La recherche s'accélère, la prise en charge des malades se personnalise. L'IA vient bouleverser les schémas acquis en santé, en améliorant la prise en charge des patients et leur qualité de vie et en contribuant à en sauver, ce qui confère à ces nouvelles technologies un côté moins menaçant et impersonnel. La e-santé représente une solution effective pour diminuer les coûts, et le contexte sociétal actuel est favorable à son déploiement.

Les données à caractère personnel de santé sont dématérialisées, et ce à grande échelle, leur circulation est dès lors difficile à contrôler. Il est nécessaire d'encadrer strictement les activités de traitement de ces données, afin d'en limiter les usages abusifs à des fins lucratives notamment. Il est également indispensable de définir clairement les « données frontières » qui sont à mi-chemin entre les données « bien-être » et les données de « santé ». Les utilisateurs doivent avoir été informés clairement de l'usage qui sera fait de leurs données, et de leurs conditions de stockage. Le RGPD vient placer le patient au cœur de son règlement. Il définit clairement les traitements autorisés des données, tout en insistant sur l'indispensabilité de leur minimisation. Il vient également responsabiliser les acteurs en soumettant les développeurs d'applications mobiles et d'objets connectés et leurs sous-traitants aux mêmes règles de confidentialité et de sanctions.

La question se pose de l'acceptabilité sociale de l'ensemble des changements induits par ces nouvelles technologies. Le système de santé est en train d'être bouleversé, et trop peu de débats publics ont lieu pour impliquer les citoyens dans ces changements. La question du rapport à la machine se pose aussi : l'homme est-il prêt à accepter et à vivre avec l'IA et à laisser sa santé être dictée, même partiellement, et ce au nom du plus grand bien, par des logiciels ?

Bibliographie

1. Big data : l'explosion de la production de données [Internet]. egora.fr. 2018 [cité 18 août 2018]. Disponible sur: https://www.egora.fr/actus-medicales/sante-publique/39040-big-data-l-explosion-de-la-production-de-donnees

2. OCDE 2010, "Améliorer le rapport coût-efficacité des systèmes de santé", OCDE Département des Affaires Économiques, Note de politique économique, no 2 [Internet]. [cité 1 oct 2018]. Disponible sur: https://www.oecd.org/fr/eco/croissance/49653347.pdf

3. Patient Adoption of mHealth - Use, Evidence and Remaining Barriers to Mainstream Acceptance [Internet]. [cité 1 oct 2018]. Disponible sur: https://pascaleboyerbarresi.files.wordpress.com/2015/03/iihi_patient_adoption_of_mhealth.pdf

4. WHO Global Observatory for eHealth, World Health Organization. MHealth: new horizons for health through mobile technologies. [Internet]. Geneva: World Health Organization; 2011 [cité 18 août 2018]. Disponible sur: http://www.who.int/goe/publications/goe_mhealth_web.pdf

5. 4 e baromètre VIDAL – CNOM L'utilisation des Smartphones chez les médecins [Internet]. [cité 1 oct 2018]. Disponible sur: http://www.vidalfrance.com/wp-content/download/CP/CP_VIDAL_Mobile_Barometre_2016.pdf

6. Santé connectée : le livre blanc du CNOM « De la e-santé à la santé connectée » | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 18 août 2018]. Disponible sur: http://esante.gouv.fr/actus/ethique/sante-connectee-le-livre-blanc-du-cnom-de-la-e-sante-a-la-sante-connectee

7. Haute Autorité de Santé - Good practice guidelines on health apps and smart devices (mobile health or mhealth) [Internet]. [cité 18 août 2018]. Disponible sur: https://www.has-sante.fr//portail/jcms/c_2681915/fr/referentiel-de-bonnes-pratiques-sur-les-applications-et-les-objets-connectes-en-sante-mobile-health-ou-mhealth

8. Draft Code of Conduct on privacy for mobile health applications [Internet]. [cité 1 oct 2018]. Disponible sur: http://www.ehealthnews.eu/images/stories/pdf/code-of-conduct-final-draft.pdf

9. Code de conduite européen « Privacy en santé mobile » [Internet]. Lexing Alain Bensoussan Avocats. 2017 [cité 18 août 2018]. Disponible sur: https://www.alain-bensoussan.com/avocats/code-de-conduite-privacy-en-sante-mobile/2017/05/02/

10. The ePrivacy Directive [Internet]. Digital Single Market. [cité 18 août 2018]. Disponible sur: https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive

11. Le règlement eIDAS [Internet]. ANSSI. [cité 18 août 2018]. Disponible sur: https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-reglement-eidas/

12. Directive 93/42/CEE du conseil du 14 juin 1993 relative aux dispositifs médicaux [Internet]. [cité 1 oct 2018]. Disponible sur: https://documents.lne.fr/publications/directives/93-42.pdf

13. L'Internet des objets : Aujourd'hui et demain - étude HPE_Aruba_IoT_Research_Report.pdf [Internet]. [cité 1 oct 2018]. Disponible sur: https://www.arubanetworks.com/assets/_fr-ca/eo/HPE_Aruba_IoT_Research_Report.pdf

14. ROCHE T. La CJCE précise les contours de la définition du « dispositif médical » [Internet]. Blog du département « Sciences du vivant » de DELSOL Avocats. 2012 [cité 19 août 2018]. Disponible sur: http://www.delsolavocats.fr/sdv/la-cjue-precise-les-contours-de-la-definition-du-dispositif-medical/

15. Un hôpital paie 17000$ pour récupérer ses fichiers cryptés - Le Monde Informatique [Internet]. LeMondeInformatique. [cité 30 sept 2018]. Disponible sur: https://www.lemondeinformatique.fr/actualites/lire-un-hopital-paie-17000$-pour-recuperer-ses-fichiers-cryptes-63961.html

16. Une attaque informatique paralyse trois hôpitaux en Angleterre [Internet]. [cité 30 sept 2018]. Disponible sur: http://www.ticsante.com/Une-attaque-informatique-paralyse-trois-hopitaux-en-Angleterre-NS_3241.html

17. Cyberveille Santé | Accompagnement Cybersécurité des Structures de Santé [Internet]. [cité 19 août 2018]. Disponible sur: https://www.cyberveille-sante.gouv.fr/

18. ASIP. Sécurité informatique, un enjeu de la transformation numérique en santé [Internet]. Le Blog de l'Asip Santé. 2017 [cité 19 août 2018]. Disponible sur: https://www.blogasipsante.fr/fiches-thematiques/editos/securite-informatique-enjeu-de-transformation-numerique-sante

19. Larousse É. Encyclopédie Larousse en ligne - intelligence artificielle [Internet]. [cité 19 août 2018]. Disponible sur: http://www.larousse.fr/encyclopedie/divers/intelligence_artificielle/187257

20. Manach JM. « Safari ou la chasse aux Français » - Le Monde 21 Mars 1974 - Philippe Boucher [Internet]. [cité 20 août 2018]. Disponible sur: http://rewriting.net/2008/02/11/safari-ou-la-chasse-aux-francais/

21. Magazine FM UP'. UP Magazine - CNIL : 40 ans au service des libertés [Internet]. [cité 29 juill 2018]. Disponible sur: http://www.up-magazine.info/index.php/transition-numerique/transition-numerique-2/7332-cnil-40-ans-au-service-des-libertes

22. Statut et organisation de la CNIL | CNIL [Internet]. [cité 1 août 2018]. Disponible sur: https://www.cnil.fr/fr/statut-et-organisation-de-la-cnil

23. Les missions de la CNIL | CNIL [Internet]. [cité 1 août 2018]. Disponible sur: https://www.cnil.fr/fr/les-missions-de-la-cnil

24. LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. 2018-493 juin 20, 2018.

25. REBEYRAT M. Proposition de règlement sur la protection des données personnelles dans les communications électroniques [Internet]. UFMD. [cité 1 août 2018]. Disponible sur: https://www.ufmd.org/Proposition-de-reglement-sur-la-protection-des-donnees-personnelles-dans-les-communications-electroniques_a38.html

26. France, Commission nationale de l'informatique et des libertés. CNIL: Rapport d'activité 2017. 2018.

27. Vollmer N. Article 58 EU règlement général sur la protection des données (EU-RGPD) [Internet]. 2018 [cité 2 oct 2018]. Disponible sur: http://www.privacy-regulation.eu/fr/58.htm

28. Missions | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 8 août 2018]. Disponible sur: http://esante.gouv.fr/asip-sante/qui-sommes-nous/missions

29. Une mission « e-santé » sera installée courant avril auprès du ministère de la santé [Internet]. [cité 8 août 2018]. Disponible sur: https://www.ticpharma.com/story.php?story=538

30. LOI n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires. 2009-879 juill 21, 2009.

31. Qu'est-ce qu'une agence régionale de santé [Internet]. [cité 8 août 2018]. Disponible sur: http://www.ars.sante.fr/quest-ce-quune-agence-regionale-de-sante

32. La stratégie nationale e-santé 2020 [Internet]. [cité 11 août 2018]. Disponible sur: http://www.ars.sante.fr/la-strategie-nationale-e-sante-2020

33. Livre blanc « 17 experts / 36 propositions pour une politique e-santé ambitieuse » - Renaissance numérique - Mars 2017 - APHP DAJ [Internet]. [cité 11 août 2018]. Disponible sur: http://affairesjuridiques.aphp.fr/textes/livre-blanc-17-experts-36-propositions-pour-une-politique-e-sante-ambitieuse-renaissance-numerique-mars-2017/

34. CNIL: Comment permettre à l'Homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle [Internet]. [cité 2 oct 2018]. Disponible sur: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

35. Les « living labs » en santé au service des citoyens [Internet]. I'MTech. 2015 [cité 11 août 2018]. Disponible sur: https://blogrecherche.wp.imt.fr/2015/01/29/vers-une-approche-participative-des-solutions-numeriques-en-sante/

36. La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 11 août 2018]. Disponible sur: http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-0

37. Stratégie de transformation du système de santé - Dossier de presse - mardi 13 février 2018 [Internet]. [cité 2 oct 2018]. Disponible sur: https://solidarites-sante.gouv.fr/IMG/pdf/dossier_de_presse_strattransformationsystemesante_13022018.pdf

38. DGOS. Le programme Territoire de Soins Numérique - TSN [Internet]. Ministère des Solidarités et de la Santé. 2016 [cité 11 août 2018]. Disponible sur: https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/tsn/article/le-programme-territoire-de-soins-numerique-tsn

39. DICOM_Jocelyne.M. 550 millions d'euros investis sur 5 ans pour accompagner les établissements de santé dans le virage numérique [Internet]. Ministère des Solidarités et de la Santé. 2017 [cité 11 août 2018]. Disponible sur: https://solidarites-sante.gouv.fr/archives/archives-presse/archives-communiques-de-presse/article/550-millions-d-euros-investis-sur-5-ans-pour-accompagner-les-etablissements-de

40. Communiqué de presse e-santé - 15 mars 2017 [Internet]. [cité 2 oct 2018]. Disponible sur: https://solidarites-sante.gouv.fr/IMG/pdf/17_03_15_-_cp_programmes_e-parcours_et_e-hop_2.0.pdf

41. Santé et protection des données [Internet]. [cité 18 août 2018]. Disponible sur: http://www.conseil-etat.fr/Actualites/Discours-Interventions/Sante-et-protection-des-donnees

42. LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique | Legifrance [Internet]. [cité 12 août 2018]. Disponible sur: https://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo

43. 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) [Internet]. [cité 12 août 2018]. Disponible sur: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

44. Article 5 : Principes relatifs au traitement des données à caractère personnel [Internet]. GDPR.expert. [cité 2 oct 2018]. Disponible sur: http://www.gdpr-expert.eu/

45. Le Privacy shield | CNIL [Internet]. [cité 12 août 2018]. Disponible sur: https://www.cnil.fr/fr/le-privacy-shield

46. RÈGLEMENT (UE) 2017/ 745 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 5 avril 2017 - relatif aux dispositifs médicaux, modifiant la directive 2001/ 83/ CE, le règlement (CE) no 178/ 2002 et le règlement (CE) no 1223/ 2009 et abrogeant les directives du Conseil 90/ 385/ CEE et 93/ 42/ CEE. :175.

47. RÈGLEMENT (UE) 2017/ 746 DU PARLEMENT EUROPÉEN ET DU CONSEIL - du 5 avril 2017 - relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/ 79/ CE et la décision 2010/ 227/ UE de la Commission. :157.

48. Entrée en vigueur de la nouvelle loi Informatique et Libertés | CNIL [Internet]. [cité 2 oct 2018]. Disponible sur: https://www.cnil.fr/fr/entree-en-vigueur-de-la-nouvelle-loi-informatique-et-libertes

49. L +Bastien. Chiffres Big Data : 15 faits impressionnants sur le Big Data [Internet]. LeBigData.fr. 2018 [cité 5 sept 2018]. Disponible sur: https://www.lebigdata.fr/chiffres-big-data

50. INSERM: Big data en santé [Internet]. Inserm. [cité 5 sept 2018]. Disponible sur: https://www.inserm.fr/information-en-sante/dossiers-information/big-data-en-sante

51. Portail Epidemiologie - France | Health Databases [Internet]. [cité 5 sept 2018]. Disponible sur: https://epidemiologie-france.aviesan.fr/

52. ameli.fr - Sniiram [Internet]. [cité 5 sept 2018]. Disponible sur: https://www.ameli.fr/l-assurance-maladie/statistiques-et-publications/sniiram/finalites-du-sniiram.php

53. Le droit à la limitation du traitement : geler l'utilisation de vos données | CNIL [Internet]. [cité 20 août 2018]. Disponible sur: https://www.cnil.fr/fr/le-droit-la-limitation-du-traitement-geler-lutilisation-de-vos-donnees

54. Le droit à la portabilité : obtenir et réutiliser une copie de vos données | CNIL [Internet]. [cité 20 août 2018]. Disponible sur: https://www.cnil.fr/fr/le-droit-la-portabilite-obtenir-et-reutiliser-une-copie-de-vos-donnees

55. Article 35 - Information du patient | Conseil National de l'Ordre des Médecins [Internet]. [cité 25 août 2018]. Disponible sur: https://www.conseil-national.medecin.fr/article/article-35-information-du-malade-259

56. CHAPITRE I - Dispositions générales | CNIL [Internet]. [cité 25 août 2018]. Disponible sur: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1

57. Chafiol F, Tubert S, Lapeyre S. M-10 : RGPD et bases légales de traitement : la place du consentement [Internet]. August Debouzy avocats. 2017 [cité 25 août 2018]. Disponible sur: https://www.august-debouzy.com/en/blog/1037-rgpd-et-bases-legales-de-traitement-la-place-du-consentement

58. Applications mobiles en santé et protection des données personnelles : Les questions à se poser | CNIL [Internet]. [cité 7 oct 2018]. Disponible sur: https://www.cnil.fr/fr/applications-mobiles-en-sante-et-protection-des-donnees-personnelles-les-questions-se-poser

59. Comprendre les grands principes de la cryptologie et du chiffrement | CNIL [Internet]. [cité 26 août 2018]. Disponible sur: https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

60. Le G29 publie un avis sur les techniques d'anonymisation | CNIL [Internet]. [cité 26 août 2018]. Disponible sur: https://www.cnil.fr/fr/le-g29-publie-un-avis-sur-les-techniques-danonymisation

61. Portail de signalement des événements sanitaires indésirables [Internet]. [cité 26 sept 2018]. Disponible sur: https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

62. La démarche de signalement des incidents de sécurité des systèmes d'information numériques de santé | esante.gouv.fr, le portail de l'ASIP Santé [Internet]. [cité 26 août 2018]. Disponible sur: http://esante.gouv.fr/services/la-demarche-de-signalement-des-incidents-de-securite-des-systemes-d-information-numeriques

63. Quelles sanctions en cas de non respect du RGPD ? [Internet]. LegalPlace. 2018 [cité 26 août 2018]. Disponible sur: https://www.legalplace.fr/guides/rgpd-sanction/

64. Condamnation d'un praticien hospitalier pour traitement de données illicite [Internet]. Desmarais Avocats. 2017 [cité 2 oct 2018]. Disponible sur: https://www.desmarais-avocats.fr/condamnation-dun-praticien-hospitalier-pour-traitement-de-donnees-illicite/

65. Terr-eSanté | Simplifions-nous la Santé [Internet]. [cité 2 oct 2018]. Disponible sur: https://www.terr-esante.fr/

66. Transition vers le RGPD : des labels à la certification | CNIL [Internet]. [cité 26 août 2018]. Disponible sur: https://www.cnil.fr/fr/transition-vers-le-rgpd-des-labels-la-certification

67. RGPD : quel premier bilan 4 mois après son entrée en application ? | CNIL [Internet]. [cité 7 oct 2018]. Disponible sur: https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application

68. Facebook : l'affaire Cambridge Analytica pourrait concerner 2,7 millions d'utilisateurs européens. Le Monde.fr [Internet]. 6 avr 2018 [cité 2 oct 2018]; Disponible sur: https://www.lemonde.fr/pixels/article/2018/04/06/cambridge-analytica-2-7-millions-d-utilisateurs-europeens-de-facebook-pourraient-etre-concernes_5281717_4408996.html

69. OMS Glossaire de la promotion de la santé [Internet]. [cité 2 oct 2018]. Disponible sur: http://apps.who.int/iris/bitstream/handle/10665/67245/WHO_HPR_HEP_98.1_fre.pdf

70. Organisation de la pharmacovigilance nationale - ANSM : Agence nationale de sécurité du médicament et des produits de santé [Internet]. [cité 27 août 2018]. Disponible sur: https://ansm.sante.fr/Declarer-un-effet-indesirable/Pharmacovigilance/Organisation-de-la-pharmacovigilance-nationale/(offset)/0

71. Bégaud B, Costagliola D. RAPPORT SUR LA SURVEILLANCE ET LA PROMOTION DU BON USAGE DU MEDICAMENT EN FRANCE. :57.

72. Pontes H, Clément M, Rollason V. Safety signal detection: the relevance of literature review. Drug Saf. juill 2014;37(7):471-9.

73. Réseau Sentinelles > France > Le réseau Sentinelles [Internet]. [cité 2 sept 2018]. Disponible sur: https://www.sentiweb.fr/?page=presentation

74. Mobile phone data highlights the role of mass gatherings in the spreading of cholera outbreaks | PNAS [Internet]. [cité 2 sept 2018]. Disponible sur: http://www.pnas.org/content/113/23/6421

75. Les « big data », nouvel outil contre les épidémies comme Ebola ? - Sciencesetavenir.fr [Internet]. [cité 2 sept 2018]. Disponible sur: https://www.sciencesetavenir.fr/sante/les-big-data-nouvel-outil-contre-les-epidemies-comme-ebola_28006

76. Barbier-Feraud I, Malafosse JB, Bouexel P, Commaille-Chapus C, Gimalac A, Jeannerod G, et al. BIG DATA ET PRÉVENTION : DE LA PRÉDICTION À LA DÉMONSTRATION - Novembre 2016. :80.

77. PLAN D'ACTION POUR LA RÉNOVATION DU DÉPISTAGE ORGANISÉ DU CANCER DU SEIN - Avril 2017 [Internet]. [cité 2 oct 2018]. Disponible sur: https://solidarites-sante.gouv.fr/IMG/pdf/plan-actions-renov-cancer-sein-2.pdf

78. DRESS : La consommation de soins et de biens médicaux (CSBM) [Internet]. [cité 2 oct 2018]. Disponible sur: https://drees.solidarites-sante.gouv.fr/IMG/pdf/fichea.pdf

79. Aidoc - AI that works for you [Internet]. Aidoc. [cité 2 sept 2018]. Disponible sur: https://www.aidoc.com/

80. Sanofi - Maladies rares - Sanofi [Internet]. [cité 1 sept 2018]. Disponible sur: https://www.sanofi.com/fr/nous-connaitre/solutions-de-sante/maladies-rares

81. Plan national maladies rares 2018-2022 [Internet]. [cité 2 oct 2018]. Disponible sur: https://solidarites-sante.gouv.fr/IMG/pdf/plan_national_maladies_rares_2018-2022.pdf

82. A radiomics approach to assess tumour-infiltrating CD8 cells and response to anti-PD-1 or anti-PD-L1 immunotherapy: an imaging biomarker, retrospective multicohort study - The Lancet Oncology [Internet]. [cité 2 sept 2018]. Disponible sur: https://www.thelancet.com/journals/lanonc/article/PIIS1470-2045(18)30413-3/fulltext#%20

83. Detecting repeated cancer evolution from multi-region tumor sequencing data | Nature Methods [Internet]. [cité 2 sept 2018]. Disponible sur: https://www.nature.com/articles/s41592-018-0108-x

84. Start-up Posos [Internet]. Posos. [cité 2 sept 2018]. Disponible sur: https://www.posos.fr/

85. Haute Autorité de Santé - Sécuriser la prise en charge médicamenteuse en établissement de santé [Internet]. [cité 2 sept 2018]. Disponible sur: https://www.has-sante.fr/portail/jcms/c_2574453/fr/securiser-la-prise-en-charge-medicamenteuse-en-etablissement-de-sante

86. ANSM: Avis aux titulaires d'AMM : Soumission à l'ANSM des documents liés à un QR code sur le conditionnement primaire ou secondaire, ou dans la notice d'un médicament. [Internet]. [cité 2 oct 2018]. Disponible sur: https://www.ansm.sante.fr/var/ansm_site/storage/original/application/ce27e5eccb149952ed344d916ff5dc16.pdf

87. HAS: DÉLÉGATION, TRANSFERT, NOUVEAUX METIERS... CONDITIONS DES NOUVELLES FORMES DE COOPÉRATION ENTRE PROFESSIONNELS DE SANTÉ [Internet]. [cité 2 oct 2018]. Disponible sur: https://www.has-sante.fr/portail/upload/docs/application/pdf/rapport_etape_cooperation.pdf

88. Project Data Sphere | Share, Integrate & Analyze Cancer Research Data | Project Data Sphere [Internet]. [cité 5 sept 2018]. Disponible sur: https://projectdatasphere.org/projectdatasphere/html/home

89. Recherche médicale et information santé : Labsanté | Sanofi [Internet]. [cité 5 sept 2018]. Disponible sur: http://labsante.sanofi.fr/esante/que-peut-on-attendre-de-la-digitalisation-de-lofficine/

90. Chiffre d'affaires | Leem [Internet]. [cité 3 sept 2018]. Disponible sur: https://www.leem.org/chiffre-daffaires

91. E-santé: Sanofi passe à la vitesse supérieure [Internet]. [cité 4 sept 2018]. Disponible sur: https://www.latribune.fr/entreprises-finance/industrie/chimie-pharmacie/e-sante-sanofi-passe-a-la-vitesse-superieure-760342.html

92. « Big data », pour le meilleur ou pour le pire ? - La Croix [Internet]. [cité 6 sept 2018]. Disponible sur: https://www.la-croix.com/Sciences-et-ethique/Ethique/Big-data-meilleur-pire-2018-03-15-1200920908

DROUIN Mathilde

Les nouveaux cadres de la e-santé à l'ère du Big Data : quels enjeux pour la santé de demain ?

Thèse pour le diplôme d'état de docteur en pharmacie
Université de Picardie Jules Vernes - 2018

Mots clés : E-santé ; Technologies de l'Information et de la Communication ; Loi Informatique et Libertés ; Règlement Général sur la Protection des Données ; Données à caractère personnel ; Big Data ; Intelligence Artificielle ; Innovation en santé ; Médecine 6P

RESUME

Les données de santé sont présentes partout et proviennent de sources multiples. Il est nécessaire d'encadrer strictement les activités de traitement de ces données, afin d'en limiter les usages abusifs. Les utilisateurs doivent avoir été informés clairement de l'usage qui en sera fait et de leurs conditions de stockage. Le Règlement Général sur la Protection des Données vient placer le patient au cœur de son règlement. Il définit clairement les traitements autorisés des données, tout en insistant sur l'indispensabilité de leur minimisation. Il vient également responsabiliser les acteurs en soumettant les responsables de traitements et leur sous-traitants aux mêmes règles de confidentialité et de sanctions. Dès lors qu'elles sont disponibles et utilisées à bon escient, les données de santé permettent une réelle avancée pour la prise en charge des patients. Elles constituent une avancée majeure en santé publique. La recherche s'accélère, la prise en charge des malades se personnalise. Les professions médicales sont repensées grâce à l'apport des algorithmes basés sur l'intelligence artificielle.

KEY WORDS : E-health ; Information and Communication Technologies ; Data Protection Act ; General Data Protection Regulation ; Personal data ; Big Data ; Artifical Intelligence ; Health innovation ; 6P medicine

SUMMARY

Health data are everywhere and comes from mulple sources. It's require to strictly control the processing activities of these data, in order to limit misuse. Users must be clearly informed of the use that will be made of them and their storage conditions. The General Data Protection Regulation puts the patient at the heart of its regulations. It clearly define the authorized processing of the data, while insisting on the indispensability of their minimization. It also empowers the actors by subjecting the controllers and their subcontractors to the same rules of confidentiality and sanctions. When they are available and used wisely, the health data allow a real advance for the care of the patients. They constitute a major breackthrough in public health. The research accelerates, the care of the patients is more personalized. Medical professions are rethought thanks to the contribution of algorithms base on artificial intelligence.

JURY :
Président de thèse : Monsieur le Professeur SONNET Pascal
Directrice de thèse : Madame le Docteur DEMAILLY Catherine
Membres : Madame le Pharmacien ELLOUZE Selima
Madame le Docteur LEMAIRE-RIQUIER Angélique