# DROIT DES AFFAIRES APPLIQUÉ AU MONDE DE LA SANTÉ

## Droit, santé et numérique

# DROIT DES AFFAIRES APPLIQUÉ AU MONDE DE LA SANTÉ

## Droit, santé et numérique

CERCRID UMR5137
centre de recherches critiques sur le droit

UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

LexisNexis®
LexisNexis SA
141, rue de Javel – 75015 Paris

## Avertissement de l'Éditeur

Toute utilisation ou traitement automatisé, par des tiers, de données personnelles pouvant figurer dans cet ouvrage sont formellement interdits.


Le logo qui figure sur la couverture de ce livre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, tout particulièrement dans les domaines du droit, de l'économie et de la gestion, le développement massif du photocopillage.
Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement soit aujourd'hui menacée.


Siège social : 141, rue de Javel - 75015 Paris



ISBN 978-2-7110-3487-1

## Liste des auteurs

Agnès AUDOIN
*Directeur juridique, IT, Ipsen*

Aurélien BIECHY
*PhD, Intellectual property Director, Ipsen*

Stéphanie CHABIN
*Vice-président, Legal R&D, Ipsen*

Seydou DIAKITE
*Doctorant, CerCrid, UJM Saint-Etienne*

Béatrice ESPESSON-VERGEAT
*Maître de conférences HDR*
*Directrice du master Droit des affaires appliqué au monde de la santé*
*Membre du CerCrid UMR CNRS 5137*

Laëtitia GAILLARD
*Avocate, Reed Smith*

Lorye HUGON
*Collaboratrice, Fidal*

Daniel KADAR
*Avocat associé, Reed Smith*

Marie KOELHER DE MONTBLANC
*Avocat*
*Directeur associé concurrence, Fidal*

Alban LAMBOUROUD
*Responsable fiscal, J&J*

Pierre MORGON
*Docteur en Pharmacie, CEO MRGN Advisors*

Deogratias NGABONZIZA
*Collaborateur, Ipsen*

Klervi SIMON
*Élève-avocat*

Avec la collaboration des étudiants du Master Droit des affaires appliqué au monde de la Santé
Promotion 2020/2021 :

Inès AGGOUNE

Ruby ARCHEN

Étienne BARA

Kamel BESSEGHIER

Manon BRUNON

Ela CAN

Aleyna CAPRAZ

Silène COUTANSON

Alexandre FAURE

Leïla GUÉRIN

Caroline KAK

Abdelaalim KEDDAD

Sasha LAVERNHE

Élisa LEMAIRE

Laurène MIGNOT

Mohamed MOKADDEM

Sandrine NTETE

Lindsay PECQUERIAUX

Anaïs PELLETIER

# Liste des sigles, acronymes et abréviations

| | |
|---|---|
| A. | Arrêté |
| AAC | Autorisation d'accès compassionnel |
| AAP | Autorisation d'accès précoce |
| ADEME | Agence de l'environnement et de la maîtrise de l'énergie |
| *ADSP* | *Actualité et dossier en santé publique* |
| AMCA | *American Medical Collection Agency* |
| AMF | Autorité des marchés financiers |
| AMM | Autorisation de mise sur le marché |
| AN | Assemblée nationale |
| ANS | Agence du numérique en santé |
| ANSM | Agence nationale de sécurité du médicament et des produits de santé |
| ANSSI | Agence nationale de la sécurité des systèmes d'information (France) |
| API | Ingrédients pharmaceutiques actifs |
| ARCEP | Autorité de régulation des communications électroniques, des postes et de la distribution de la presse |
| *Arch. pol. crim.* | *Archives de politique criminelle* |
| ARS | Agence régionale de santé |
| art. | Article |
| ASA | Amélioration du service attendu |
| ASIP Santé | Agence des systèmes d'information partagés en santé |
| ASMR | Amélioration du service médical rendu |
| ATU | Autorisation temporaire d'utilisation |
| Aut. conc. | Autorité de la concurrence |
| BARDA | *Biomedical Advanced Research and Development Authority* |
| BDMA | Base de données médico-administratives |
| BNDS | Bibliothèque numérique du droit de la santé et de l'éthique médicale |
| BPD | Bonnes pratiques de distribution |
| BPF | Bonnes pratiques de fabrication |
| *BRDA* | *Bulletin rapide de droit des affaires Francis Lefebvre* |
| *Bull. Cancer* | *Bulletin du Cancer* |
| CA | Cour d'appel |
| CAA | Cour administrative d'appel |
| Cass. 1re, 2e ou 3e civ. | Cour de cassation, 1re, 2e ou 3e chambre civile |
| Cass. ch. réunies | Cour de cassation, chambres réunies |
| Cass. com. | Cour de cassation, chambre commerciale |

| | |
|---|---|
| Cass. crim. | Cour de cassation, chambre criminelle |
| C. civ. | Code civil |
| CBE | Convention sur le brevet européen |
| CCNE | Comité consultatif national d'éthique |
| C. com. | Code de commerce |
| C. consom. | Code de la consommation |
| *CDE* | *Cahiers de droit de l'entreprise* |
| C. déont. méd. | Code de déontologie médicale |
| CE | Conseil d'État |
| CEDH | Cour européenne des droits de l'homme |
| C. env. | Code de l'environnement |
| CEPS | Comité économique des produits de santé |
| CERNA | Comité d'éthique de la recherche sur le numérique |
| CESCE | Conseil économique et social des Communautés européennes |
| CESE | Comité économique et social européen |
| CESP | *Common European Submission Platform* |
| CGI | Code général des impôts |
| cGMP | *current Good Manufacturing Practices* |
| CHMP | Comité des médicaments à usage humain |
| CIMAP | Comité interministériel pour la modernisation de l'action publique |
| Circ. | Circulaire |
| CI-SIS | Cadre d'interopérabilité des systèmes d'information de santé |
| CJCE | Cour de justice des Communauté européennes |
| CJUE | Cour de justice de l'Union européenne |
| CNAM | Caisse nationale d'assurance maladie |
| CNC | Conseil national de la consommation |
| CNEDiMTS | Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé |
| CNIL | Commission nationale de l'informatique et des libertés (France) |
| CNNum | Conseil national du numérique |
| CNOM | Conseil national de l'Ordre des médecins |
| CNOP | Conseil national de l'Ordre des pharmaciens |
| CNRS | Centre national de la recherche scientifique |
| CNS | Conseil du numérique en santé |
| Comm. CE | Commission des Communautés européennes |
| *Comm. com. électr.* | *Communication commerce électronique* |
| Comm. UE | Commission de l'Union européenne |
| Cons. const.. | Conseil constitutionnel |
| Const. | Constitution |
| Cons. UE | Conseil de l'Union européenne |

| | |
|---|---|
| *Contrats, conc. consom.* | *Contrats, concurrence consommation* |
| Conv. EDH | Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales |
| C. pén. | Code pénal |
| CPI | Code de la propriété intellectuelle |
| CREDOC | Centre de recherche pour l'étude et l'observation des conditions de vie |
| CRO | *Contract Research Organization* |
| CSA | Conseil supérieur de l'audiovisuel |
| C. santé publ. | Code de la santé publique |
| CSF | Comité stratégique de filière |
| CSF-ITS | Comité stratégique de filière des industries et technologies de santé |
| CSS | Code de la sécurité sociale |
| CT | Commission de la transparence |
| CTD | *Common Technical Document* |
| *D.* | *Dalloz (recueil)* |
| D. | Décret |
| *Dalloz IP/IT* | *Dalloz IP/IT : droit de la propriété intellectuelle et du numérique* |
| DDHC | Déclaration des droits de l'homme et du citoyen |
| DEEP | Dispositif d'enregistrement électronique partagé |
| Délib | Délibération |
| DGCCRF | Direction générale de la concurrence, de la consommation et de la répression des fraudes |
| DGS | Direction générale de la santé |
| *Dict. perm.* | *Dictionnaire permanent* |
| Dir. | Directive |
| DIV | Diagnostic *in vitro* |
| DM | Dispositif médical |
| DMC | Dispositif médical connecté |
| DME | Dossiers médicaux électroniques |
| DMI | Dispositif médical implantable |
| DMP | Dossier médical partagé (anciennement « Dossier médical personnel ») |
| DMT | Dossier médico technique |
| Doc. COM | Document communautaire (Europe) |
| Doc. fr. | Documentation française (La) |
| DPO | *Data Privacy Officers* |
| DREES | Direction de la recherche, des études, de l'évaluation et des statistiques |
| *DSIH* | *L'actualité des systèmes d'information hospitaliers et de la e-santé* |
| DSSIS | Délégation à la stratégie des systèmes d'information de santé |
| DUDH | Déclaration universelle des droits de l'homme |
| E-CTD | *Electronic Common Technical Document* |

| | |
|---|---|
| EEE | Espace économique européen |
| ELAN (Loi) | Loi portant évolution du logement, de l'aménagement et du numérique |
| EMA | Agence européenne des médicaments (*European Medicines Agency*) |
| ETP | Équivalent temps plein |
| EUDAMED | Base de données européenne du dispositif médical |
| FDA | *Food and Drug Administration* |
| FM Litec | Feuillets mobiles Litec |
| FNDP | Fédération nationale des dépositaires pharmaceutiques |
| FRANCE MVO | *Medicines Verification Organisation* |
| GAFAM | Google, Amazon, Facebook, Apple, Microsoft |
| *Gaz. Pal.* | *Gazette du Palais (La)* |
| GHS | Groupe homogène de séjour |
| GRADeS | Groupement régional d'appui au développement de l'e-santé |
| HAD | Hôpital à domicile |
| HAS | Haute Autorité de santé |
| HDH | *Health Data Hub* |
| HIPAA | *Health Insurance Portability and Accountability Act* |
| HPST (Loi) | Loi portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires |
| IA | Intelligence artificielle |
| ICO | *Initial Coin Offering* |
| *infra* | ci-dessous |
| INPI | Institut national de la propriété intellectuelle |
| INS | Identifiant national de santé |
| INSEE | Institut national de la statistique et des études économiques |
| INSERM | Institut national de la santé et de la recherche médicale |
| IoT | *Internet of Things* (en français : Internet des Objets [IdO]) |
| IPO | *Initial Public Offering* |
| IRDES | Institut de recherche et de documentation en économie de la santé |
| IRSN | Institut de radioprotection et de sûreté nucléaire |
| IT | *Information Technology* |
| *JCl.* | *JurisClasseur* (Encyclopédie) |
| *JCP* A | *JurisClasseur Périodique* (Semaine juridique), édition Administration et collectivités territoriales |
| *JCP* E | *JurisClasseur Périodique* (Semaine juridique), édition Entreprise et affaires |
| *JCP* G | *JurisClasseur Périodique* (Semaine juridique), édition Générale |
| *JO* | *Journal officiel* (de la République française) |
| *JOUE* | *Journal officiel* (de l'Union européenne) |
| L. | Loi |
| L. const. | Loi constitutionnelle |

| | |
|---|---|
| L. fin. | Loi de finances |
| LAP | Logiciel d'aide à la prescription |
| LEEM | Les Entreprises du médicament |
| LME | Loi de modernisation de l'économie |
| *LPA* | *Petites affiches (Les)* |
| LPF | Livre des procédures fiscales |
| LPPR | Liste des produits et prestations remboursables |
| *M&A* | *Merger and Acquisition* |
| *Mél.* | *Mélanges* |
| *Med Sci* | *Médecine/sciences* |
| NEC | Numérique en commun |
| NIR | Numéro d'identification au répertoire |
| *Nouv. Cah. Cons. const.* | *Nouveaux Cahiers du Conseil constitutionnel* |
| NTA | *Notice To Applicant* |
| OCDE | Organisation de coopération et de développement économiques |
| OEB | Office européen des brevets |
| OMS | Organisation mondiale de la santé |
| ONIAM | Office national d'indemnisation des accidents médicaux, des affections iatrogènes et des infections nosocomiales |
| ONU | Organisation des Nations unies |
| OPECST | Office parlementaire d'évaluation des choix scientifiques et technologiques |
| Ord. | Ordonnance |
| PCG | Plan comptable général |
| PE et Cons. UE | Parlement européen et Conseil de l'Union européenne |
| PFTHD | Plan France Très Haut Débit |
| PIB | Produit intérieur brut |
| PIPAME | Pôle interministériel à la prospective et à l'anticipation des mutations économiques |
| PLFSS | Projet de loi de financement de la sécurité sociale |
| PMF | Prescription médicale familiale |
| Préc. | Précité |
| Prop. | Proposition |
| QPC | Question prioritaire de constitutionnalité |
| QR code | *Quick Response code* |
| Rapp. | Rapport |
| R&D | Recherche et développement |
| *RD sanit. soc.* | *Revue de droit sanitaire et social* |
| Recomm. | Recommandation |
| Règl. | Règlement |
| *Rev. Lamy dr. aff.* | *Revue Lamy Droit des affaires* |

| | |
|---|---|
| *Rev. Lamy dr. civ.* | *Revue Lamy Droit civil* |
| RF | Référentiel fonctionnel de labellisation |
| *RF adm. publ.* | *Revue française d'administration publique* |
| *RF aff. soc.* | *Revue française des affaires sociales* |
| RFID | *Radio Frequency Identification* |
| *RGDM* | *Revue générale de droit médical* |
| RGPD | Règlement général sur la protection des données |
| *RID comp.* | *Revue internationale de droit comparé* |
| *RID éco.* | *Revue internationale de droit économique* |
| *RJDA* | *Revue de jurisprudence de droit des affaires* |
| *RLDI* | *Revue Lamy Droit de l'immatériel* |
| *RPPI* | *Revue pratique de la prospective et de l'innovation* |
| *RTD com.* | *Revue trimestrielle de droit commercial et de droit économique* |
| RTU | Recommandation temporaire d'utilisation |
| SA | Service attendu |
| SI | Système d'information |
| SIH | Système d'information hospitalier |
| SIS | Système d'information de santé |
| SMR | Service médical rendu |
| SNDS | Système national des données de santé |
| ss dir. | sous la direction de |
| *supra* | ci-dessus |
| T. confl. | Tribunal des conflits |
| TFUE | Traité sur le fonctionnement de l'Union européenne |
| TGI | Tribunal de grande instance |
| TIC | Technologies de l'information et de la communication |
| UDI | *Unique Device Identification* |
| UE | Union européenne |
| UNCAM | Union des caisses nationales d'assurance maladie |
| V. | Voir |

# Préface

Le développement du numérique dans le domaine de la santé questionne la société. Ce que certains qualifient de *e-santé* qui regrouperait la télé-médecine, l'information médicale, l'intelligence artificielle, etc., interroge quant à ses usages quant au rôle renouvelé des acteurs de la santé sur fond d'exigence juridique mais aussi éthique.

Le développement du numérique dans le domaine de la santé et les questions soulevées par ses conséquences en termes juridiques sur la réorganisation du système de santé constituent le thème de cet ouvrage.

Nul doute que la crise dite de « la COVID 19 » aura catalysé les questions soulevées par les rapports entre la santé et le numérique et qu'elle aura permis encore mieux d'identifier ses enjeux, ses règles du jeu et les difficultés techniques, juridiques et sociales que ce rapport entre santé et numérique peut susciter, notamment en temps de crise.

L'insertion du numérique dans le domaine de la santé peut générer des révolutions dans la manière d'appréhender la relation entre le patient et le domaine médical en termes de pratiques professionnelles et concernant l'organisation même du système de santé. Le numérique va bouleverser bien des points et peut-être modifier profondément la conception et les acceptions que la société peut avoir du domaine de la santé et que les acteurs peuvent avoir eux-mêmes de leur rôle dans l'organisation et le fonctionnement de ce secteur.

L'ouvrage, dirigé par M$^{me}$ Béatrice ESPESSON, est remarquable à bien des égards. Il est, comme toujours dans le travail de la Directrice du « Master Droit des Affaires appliqué aux industries de santé » extrêmement innovant. Il ouvre de nombreuses portes sur un plan juridique mais plus largement sur un plan intellectuel. Il est très bien organisé autour de thèmes qui le rendent pédagogique.

L'ouvrage aborde d'abord la politique de santé et la révolution numérique puis les nouvelles technologies connectées et l'intelligence artificielle avant de s'intéresser à l'impact du numérique dans la recherche du développement des produits de santé, à l'impact du numérique dans l'évaluation de la mise sur le marché et enfin dans la production des produits de santé.

Il développe ensuite la question très délicate de l'intelligence artificielle et de la « Blockchain » au service de la sécurisation logistique des produits dans le secteur pharmaceutique.

Des développements tout à fait pertinents et passionnants sont également consacrés à l'impact du numérique dans la distribution des produits de santé quant à l'intelligence artificielle et aux algorithmes comme nouveaux modes de concurrence, quant à l'impact du numérique sur la consommation des produits et des prestations de santé et sur le mode de consommation du patient consommateur des produits de santé connectés et enfin dans le domaine de l'environnement et de la fiscalité des industries de santé.

C'est dire si l'ouvrage est complet s'il est particulièrement arborescent sur un sujet qui est, à ce stade, sur un plan scientifique et substantiel, à peine défloré par la communauté scientifique. Il constituera donc très certainement un ouvrage de référence pour lequel il convient de remercier sa directrice qui offre ainsi un magnifique outil de travail et de savoir aussi bien aux acteurs de la santé qu'à ceux qui réfléchissent à ces sujets.

**Baptiste BONNET**
**Professeur à l'Université Jean Monnet de Saint-Étienne**
**Doyen de la faculté de Droit.**

# Sommaire

# INTRODUCTION

Béatrice ESPESSON-VERGEAT

Le numérique en santé est un sujet majeur d'analyse dans un contexte inédit de développement numérique et scientifique, d'engagement dans l'amélioration et la protection de la santé publique. La pandémie Covid-19 joue comme un accélérateur et un catalyseur des énergies concernant le développement du numérique en santé, mais elle cristallise aussi toutes les problématiques autour de la protection des patients. Elle met en exergue toute la difficulté d'un monde économique à se tourner avec rapidité, agilité vers de nouveaux concepts, de nouveaux modèles économiques depuis la recherche jusqu'à la distribution des produits ou services. Ce monde brutalement bouleversé a été propulsé dans un univers numérique peu ou mal maîtrisé par les acteurs de santé, avec des fractures profondes dans la connaissance et l'utilisation des produits qui en sont issus entre les professionnels et établissements de santé, les industries de santé et les prestataires numériques au sens large, comprenant les programmeurs, plateformes de services qui deviennent les acteurs centraux du système de santé.

Les questions juridiques autour de la réorganisation de ce système de santé sont multiples et nécessitent une approche rigoureuse permettant d'identifier la possibilité de traitement des problématiques sur les bases du droit positif existant, ou la nécessité d'avoir une analyse créative, prospective, adaptée aux innovations numériques et scientifiques. Dans ce contexte sanitaire mouvant, aux impacts économiques, sociologiques, politiques phénoménaux, la difficulté consiste à adapter le rythme juridique à celui de l'innovation, voire à anticiper les questionnements afin d'en cadrer les conséquences dans une vision éthique du progrès de la société.

L'étude portant sur droit, santé et numérique implique de s'intéresser à l'évolution globale du système de santé national, européen, mais aussi international. La pandémie démontre parfaitement l'impossibilité de limiter l'approche aux seules questions territoriales, dès lors que l'enjeu sanitaire est mondial tant dans les effets de la pandémie sur la santé des populations, que dans les enjeux économiques et juridiques portant sur la localisation des activités d'innovation de production et distribution des produits, sur la coopération européenne dans l'organisation des soins au cœur de la crise.

Les innovations portant sur la mise en œuvre accélérée des recherches, celle de la mise sur le marché des produits, notamment des vaccins, l'organisation sécurisée des chaînes de production et circuits logistiques, enfin la coordination des soins sont fondamentalement basés sur l'utilisation du numérique qui favorise cette

accélération. Cette situation a permis de renforcer le poids des *start-up*, licorne du numérique face aux acteurs big pharma notamment, mais aussi face aux établissements de santé, laboratoires de biologie médicale ou patients utilisateurs dans leurs relations avec les professionnels de santé.

Ce contexte particulier est marqué par un besoin puissant d'une réglementation stricte et rassurante permettant d'organiser avec une certaine prévisibilité juridique les effets de la pandémie, afin de retrouver un univers sécurisé, mais aussi dans le même temps un besoin de souplesse normative et de mouvement marquant la nécessité d'avoir une approche agile, au sens du management agile des entreprises. Les juristes et directions juridiques des industries de santé ont pris pendant cette période une importance considérable dans l'analyse de l'adaptabilité de la norme afin de rendre possibles et efficaces les activités économiques et de santé grâce au numérique.

Le rôle du juriste est désormais considérable dans l'élaboration d'un équilibre entre la sécurité et l'efficacité médicale et scientifique dans un contexte d'emballement de l'innovation numérique et de risques aggravés concernant la protection des données personnelles et de santé. Il doit arbitrer les décisions et enjeux en favorisant l'innovation tout en garantissant la protection de la santé publique. La dichotomie entre liberté d'entreprendre, notamment dans le secteur numérique en santé, et protection de la personne et de la santé publique est portée à son paroxysme.

Les nouveaux outils tels que l'intelligence artificielle, les algorithmes, la *blockchain* sont au cœur de toutes les études économiques, politiques, sociologiques, mais, dans le secteur de la santé, ces outils doivent être approchés au plan juridique dans une vision éthique de la protection des données du patient.

Cet ouvrage sur droit santé et numérique a pour vocation de cibler au cours des différentes phases de la vie d'un produit de santé, l'impact du numérique dans le développement et la croissance de l'activité d'une entreprise de santé, en intégrant le fait que le numérique peut revêtir une double fonction. Il peut être un moyen technique permettant d'améliorer l'activité traditionnelle des industries de santé ou des établissements de santé, et acteurs de santé. Le numérique peut aussi être approché comme un objectif, c'est à dire comme la possibilité d'un nouveau marché de produits dans lesquels sont intégrés comme centraux les objets connectés, les robots, les plateformes numériques de santé, ou encore les algorithmes d'analyse médicale. Les acteurs de santé portent leurs efforts économiques vers l'intégration de ces nouveaux objets de produits ou prestations de services, en faisant alliance avec les acteurs spécialistes du numérique, généralement portés par des *start-up*, plus agiles, plus mobiles et réactives que les big pharma.

Le marché économique est alors fortement engagé au niveau mondial dans une reconfiguration générale de son modèle, au-delà des frontières et au-delà des équilibres de pouvoir historiques est-ouest ou nord-sud, au milieu desquels se trouve la vieille Europe en recherche d'un nouvel élan de compétitivité par la relocation des industries de santé.

La pandémie Covid-19 a permis de mettre en exergue ces changements avec une percée fulgurante de la recherche vaccinale, fondée sur des alliances de *start-up* et laboratoires big pharma, mais aussi sur des coopérations inédites entre les industries

de santé, favorisées par la Commission européenne. Elle a permis de révéler également la trop forte dépendance de l'industrie mondiale à l'Asie, et les risques concernant l'organisation générale du système de santé, caractérisés notamment par les retards, tensions et ruptures dans l'approvisionnement de vaccins liés aux ruptures de stocks de matières premières, ainsi que des médicaments essentiels, dispositifs médicaux et équipements de protection individuelle.

Cette crise est un révélateur de l'urgence pour le monde de la santé à s'adapter aux nouvelles techniques numériques permettant une amélioration dans l'organisation du système sanitaire.

L'analyse qui sera développée conduit donc à s'interroger sur cette évolution au plan des politiques de santé, nationale, européenne et internationale avant d'entrer dans les problématiques liées à l'organisation des soins et services et produits numériques autour du patient acteur de sa santé, puis d'approcher par strates successives les différents stades de la chaine de vie des produits, grâce et avec le numérique. L'innovation est la première phase la plus marquée par l'utilisation du numérique dans la recherche et développement, qui permet de créer des algorithmes et IA plus puissantes sans toutefois écarter la nécessité d'une création et d'un contrôle humain. Puis vient la phase de protection de cette innovation dans un contexte d'interrogation sur le produit de santé comme bien commun de l'humanité, produit néanmoins par des sociétés commerciales soucieuses de préserver leur modèle. La phase d'essais clinique est la plus risquée car elle nécessite l'accélération des procédures *in vitro* avant de passer à une phase d'essai sur l'humain et de contrôle *in vivo*. L'accélération dans la recherche pendant la phase pandémique a permis de tordre les dispositions réglementaires afin d'intégrer cette nécessité de célérité dans l'intérêt de la santé publique mondiale. Mais les risques juridiques importants auxquels sont exposés les fabricants les ont conduits à une négociation sur la responsabilité du fait de l'utilisation des produits innovants mis sur le marché de manière anticipée. La mise sur le marché et les conditions de surveillance du produit grâce aux outils numériques sont aussi marquées par cette nouvelle approche numérique de la santé. En parallèle la production et la *Supply chain* sont accélérées avec le recours à l'IA et à la BC améliorant le contrôle et la rapidité dans l'acheminement des produits au niveau international. Autant d'activités fortement impactées par le numérique et qui exigent des analyses et adaptations juridiques constantes notamment sur les questions contractuelles ou encore dans l'analyse des risques et responsabilités des acteurs de santé.

Enfin, l'utilisation du produit et sa mise à disposition au profit des établissements de santé, laboratoires de biologie, radiologie, professionnels de santé, utilisateurs et patients est la phase la plus visible avec une pénétration généralisée du numérique, et une porosité entre les activités. La question majeure et fondamentale de la protection des données de santé est alors la plus analysée, mais cette question en cache de nombreuses autres et tout particulièrement celles portant sur la valorisation des données par le patient lui-même, l'encadrement normatif indispensable dans une perspective de protection de l'éthique, ou encore la nécessité de redéfinir et identifier les responsabilités du fait des produits connectés et la possible responsabilité du robot intelligent.

La vie du produit de santé marqué par le numérique, et celle du produit de santé connecté, l'organisation du service de santé confronté aux évolutions numériques, l'élaboration du parcours de santé du patient numérique ou encore la création du *hub* santé conduisent le juriste à intégrer au sein de son analyse une dimension scientifique, pharmaceutique, médicale et numérique, c'est-à-dire à s'engager dans une approche transversale de l'environnement économique dans lequel se situent les acteurs afin de résoudre au mieux les cas qui lui seront soumis.

L'approche juridique suppose, au-delà de la connaissance de l'univers de la santé numérique, d'avoir une approche prospective sur le déploiement de ces outils et solutions afin d'envisager le traitement des questions qui ne manqueront pas de survenir, dans une démarche d'efficience.

Cette vision suppose une analyse de l'encadrement législatif, réglementaire existant,(1) de la position du juge au niveau national et européen, mais aussi d'une interprétation de l'encadrement juridique souple qui se traduit par l'élaboration de guides et recommandations, d'accords, conventions, traduisant la force d'un droit en mouvement, agile, adaptable aux évolutions et risques sanitaires. Dans une perspective d'internationalisation des questions de santé publique, les acteurs de santé s'appuient sur ces techniques permettant une inter-régulation hors du champ écrit de la norme. Ainsi, le Royaume-Uni, par la coordination (sans texte) des différentes autorités publiques indépendantes nationales s'ajuste aux textes de l'Union européenne pour superviser l'espace digital avec les objectifs articulés de sauvegarde de l'innovation par la concurrence, de supervision des contenus, de préservation de la liberté d'expression(2).

C'est dans une vision de l'adaptabilité de la norme afin de garantir l'équilibre entre enjeux économiques et protection de la personne et de la santé publique, que cet ouvrage a été conçu autour de la thématique droit-santé et numérique. Ces études ont été réalisées avec le concours d'experts, juristes et avocats, spécialistes du secteur de la santé, confrontés à la difficulté d'adapter la temporalité des innovations scientifiques et médicales à celle de l'élaboration de la norme.

Innovation, temporalité, territorialité, sont les sujets forts soulevés par le numérique, mettant en exergue les questions relatives à la protection des données de santé, à l'encadrement des libertés fondamentales, et enfin et surtout à l'équilibre entre protection de la santé publique et préservation des libertés individuelles de l'humain dans un contexte sanitaire frappé par la pandémie Covid-19.

(1) La loi relative à l'organisation et transformation du système de santé, promulguée le 24 juillet 2019, a étendu le Système National des Données de Santé (SNDS), initialement limité aux données médico-administratives, aux données associées à un financement public afin d'en faciliter l'accès. La loi prévoit également la création d'une plateforme des données de santé ou « Health Data Hub » qui fut créée le 30 novembre dernier. Cette structure reprend et élargit les missions de l'INDS en proposant davantage de services pour les demandeurs d'accès aux données de santé.

(2) Digital regulation cooperation forum, plan of work for 2021 to 2022, 10 mars 2021, competition and markets authority.

CHAPITRE 1

# LA POLITIQUE DE SANTÉ ET LA RÉVOLUTION NUMÉRIQUE

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Kamel BESSEGHIER
Alexandre FAURE

L'Organisation mondiale de la santé (OMS) définit la santé numérique comme un ensemble d'activités et de composantes (telles que les applications mobiles, les objets connectés comme les montres, ou encore le dossier médical personnalisé) ayant recours à des moyens électroniques pour délivrer des informations, des ressources et des services en lien avec la santé[1]. Lors de l'Assemblée mondiale de la santé de 2018, les gouvernements ont adopté à l'unanimité une résolution appelant l'OMS à mettre au point une stratégie mondiale sur la santé numérique pour soutenir les efforts nationaux en faveur de la couverture sanitaire universelle. L'OMS émet des avis et recommandations qui doivent permettre de conduire les États sur le chemin de l'intégration du numérique dans leur politique de santé interne. Pour aider les gouvernements à suivre et à coordonner les investissements en faveur des technologies numériques, l'OMS a mis au point le *Digital Health Atlas*, une base de données mondiale en ligne où les personnes chargées de la mise en œuvre peuvent enregistrer leurs activités dans le domaine de la santé numérique. Au fil des années, l'OMS a publié plusieurs documents pour renforcer la recherche et la mise en œuvre dans le domaine de la santé numérique. En 2019, le Dr Tedros a annoncé la création du département « Santé numérique » afin que l'OMS joue un plus grand rôle dans l'évaluation des technologies numériques et aide les États membres à les hiérarchiser, à les intégrer et à les réglementer. Le projet de stratégie mondiale pour la santé numérique 2020-2025 énonce les stratégies à développer afin d'atteindre cet objectif. En 2005, dans sa résolution WHA58.28 sur la cybersanté, l'Assemblée mondiale de

(1) A. Becuwe et C. Thébaut, *Introduction du numéro spécial : les impacts des nouvelles technologies sur les systèmes de santé : Marché et organisation* 2020, « La santé connectée, nouvelles technologies et réorganisation des soins », p. 9-13.

la santé invitait instamment les États membres « à envisager d'élaborer un plan stratégique à long terme pour concevoir et mettre en œuvre des services de cybersanté dans les différents domaines du secteur de la santé (…) à développer des infrastructures pour appliquer à la santé les technologies de l'information et de la communication (…) afin de promouvoir un accès équitable, d'un coût abordable et universel à leurs avantages ». Puis, en 2013, l'Assemblée mondiale de la santé a adopté la résolution WHA66.24 intitulée « Normalisation et interopérabilité en cybersanté », dans laquelle elle invitait instamment les États membres à « envisager d'élaborer (…) des politiques et des mécanismes législatifs liés à une stratégie nationale globale de cybersanté ». Le Programme de développement durable à l'horizon 2030 souligne que l'expansion des technologies de l'information et de la communication ainsi que l'interdépendance mondiale des activités ont le potentiel d'accélérer les progrès de l'humanité, de réduire la fracture numérique et de donner naissance à des sociétés du savoir[(2)]. L'utilisation stratégique et novatrice des technologies numériques et des technologies de pointe en matière d'information et de communication sera un facteur essentiel qui permettra d'atteindre l'objectif du « triple milliard » de l'OMS, soit un milliard de personnes supplémentaires bénéficiant de la couverture sanitaire universelle, un milliard de personnes supplémentaires mieux protégées face aux situations d'urgence sanitaire, et un milliard de personnes supplémentaires bénéficiant d'un meilleur état de santé et d'un plus grand bien-être (figurant dans son treizième programme général de travail, 2019-2023). L'intégration du numérique en santé dans l'application concrète des politiques nationales est un enjeu majeur et complexe, mais incontournable pour l'évolution du monde de la santé et de la santé dans le monde. La transformation numérique des soins de santé peut être déstabilisante. Toutefois, des technologies telles que l'Internet des objets (Iot), les soins virtuels, le suivi à distance, l'intelligence artificielle (IA), l'analyse de mégadonnées, la chaîne de blocs (*blockchain*), les dispositifs portables intelligents, les plateformes, les outils facilitant l'échange et le stockage de données, les outils permettant la saisie et l'échange de données à distance, ainsi que le partage d'informations pertinentes dans tout l'écosystème de la santé contribuant ainsi à la continuité des soins, ont prouvé leur efficacité. Elles permettent d'améliorer les résultats sanitaires grâce à la performance des diagnostics médicaux, des décisions de traitement fondées sur des données, des thérapies numériques, des essais cliniques, de l'autogestion des soins et des soins centrés sur la personne, ainsi qu'à la production de connaissances, d'aptitudes et de compétences davantage fondées sur des bases factuelles à l'intention des professionnels en vue de soutenir les soins de santé.

Ce sont donc de nouveaux paradigmes en santé qui apparaissent grâce au numérique. Cette évolution vers une nouvelle forme de santé et de soins permet de réduire les inégalités en santé, d'accélérer l'accès à la santé pour tous, et surtout de favoriser le développement de nouveaux produits innovants complexes dotés de numérique permettant d'améliorer l'approche du soin et du diagnostic[(3)].

(2) AG ONU, Rés. 70/1 (2015).

(3) Reconnaissant la nécessité de renforcer la mise en œuvre de la santé numérique, la soixante et onzième Assemblée mondiale de la Santé a adopté en mai 2018 la résolution WHA71.7 sur la santé numérique.

En conséquence, la santé numérique doit faire partie intégrante des priorités en matière de santé et bénéficier aux personnes dans le respect de l'éthique et de manière sûre, fiable, équitable et durable. Elle doit être élaborée selon les principes de transparence, d'accessibilité, de transposition à plus grande échelle, de répétabilité, d'interopérabilité, de respect de la vie privée, de sécurité et de confidentialité. L'objectif de la stratégie mondiale est de renforcer les systèmes de santé moyennant l'application des technologies numériques pour les consommateurs, les professionnels de la santé, les prestataires de soins de santé et l'industrie afin de parvenir à l'autonomisation des patients et à concrétiser la vision de la santé pour tous. La santé numérique signifie « le domaine de connaissances et de pratiques associé au développement et à l'utilisation des technologies numériques pour améliorer la santé ». Cette définition englobe la cybersanté[4]. La santé numérique élargit le concept de cybersanté pour inclure les consommateurs numériques, avec un plus large éventail d'appareils intelligents et connectés. Cette approche est d'autant plus prégnante depuis le début de la pandémie de Covid-19 qui est apparue comme un catalyseur révélant le caractère indispensable du numérique dans la gestion de la santé publique[5].

L'approche de la stratégie mondiale cible l'ensemble des difficultés et obstacles à franchir pour atteindre l'objectif et notamment assurer la protection des données sensibles et de santé du patient, assurer la sécurisation des données au niveau international, lutter contre la cybercriminalité, et promouvoir le consentement des patients. Parvenir à cet objectif suppose l'adoption de dispositions législatives et réglementaires, de normes, *guidelines*, chartes permettant d'assurer un encadrement tout à la fois solide et souple, innovant et sécurisant, sans y voir d'oxymore. L'adaptation agile des aspects juridiques au numérique en santé est une priorité. La nécessité de disposer d'une base juridique et réglementaire solide s'impose afin de protéger la vie privée, la confidentialité, l'intégrité et la disponibilité des données ainsi que le traitement des données sanitaires personnelles, et de gérer les questions de cybersécurité, l'établissement de relations de confiance, de responsabilisation et de gouvernance, d'éthique, d'équité, de renforcement des capacités et de connaissances, en veillant à ce que des données de bonne qualité soient collectées et ensuite partagées pour appuyer les efforts en matière de planification, de mise en service et de transformation des services. Il est important de maintenir la transparence et de communiquer efficacement sur les stratégies relatives à la sécurité des données.

Ces principes, mis en avant par l'OMS, sont largement repris par les États et intégrés dans leurs politiques nationales de santé[6]. Ainsi, en France, la stratégie « Ma

(4) *WHO guideline recommendations on digital interventions for health system strengthening : evidence and recommendations*, Genève, Organisation mondiale de la santé, 2019. Le document EB142/20 sur la cybersanté, dont le Conseil exécutif a pris note à sa cent quarante deuxième session (V. le document EB142/2017/REC/2, procès-verbaux de la treizième séance, section 2), indiquait qu'« à l'heure actuelle, on entend souvent par "santé numérique" un terme générique englobant la cybersanté ainsi que des domaines innovants comme l'utilisation de l'informatique de pointe (dans les secteurs des "mégadonnées", de la génomique et de l'intelligence artificielle, par exemple) ».

(5) A. Motulsky, P. Després, C. Petitgand, J.-N. Nikiema, C. Régis et J.-L. Denis, *Veille sur les outils numériques en santé dans le contexte de Covid-19*, Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA), oct. 2020.

(6) Ministère des Solidarités et de la Santé, *Recours au numérique pour mieux soigner*, « Ma santé 2022 », feuille de route « Accélérer le virage numérique », publiée le 12 février 2019, dernière mise à jour 5 juin 2019 (https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/masante2022/article/recourir-au-numerique-pour-mieux-soigner).

santé 2022 » présente un plan actif et ambitieux pour établir le numérique en santé. Les travaux d'études sur l'application du numérique dans la société, et plus particulièrement en santé, pullulent afin de promouvoir un encadrement souple et sécurisé[7]. Elles sont aussi intégrées par la Commission européenne dans sa politique de santé numérique. Toutefois, il convient de préciser que l'Union européenne, bien que très active désormais dans le secteur de la santé, et notamment depuis le début de la pandémie, n'a qu'une compétence d'appui. En conséquence, elle ne dispose que d'un pouvoir d'accompagnement, de guides des États membres, qui demeurent souverains dans leur politique de santé[8], et d'accompagnement dans le financement des États membres pour la mise en place des politiques de santé nationales dans l'objectif visé par la Commission notamment dans le programme *EU4Health* institué par le règlement UE 2021/522, en réponse à la pandémie Covid-19[9]. L'initiative intitulée « Une Europe adaptée à l'ère numérique » fait partie des six priorités politiques de la Commission pour la période 2019-2024. S'appuyant sur des initiatives antérieures en faveur de la création d'un marché unique numérique, la transition numérique devrait profiter à tous, donner la priorité aux citoyens et ouvrir de nouvelles perspectives aux entreprises. La santé figure parmi les secteurs visés par cette initiative, étant donné les avantages potentiels que les services numériques peuvent offrir aux citoyens et aux entreprises dans ce domaine. Comme l'indique la Commission européenne, « la santé en ligne comporte des avantages pour les individus, les patients, les professionnels des secteurs de la santé et des soins, mais aussi pour les organismes du secteur de la santé et les pouvoirs publics »[10]. Elle permet un suivi des patients qui ne peuvent sortir de chez eux et les aide à garder le lien social avec leur médecin, ce qui représente un avantage certain.

Ainsi, la Commission incite les États à encourager les innovations technologiques portées par le numérique en matière de santé[11]. La pandémie de Covid-19 a permis d'établir que la maîtrise des outils numériques de santé par les citoyens et les informations numériques générales dans le domaine de la santé[12], tels que les applications de santé ou le dossier médical partagé, permettent d'aller plus loin et plus vite dans de nombreux domaines, et notamment dans le milieu médical. Cette crise a permis de révéler l'enjeu des outils numériques dans l'organisation de la politique de santé auprès des populations avec un objectif de réduction des inégalités qui s'accroissent considérablement[13]. Néanmoins, ces évolutions numériques doivent s'opérer au sein de l'espace européen dans le cadre de la protection des données de santé et données personnelles, qui représente un droit fondamental

(7) S. Duboc et D.-J. Noël, *Économie et gouvernance de la donnée*, Avis du Conseil économique, social et environnemental présenté au nom de la section des activités économiques, 10 févr. 2021.

(8) A. Becuwe et C. Thébaut, *Introduction du numéro spécial : les impacts des nouvelles technologies sur les systèmes de santé : Marché et organisations* 2020, vol. 38, n° 2, p. 9-13.

(9) Règl. UE 2021/522 établissant un programme d'action de l'Union dans le domaine de la santé (programme « L'UE pour la santé ») pour la période 2021-2027.

(10) Communication de la Comm. au PE, au CESCE et au CdR, Plan d'action pour la santé en ligne 2012-2020 – des soins de santé innovants pour le XXIe siècle : Doc. COM (2012), 0736 final.

(11) *Summary report*, 18th Meeting of the eHealth Network, 12-13 nov. 2020.

(12) CESE, avis relatif à « La maîtrise des outils numériques de santé – pour des soins de santé adaptés aux besoins des citoyens en Europe en période de changement démographique » (avis d'initiative) : *JO* n° C228, 5 juill. 2019, p. 01.

(13) V. Ramel, *Les technologies numériques en santé face aux inégalités sociales et territoriales : une sociologie de l'action publique comparée*, thèse, Médecine humaine et pathologie, Université de Bordeaux, 2020.

des citoyens européens (règlement général sur la protection des données personnelles [RGPD])[14]. Une récente étude de la Commission européenne pointe les difficultés d'application de cette politique de protection des données en santé au sein des États membres. L'objectif de l'étude était d'examiner et de présenter les règles des États membres de l'UE qui régissent le traitement des données de santé à la lumière du RGPD, de mettre en évidence les différences possibles, d'identifier les éléments susceptibles d'affecter l'échange transfrontalier de données sur la santé dans l'UE pour les soins de santé ou pour la recherche, l'innovation et l'élaboration des politiques, et d'examiner le potentiel d'action au niveau de l'UE pour soutenir l'utilisation des données dans le secteur de la santé et leur réutilisation. L'étude constate que si le règlement général sur la protection des données (RGPD) établit des règles horizontales directement applicables dans tous les États membres, il subsiste des variations dans l'éventail des législations nationales liées à sa mise en œuvre dans le domaine de la santé. En conséquence, une approche fragmentée de la manière dont le traitement des données de santé pour la santé et la recherche est conduit dans les États membres peut avoir un impact négatif sur la coopération transfrontalière pour la fourniture de soins, l'administration du système de santé, la santé publique ou la recherche. L'objectif est de parvenir à garantir que les systèmes de santé européens puissent utiliser au mieux les données de santé et soutenir le développement de l'espace européen des données de santé. Pour cela, un certain nombre de questions juridiques et opérationnelles doivent être abordées dans une approche à multiples facettes. Plusieurs actions sont envisageables au niveau de l'UE, y compris des codes de conduite axés sur les parties prenantes ainsi qu'une nouvelle législation au niveau de l'UE ciblée et sectorielle. Cette avancée implique d'élaborer une nouvelle réglementation européenne portant sur les exigences légales et la gouvernance. Elle traduit également la nécessité d'une approche plus harmonisée entre les États membres en ce qui concerne l'infrastructure technique, l'interopérabilité technique et sémantique. La qualité et l'acquisition des données, les compétences numériques et le renforcement des capacités pour l'utilisation primaire et secondaire des données sur la santé ont également été identifiés, dans lesquels une approche harmonisée pourrait être bénéfique. La construction d'une approche européenne du numérique en santé est une priorité absolue, avec la protection environnementale pour les années à venir. Cette dynamique est en route avec le programme *EU4Health* qui invite les États à s'engager activement dans la démarche du numérique en santé, grâce notamment au plan de financement de la relance économique post-Covid dégagé par la Commission européenne. Cet élan est également accéléré par l'utilisation de l'intelligence artificielle (IA) dans le secteur de la santé, dont l'encadrement juridique est visé dans un projet de règlement fort attendu, notamment sur la question de la responsabilité de l'IA forte.

En France, le développement du numérique en santé est devenu une priorité dans les politiques économique et de santé publique. Le déploiement de mesures gouvernementales permettant la croissance de ce secteur d'activité est dans une dynamique très active. Toutefois, au niveau privé, le développement du numérique

(14) *Commission publishes study on Assessment of the EU Member States' rules on health data in the light of GDPR.*

en santé avance en ordre dispersé, avec l'apparition de produits numériques dont la qualification juridique et l'exploitation interrogent, et conduisent à des positionnements des autorités de santé sur les conditions d'utilisation et de remboursement des produits améliorant les soins. La Haute Autorité de santé[15] a annoncé, début d'année 2021, la première classification des solutions numériques en santé[16]. Dans un contexte de multiplication des outils numériques utilisables en santé, la Haute Autorité de santé (HAS) vient d'élaborer un système de classification des solutions numériques selon leur finalité d'usage, leur capacité à apporter une réponse personnalisée et leur autonomie, c'est-à-dire leur capacité à agir avec ou sans intervention humaine. L'objectif : aider les acteurs à s'y retrouver et contribuer à une meilleure intégration de ces outils dans le secteur sanitaire et médico-social[17]. La grille proposée par la HAS pourrait aider à structurer les échanges et, *in fine*, contribuer à une intégration efficiente des solutions numériques dans le système de santé, dans ses dimensions sanitaires et médico-sociales. Il convient de bien préciser qu'au niveau national et européen, le cadre du numérique se construit sur les questions d'autonomie et d'intelligence artificielle (IA), sujets sur lesquels la Commission européenne est très active avec un travail fourni sur le rôle de l'intelligence artificielle dans la construction de la santé de demain, dans un contexte d'IA forte et faible[18]. L'intelligence artificielle porte en elle toute la question non résolue de l'autonomie des systèmes et de la responsabilité de l'IA face à celle de l'humain, vaste sujet à traiter[19].

Sur le plan économique, les technologies médicales permettent à plus de neuf cents entreprises de rayonner à l'échelle internationale, et ce dans tous les domaines d'expertises[20]. Il est incontestable que la prise en charge des patients a été considérablement améliorée grâce à ces technologies. Elles permettent la facilitation de la coopération entre professionnels de santé, la sécurisation des prescriptions et le suivi des maladies chroniques, les évaluations des pratiques professionnelles individuelles et les observatoires à partir de cohortes, *etc.* La politique économique actuelle est tout particulièrement favorable aux *startups* et au développement de leurs activités et leurs innovations dans de nouveaux lieux tels que les campus numériques qui fleurissent en France et mettent en relation la formation, la

(15) HAS, *Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (mobile Health ou mHealth)*, 2016 (www.has-sante.fr/jcms/c_2681915/fr/referentiel-de-bonnes-pratiques-sur-les-applications-et-les-objets-connectes-en-sante-mobile-health-ou-mhealth). – HAS, Rapport d'analyse prospective 2019, *Numérique : quelle (R) évolution ?*, 2019 (www.has-sante.fr/upload/docs/appli-cation/pdf/2019-07/rapport_analyse_prospective_20191.pdf).

(16) Classification fonctionnelle, selon leur finalité d'usage, des solutions numériques utilisées dans le cadre de soins médicaux ou paramédicaux, validée par le Collège de la HAS, le 4 février 2021. – HAS, Rapport d'analyse prospective 2019, *Numérique : quelle (R)évolution ?*, 2019 (www.has-sante.fr/upload/docs/application/pdf/2019-07/rapport_analyse_prospective_20191.pdf).

(17) Elle compte au total, onze types de solutions numériques classés en 4 niveaux (A, B, C, D), selon leur finalité d'usage, leur capacité à proposer une réponse personnalisée et leur autonomie dans la décision (celles nécessitant une intervention humaine pour mettre en œuvre une action thérapeutique, de dépistage ou de diagnostic, et celles générant d'elles-mêmes, c'est-à-dire sans intervention humaine préalable, ce même type d'action).

(18) Comm. UE, *Livre blanc : Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance* : Doc. COM(2020), 0065 final, 2020 (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pd).

(19) PE, *Un régime de responsabilité civile pour l'intelligence artificielle*, 2020/2014(INL), 2020 (www.europarl.europa.eu/doceo/document/TA-9-2020-0276_FR.htm).

(20) P. Moustial, *La France dans la compétition mondiale des technologies médicales ? : Les Tribunes de la santé* 2019, n° 60, p. 67-72.

transformation de l'entreprise et l'innovation numérique. Cet emballement pour la santé numérique n'est toutefois pas sans risque, dans la mesure où il est encore sous la dépendance de plateformes étrangères et fait courir des risques de piratages de données de santé de plus en plus fréquents[21]. Par ailleurs, il faut bien comprendre au plan économique le coût du numérique en santé dans la politique de santé, dont l'évaluation est particulièrement complexe à prendre en considération[22]. Le sujet est d'autant plus important dans le traitement de la pandémie de Covid-19 impliquant une démultiplication des outils numériques dans l'organisation des soins avec un impact économique et environnemental particulièrement marqué. Souvent présenté comme une révolution, le numérique en santé traduit incontestablement un virage complet qui touche la société dans son ensemble et plus particulièrement tous les acteurs de santé, publics et privés, et patients acteurs, moteurs dans la mise en œuvre de ces outils[23].

Face à ces bouleversements techniques, technologiques, médicaux et scientifiques, dans un encadrement juridique et réglementaire en constante évolution, la position du patient a considérablement évolué elle aussi, toute la question étant de savoir quel est pour lui le rapport bénéfice/risque de ces innovations. Bien plus qu'un acteur passif, le patient est aujourd'hui un acteur, moteur de sa santé. Il est devenu actif, et même au-delà, il est un acteur déterminant dans la prise en charge de sa santé, notamment dans le choix de son traitement[24]. Ce nouveau rôle est voulu comme central par le législateur au niveau national et européen. La loi Buzyn du 26 juillet 2019[25] a instauré le principe du « patient acteur de sa santé » avec une santé connectée. Au niveau européen, une initiative équivalente a été instaurée, intitulée « Une Europe adaptée à l'ère du numérique »[26], afin de donner plus d'importance au patient dans la prise en charge de sa santé. Ce nouveau rôle était d'ailleurs central dans le rapport de Philippe Lemoine, remis en 2014, sur la « Transformation numérique de l'économie »[27], sur lequel s'appuient notamment les recommandations du Conseil national de l'Ordre des médecins (CNOM)[28]. Cette évolution permet au patient d'envisager sereinement sa santé et, notamment, la consultation et les soins à domicile, ou au travail, offrent un confort et un gain de temps et une meilleure observance des traitements en évitant tous types de transports, mais aussi en assurant une relative sécurité dans le parcours de soin et dans le suivi du patient par Internet.

Au-delà du bénéfice incontestable qu'apportent toutes ces nouvelles technologies numériques à la population et aux patients, celles-ci s'accompagnent

(21) G. Bonnaud, *Des données personnelles médicales sur Google : danger réel du numérique en santé ? : Hegel* 2013, n° 3, p. 161-162.
(22) C. Pascal, *Le coût des innovations numériques : l'impossible évaluation : Ethics, Medicine and Public Health* 2020, 15, 100595.
(23) J.-F. Nys, *La télémédecine, simple évolution ou véritable révolution des usages dans le système de santé français ? : Marché et organisations* 2020, vol. 38, n° 2, p. 15-36.
(24) H. Delmotte, *De la e-santé à la santé connectée : accompagner la transformation de notre modèle de santé : Hegel* 2015, p. 123-126.
(25) L. n° 2019-774, 24 juill. 2019, relative à l'organisation et à la transformation du système de santé.
(26) https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fr.
(27) P. Lemoine, Rapport, *La nouvelle grammaire du succès – La transformation numérique de l'économie française*, 2014.
(28) CNOM, *Pour l'avenir de la santé – De la grande consultation aux propositions*, 2015.

malheureusement de nouvelles problématiques et risques graves de piratages, d'atteinte à la vie privée, et surtout de nouveaux dangers pour la société tout entière avec des risques forts de fractures sociales. Certaines catégories comme les personnes âgées, les résidents des déserts numériques ou encore les personnes les plus démunies, qui n'ont parfois pas d'accès à Internet ou ne savent pas l'utiliser, sont concernées par cette fracture. Très tôt, le législateur, conscient de ces risques sociétaux, a souhaité intervenir au travers de la loi n° 2001-624 du 17 juillet 2001 portant diverses dispositions d'ordre social, éducatif et culturel. Dans son article 19, celle-ci introduit plusieurs mesures visant à faciliter le développement des infrastructures de télécommunication. En effet, l'arrivée d'Internet a été une véritable révolution numérique et, depuis le milieu des années 2000, une prise de conscience des dangers des réseaux a émergé[29] et s'est imposée progressivement dans l'esprit des citoyens[30].

L'un des principaux enjeux concerne la protection des données personnelles des utilisateurs des outils numériques. En effet, pour accéder à certains services numériques et pour recevoir des informations, l'utilisateur doit donner des renseignements sur son identité, à charge pour les concepteurs de ces services de veiller au respect des droits et libertés des individus. Le droit doit donc s'y adapter en apportant une sécurité juridique concrète. Le règlement général sur la protection des données (RGPD)[31], entré en vigueur le 25 mai 2018 sur le territoire européen, vient renforcer l'article 16, § 1, du Traité sur le fonctionnement de l'Union européenne (TFUE)[32] et vise à encadrer le processus de traitement des données personnelles, à partir de leur collecte par des personnes physiques ou morales jusqu'à la fin de leur durée de conservation. Une donnée, dans la définition apportée par la Commission nationale de l'informatique et des libertés (CNIL)[33], correspond à tout type d'informations permettant d'identifier une personne physique. Elle peut être identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. La liste est vaste et le risque pour une personne de voir ses données dérobées, altérées ou supprimées, est dès lors bien réel. Il est donc indispensable de se munir d'outils informatiques afin de protéger à la fois les données personnelles et les données de santé.

Le Gouvernement français a bien mesuré l'enjeu qui se cache derrière ces données de santé, comme le montre un récent décret du 25 décembre 2020[34] portant sur la création d'un traitement de données à caractère personnel ayant pour

(29) O. Kempf, *Introduction à la Cyberstratégie*, Paris, Economica, coll. « Cyberstratégie », 2012.

(30) F. Vidalo, *Les enjeux sécuritaires de l'entreprise mondialisée : Sécurité et stratégie* 2018, p. 5 à 12.

(31) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 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).

(32) L'article 16, § 1, TFUE prévoit que toute personne a droit à la protection de ses données à caractère personnel. La Charte des droits fondamentaux de l'Union européenne, dans son article 8, § 1, y fait directement référence également.

(33) CNIL, *Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises*, 2018.

(34) D. n° 2020-1690, 25 déc. 2020, autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la Covid-19. La CNIL a en effet rendu un avis favorable à cette création de traitement le

finalité la mise en œuvre, le suivi et le pilotage des campagnes vaccinales contre la Covid-19, ou encore la stratégie « Ma santé 2022 »[35]. La France possède, en effet, l'un des environnements juridiques les plus sophistiqués en matière de protection des données, depuis la loi du 6 janvier 1978[36]. La CNIL[37] assure la mission de contrôle de ces données et contribue à l'application du RGPD, largement inspiré de la réglementation française en matière de protection numérique. La pandémie de Covid-19 a fortement mis à l'épreuve les autorités de contrôle, et notamment la CNIL qui a publié des rapports et études d'impact portant sur la protection des données personnelles et de santé pendant la phase pandémique[38]. Il en résulte la nécessité absolue, dans un monde désormais résolument tourné vers le numérique, et interdépendant de son efficience pour la protection de la santé publique, de s'assurer d'une part de son efficacité et de sa protection contre tous risques techniques ou technologiques (et notamment la destruction des *datas centers*), mais aussi de la protection des données dans des systèmes publics et privés interconnectés (*Health Data Hub*). La Plateforme des données de santé (PDS), également appelée *Health Data Hub* (HDH), a été créée par arrêté du 29 novembre 2019 pour faciliter le partage des données de santé, issues de sources très variées afin de favoriser la recherche. Sa création a ainsi pour ambition de répondre au défi de l'usage des traitements algorithmiques (dits d'« intelligence artificielle ») dans le domaine de la santé et suit les préconisations du rapport du député Cédric Villani de mars 2018 intitulé « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne ». Les missions de la Plateforme, prévues par l'article L. 1462-1 du Code de la santé publique, sont multiples, et les risques sont patents de piratage, fuites de données dans des pays tiers, sécurisations insuffisantes des plateformes. Ces risques, accrus pendant la pandémie, sont soulignés par la CNIL qui appelle à la sécurisation complète des outils numériques[39].

Il existe d'autres risques liés à la très grande utilisation du numérique, notamment la désinformation qui représente des dangers relativement graves pour les patients et plus généralement pour tous les citoyens. L'Organisation mondiale de la santé (OMS) a récemment présenté le phénomène appelé « l'infodémiologie » dans une conférence en date du 21 juillet 2020. Ce phénomène d'« infodémie » présente les risques liés à la surabondance d'informations, certaines fiables et d'autres non, observées au cours d'une épidémie. Elle rend difficile pour les personnes de trouver

10 décembre 2020, et a rappelé, à cette occasion, qu'elle exercerait son pouvoir de contrôle une fois que le traitement sera mis en œuvre.

(35) « Ma santé 2022 » est un système proposant diverses améliorations, notamment dans l'accès aux soins et l'organisation des professionnels de santé pour une meilleure coopération au service de la santé du patient.

(36) L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés.

(37) CNIL, délib. n° 2018-326, 11 oct. 2018, portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données (AIPD) prévues par le règlement général sur la protection des données (RGPD) : *JO* 6 nov. 2018, p. 81.

(38) CNIL, *Le traitement des données personnelles dans le contexte du Covid-19. Point d'étape sur les activités de la CNIL dans le contexte du Covid-19, le rôle du régulateur et les enjeux de la crise sanitaire en termes de protection des données*, rapport présenté à la séance plénière, 12 nov. 2020.

(39) A. 29 nov. 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé ». – A. 21 avr. 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de Covid-19 dans le cadre de l'état d'urgence sanitaire.

des sources d'informations et des orientations dans lesquelles avoir confiance, au moment où elles en ont besoin[40].

Pour s'en rendre compte, il suffit d'observer le cas d'Internet, qui est devenu le vecteur par lequel les citoyens s'expriment le plus librement, permettant des « échanges instantanés planétaires » et une « diffusion simple, rapide »[41] des informations sur tout type de sujet. La loi pour la confiance dans l'économie numérique prévoit cette liberté de communication au public[42], qui s'ajoute ainsi à la liberté d'expression, principe inscrit dans le bloc de constitutionnalité[43]. La loi relative à la liberté de la presse du 29 juillet 1881 définit les libertés et responsabilités de la presse française. Elle impose un cadre légal à toute publication, ainsi qu'à l'affichage public, au colportage et à la vente sur la voie publique. Toutefois, la liberté de la presse est très complexe de nos jours avec l'avènement du numérique car elle renvoie à une réglementation internationale à construire, afin de poser un cadre juridique clair. La liberté de la presse est donc une norme à développer et à harmoniser avec celles en vigueur sur le plan international.

Cependant, cette liberté de la presse ne doit pas porter atteinte aux autres droits et libertés avec lesquels elle est en lien étroit, tels que la protection du droit au respect de la vie privée et la défense de l'ordre public[44]. Il s'agit d'une problématique très complexe, car la frontière entre la libre expression et l'intrusion dans la vie privée des individus est parfois ténue.

Le risque de la liberté d'expression, utilisée d'une manière abondante, est de voir chacun au sein de la société exprimer son avis, opinion, courant de pensée, qu'il s'agisse des citoyens, mais aussi experts scientifiques, médecins, spécialistes de santé publique, économistes, journalistes. Cette expression individuelle sur sa propre vérité dans les lieux publics fait courir le risque que certains discours soient porteurs de fausses informations avec pour conséquence de tromper le public. Ceci est d'autant plus grave si ces contenus concernent la santé des malades (notamment sur leurs diagnostic et pronostic, leurs traitements, leurs effets, leurs risques et leurs bénéfices). À titre d'exemple, la pandémie de coronavirus en 2020 s'est accompagnée d'une forte vague d'informations erronées ou trompeuses, et plusieurs tentatives de certains acteurs étrangers d'influencer les citoyens et les débats de l'UE. Vera Jourova, vice-présidente chargée des valeurs et de la transparence au sein de la Commission européenne, a déclaré à ce sujet que des vagues de désinformation sont issues du territoire de l'UE, mais également de l'extérieur[45]. Elle précise que « pour lutter contre la désinformation, nous devons mobiliser tous les acteurs concernés, des plateformes en ligne aux pouvoirs publics, et soutenir les vérificateurs de faits et les médias indépendants ». Les plateformes en ligne ont pris des mesures positives au cours de la pandémie, et doivent accentuer leurs efforts, avec le risque au niveau international de confier aux GAFAM le contrôle de la circulation

(40) OMS, *Première conférence de l'OMS sur l'infodémiologie*, juill. 2020.
(41) B. Espesson-Vergeat et P. Morgon, *Le défi de la prévention vaccinale : surmonter les résistances personnelles plutôt que microbiologiques : Droit, Santé et Société* 2019, p. 47-64.
(42) L. n° 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique, art. 1, IV.
(43) DDHC 26 août 1789, art. 10 et 11.
(44) Conv. EDH, art. 10, § 2.
(45) Comm. UE, *Coronavirus : l'UE renforce son action contre la désinformation*, communiqué du 10 juin 202.

des informations. Les actions sont profondément enracinées dans les droits fondamentaux, en particulier la liberté d'expression et d'information, mais nécessitent, dans un contexte de santé publique chaotique, de prévoir une méthode agile d'encadrement juridique[46].

Face aux innovations technologiques, le droit doit constamment s'adapter pour réguler et encadrer l'évolution numérique, et cela soulève, pour les acteurs de santé, plusieurs problématiques dans le périmètre de la politique de santé (Section 1).

Cette montée en puissance du numérique entraîne de nouveaux enjeux pour les patients comme pour les professionnels de santé, à travers une protection des données qui peut paraître être à la fois une sécurité, mais également une intrusion dans certaines libertés et droits fondamentaux. Ces problématiques génèrent de nouveaux dangers, tels que le phénomène de la désinformation attaché à la complexité historique de l'humain (Section 2).

SECTION 1

## LE PÉRIMÈTRE DE LA POLITIQUE DE SANTÉ

Depuis sa découverte et son adoption massive dans notre société, le numérique a modifié et façonné notre monde, créant ainsi une véritable révolution. Il a été intégré dans le cadre de la santé, provoquant ainsi des innovations dans ce secteur. La façon de se soigner, la virtualisation et la dématérialisation des échanges affectent le quotidien des personnes. Ce faisant, le numérique en santé est un bouleversement transversal (§ 1). Il a impacté plusieurs notions et normes différentes créant ainsi des perspectives d'avancées majeures dans plusieurs domaines, tant sociologique, économique, médical, que juridique, et des interrogations dans le milieu de la santé et de l'éthique. Cette révolution en matière de santé numérique donne accès à des innovations qui propulsent les différents acteurs de santé dans une médecine « 6P » préventive, prospective, participative, personnalisée fondée sur la preuve et l'organisation du parcours de soin. Elle engendre l'apparition de nouveaux instruments dotés d'une intelligence artificielle autonome (§ 2).

### § 1. – Le numérique en santé, un bouleversement transversal

L'application du numérique évolue à plusieurs niveaux et de façon tentaculaire. À titre d'illustration, l'Institut Montaigne a publié dans son rapport d'avril 2015 que le nombre de données créées a été plus important sur la seule année de 2011 que durant toute l'histoire de l'humanité. La masse de données numériques est passée de 480 milliards de gigaoctets en 2008 à 2,72 zettaoctets en 2012. Jusqu'en 2030,

(46) B. Espesson-Vergeat (ss dir. juridique), *Rapport sur l'encadrement juridique de la désinformation*, Université de Lyon, juill. 2021.

cette masse va continuer à progresser à une vitesse exponentielle pour atteindre plus de 600 zettaoctets[47]. La Commission européenne a ainsi estimé que le volume mondial des données devrait augmenter de 530 % d'ici à 2025 (1 zettaoctet correspondant à 10 puissances 21 octets, autrement dit mille milliards de gigaoctets)[48]. Ces chiffres donnent le vertige.

Cette montée en puissance du numérique démontre un accroissement des innovations dans le domaine de la santé. L'intégration des outils numériques, de l'intelligence artificielle, des *blockchains* est déterminante notamment au niveau juridique, économique et social. Il est donc apparu nécessaire de réglementer ces interactions, d'encadrer ces nouvelles technologies, et de définir leur champ d'utilisation.

En France, le législateur a voulu réglementer les rapports entre le système de santé et les individus, en intégrant le numérique au sein des populations, communautés de patients et de professionnels de santé.

Plusieurs plans ont été élaborés pour instaurer une santé numérique en France. Une circulaire était lancée fin 1999 par la Direction de l'hospitalisation et de l'organisation des soins (DHOS) avec le plan « e-santé 2000 »[49], par les pouvoirs publics de l'époque. Cette circulaire adressée aux directeurs des agences régionales de l'hospitalisation (ARH) était un plan, doté d'une enveloppe de 20 millions d'euros, qui encourageait les hôpitaux à développer leur système d'information et des solutions de télémédecine entre eux dans le but de créer une nouvelle dynamique au sein d'un territoire de santé. Toutefois, cette circulaire était un échec ayant fait l'objet d'un rapport ministériel publié en novembre 2008.

Un second plan fut adopté et confié au député Lasbordes, informaticien, à la demande du Premier ministre de l'époque. Les propositions furent remises à la ministre de la Santé en octobre 2009[50]. Néanmoins, le déploiement de ce plan a été considérablement freiné par l'assurance maladie qui a refusé, en 2009, le financement dans le droit commun de la sécurité sociale des pratiques professionnelles de télémédecine.

Ainsi, une nouvelle approche en trois points a été proposée dans la loi du 26 janvier 2016[51] sur la modernisation de notre système de santé.

Cette loi a pour objectif le renforcement de la prévention, la réorganisation autour des soins de proximité à partir du médecin généraliste, et le développement des droits des patients. Elle instaure une amélioration du système de santé, obtenue grâce aux données numériques, afin de permettre aux usagers d'être mieux informés. En France, prenant conscience de l'importance du numérique dans l'information et la formation des acteurs de santé, la loi de modernisation du système de santé français[52] instaure les prémices d'un dossier médical partagé[53]. Par la suite, ce mouvement a été accentué par la loi pour une République numérique,

(47) Institut Montaigne, *Big data et objets connectés – Faire de la France un champion de la révolution numérique*, avr. 2015, p. 3.
(48) S. Duboc et D.-J. Noël, *Économie et gouvernance de la donnée*, avis du CESE, au nom de la section des activités économiques, 10 févr. 2021.
(49) F. Granjon, *Fracture numérique*, in *Communications* 2011/1, n° 88, p. 67 à 74. – R. Bouvet, P. Desmarais et É. Minvielle, *Legal and organizational barriers to the development of ehealth in France : Med Law* (2015) 34 : 361-380.
(50) P. Lasbordes, *La télésanté : un nouvel atout au service de notre bien-être*, 2009 (vie-publique.fr).
(51) L. n° 2016-1321, 7 oct. 2016, pour une République numérique.
(52) L. n° 2016-41, 26 janv. 2016, de modernisation de notre système de santé.
(53) Le dossier médical partagé (DMP) est un carnet de santé numérique qui conserve et sécurise les informations de santé : traitements, résultats d'examens, allergies, *etc.*

promulguée le 7 octobre 2016 et préparant la transition numérique à l'économie française[54]. Cette loi a eu pour but de promouvoir l'innovation et le développement de l'économie numérique, ainsi que la formation et la recherche avec l'ouverture de l'accès aux données publiques. Ce phénomène a été explicité à l'article 6 de la loi du 7 octobre 2016 selon lequel : « Lorsque les documents sont disponibles sous forme électronique, les administrations peuvent mettre en ligne les publications ayant un intérêt économique, social, sanitaire et environnemental ».

Dans une volonté marquée du gouvernement de s'engager pleinement et activement sur le chemin de la santé numérique, la stratégie « Ma santé 2022 »[55] est un engagement de l'État afin d'améliorer le système de santé français. Cette volonté des pouvoirs publics, consacrée par le législateur, a pour but de moderniser les pratiques des professionnels pour mieux soigner par le recours au numérique. À titre d'exemple, la santé numérique doit devenir un outil de traitement de la délicate question de la désertification médicale au sein des territoires français. En effet, la France est confrontée à un manque de médecins sur le territoire, pour des raisons multifactorielles dont l'impact de la pyramide des âges, l'organisation des études de médecine, l'organisation de l'exercice médical généraliste et spécialiste, l'urbanisation des populations, le vieillissement des populations notamment sur les territoires isolés, *etc.* Face à ces déserts médicaux, urbains ou ruraux, la stratégie du numérique consiste alors à déployer pleinement la télémédecine afin de pallier ce manque et de reconnecter les populations aux services de santé. Le numérique devrait ainsi offrir un bouquet de services facilitant l'exercice des professionnels et renforçant leur coordination par des outils sécurisés. « Ma santé 2022 » a également pour but de tirer bénéfice de l'intelligence artificielle dans le domaine de la santé, en garantissant un haut niveau de sécurité et de confidentialité des données personnelles avec l'instauration de la plateforme *Health Data Hub*[56]. Le projet de loi « Buzyn » présenté le 13 février 2019, en reprenant une partie des éléments de la stratégie « Ma santé 2022 », a définitivement été adopté le 16 juillet 2019.

La Commission européenne a pris conscience de l'importance du numérique. Cette dernière a mis en œuvre une politique de santé commune qui permet d'appréhender les rapports entre le juridique et les innovations de santé. La Commission européenne a démarré une initiative intitulée « Une Europe adaptée à l'ère du numérique », qui a pour but de faire du numérique une priorité pour la période 2019-2024. Cette stratégie repose sur des initiatives antérieures, notamment celle de « la transition numérique »[57]. La santé est au cœur de cette initiative, qui apporte des avantages significatifs dans le domaine de la santé et des sciences du vivant. Un communiqué publié en avril 2018 par la Commission européenne vise à renforcer les informations relatives sur la santé et les soins de santé[58]. Ce texte a défini trois moyens d'action pour fonder cette ère numérique.

(54) L. n° 2016-1321, 7 oct. 2016, pour une République numérique.
(55) B. Granger, « *Ma santé 2022 : un plan ambitieux, des moyens limité* », in *Le Débat* 2019, n° 203.
(56) La Plateforme des données de santé (PDS), infrastructure officiellement créée le 30 novembre 2019, est destinée à faciliter le partage des données de santé issues de sources très variées afin de favoriser la recherche.
(57) Priorités de l'UE pour 2019-2024, rubrique « À propos de l'UE ».
(58) Comm. UE, Communication « Intelligence artificielle : la Commission présente une approche européenne visant à stimuler l'investissement et à fixer des lignes directrices en matière d'éthique », 25 avr. 2018.

Le premier moyen consiste en l'accès sécurisé aux données et un partage sécurisé des informations. L'objectif étant d'élargir les soins aux pays de l'Union européenne, la Commission commence à installer un dossier patient et des ordonnances électroniques qui circuleraient parmi les médecins et professionnels de santé pour les bienfaits du patient malade *via* l'instauration d'un service en ligne. Le deuxième moyen consiste dans le partage de données de santé à des fins de recherche et de diagnostics, dans le but d'améliorer le dispositif de soins. Cette approche vise à exploiter ces données toujours en expansion à des fins de recherche médicale. Enfin, le dernier moyen consiste à rendre les citoyens européens acteurs de leur santé. Pour cela, des services numériques doivent être créés pour mieux informer la population sur les maladies et pour favoriser l'adoption d'un mode de vie plus sain. Ce plan d'action lancé par la Commission européenne reprend les stratégies adoptées par la France, notamment la stratégie « Ma santé 2022 ». La convergence des politiques de santé française et européenne montre l'intégration du numérique dans la santé.

Cette collaboration s'est renforcée avec la crise sanitaire due à la Covid-19. Il existe un engagement européen pour lutter contre le virus, et l'Union européenne joue un rôle actif et moteur dans cet effort de collaboration contre la pandémie[59], notamment par la coordination des actions visant à l'approvisionnement des produits de santé, par la coordination des actions portant sur la production et la distribution des vaccins en favorisant les accords et négociations concernant les achats de vaccins[60]. Des efforts de coopération interétatique sont réalisés dans l'optique de prendre en charge les patients issus de l'Union européenne. Cet élan de solidarité a pour but de soigner le maximum de patients au sein de l'Union européenne, mais aussi de garantir l'approvisionnement de vaccins hors Union européenne dans le cadre du programme COVAX. L'UE est déterminée à faire en sorte que des vaccins sûrs soient disponibles au niveau mondial. La Commission et les pays de l'UE se sont engagés à verser plus de 2,2 milliards d'euros à COVAX, l'initiative mondiale visant à garantir un accès équitable aux vaccins contre la Covid-19, et ils soutiennent les campagnes de vaccination dans les pays partenaires. La place de l'Union européenne dans la stratégie de santé européenne est mise en avant par la crise sanitaire, ce qui pousse à s'interroger sur l'évolution indispensable des compétences de l'Union européenne auprès des États membres et la reconnaissance de la santé comme priorité politique européenne. Cela exigerait une modification des dispositions du Traité sur le fonctionnement de l'Union européenne afin de donner compétence à la Commission en matière de santé, comme en matière de concurrence. Cette évolution n'est pas à l'ordre du jour. La politique de l'Union européenne en matière de santé passe aussi par le droit dérivé, et par l'adoption de règlements et directives sectorielles qui viennent respectivement imposer aux États membres l'application immédiate des dispositions adoptées ou le respect des objectifs fixés.

(59) Cons. UE, « Pandémie de coronavirus Covid-19 : la réaction de l'UE » ; « Covid-19 : la réaction de l'UE dans le domaine de la santé publique », 15 déc. 2020.

(60) Comm. UE, *Des vaccins sûrs contre la Covid-19 pour les Européens*, 2020 (https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans_fr).

Ainsi, l'Union européenne, au travers du règlement n° 2017/745, a mis en place une série de mesures afin de garantir la sécurité des produits issus d'entreprises produisant des dispositifs médicaux, et notamment des dispositifs contenant des outils numériques, ou étant des logiciels, en harmonisant les normes prévues dans trois directives, au sein du territoire européen. Le règlement renforce la coopération entre les États membres, et cet effort a pour but d'instaurer une harmonisation dans la conformité des dispositifs médicaux aux normes européennes, dans le respect des pratiques par les organismes notifiés en charge du contrôle et de l'octroi du marquage CE du dispositif médical, lequel constitue la carte d'identité du produit au sein de l'UE. Ce règlement a aussi pour objectif de viser le bon fonctionnement du marché intérieur des dispositifs médicaux en relevant le niveau de protection de la santé des patients et de leurs utilisateurs. L'augmentation des normes de qualité et de sécurité a un double objectif. Elle vise, en premier lieu, à l'harmonisation de ces dispositifs au sein de l'Union européenne. Ils pourront ainsi bénéficier de la libre circulation des biens et des marchandises issus du territoire européen. Le second objectif consiste en une transparence des données. Les dispositifs médicaux doivent être fiables et garantir la sécurité des utilisateurs, tout particulièrement lorsqu'ils sont numériques.

La réglementation met en place, pour les entreprises produisant ce matériel, une surveillance accrue. Celle-ci doit être effectuée tout au long du cycle de vie du produit, c'est-à-dire pendant sa conception et sa fabrication et après la commercialisation. La complexité provient du nombre très important de catégories de dispositifs médicaux (DM), et désormais de DM connectés ou dotés d'un logiciel apprenant ou non, qui aura lui-même le statut de DM. La sécurisation du dispositif et des conditions d'utilisation du DM, activé notamment par une intelligence artificielle, pose d'importantes questions juridiques sur la responsabilité du fait du produit, celle de l'auteur, concepteur du produit, du logiciel. Ces sujets sont amenés à se complexifier avec l'innovation numérique qui impactera ce secteur d'activité dans les années à venir. La question est particulièrement importante concernant les dispositifs médicaux implantables actifs (DMIA) dotés d'une intelligence artificielle. Dans le nouveau règlement « DM », la volonté est d'assurer la transparence et la traçabilité du produit afin d'apporter aux patients et utilisateurs les garanties nécessaires sur le produit. Le patient et les professionnels de santé pourront suivre cette traçabilité *via* la plateforme EUDAMED. Il s'agit de l'une des innovations du règlement n° 2017/745 avec l'intégration d'une base de données *via* un outil électronique. Cette base de données comportera l'enregistrement des produits et la publication des informations concernant les DM. Au niveau européen, il y a eu une prise de conscience de l'impact du numérique dans les produits de santé. Les outils électroniques et logiciels ont une place prééminente, et sont de plus en plus intégrés au sein même de la sphère médicale propulsant la science médicale dans une nouvelle ère de la médecine « 6P ».

Toutefois, malgré les avancées que peut apporter le numérique, les questionnements sont encore nombreux. En France, cette intégration pose divers problèmes juridiques. Le numérique, avec l'apport de l'intelligence artificielle, peut amener à la problématique de la responsabilité médicale en cas d'erreur du logiciel médical.

Se pose la question de savoir si la pratique de la télémédecine peut amener un recours en responsabilité en cas de diagnostic faux ou de non-diagnostic d'une pathologie qui n'aurait pas été vue par le biais de cette nouvelle technologie ou aurait été mal diagnostiquée au cours de la consultation numérique. Une consultation en télémédecine apporte une nouvelle approche du diagnostic et de la relation patient-médecin et fait réfléchir quant à l'efficacité de la télémédecine[61]. La question doit être appréciée au regard des différentes spécialités, et notamment de l'importance de la consultation physique indispensable à la prise de décision et au consentement du patient. Au-delà de la télémédecine, c'est l'ensemble de l'activité médicale soumise à l'utilisation et l'interprétation des outils numériques de santé dotés d'intelligence artificielle, et notamment les activités de radiologie, de biologie médicale, de gestion des blocs opératoires, mais aussi la surveillance du patient par le biais des objets connectés et applications de santé, dont le statut juridique peut entrer dans la catégorie des DM. C'est pourquoi le projet de règlement de la Commission européenne sur l'IA est très attendu pour l'année 2021.

Les exemples dans le monde entier de l'utilisation déviée ou déviante du numérique en santé sont légion. C'est pourquoi la réglementation de l'Union européenne et la réglementation française en matière de bioéthique conduisent à encadrer strictement des logiciels dont le statut pourrait porter atteinte à l'intégrité de l'être humain. La Chine en est un exemple : un médecin a récemment apporté des modifications à un fœtus, car ce dernier était pourvu de malformations[62]. En France, la question s'est aussi posée avec la loi bioéthique[63] du 15 octobre 2019. Le Comité consultatif national d'éthique est en faveur d'une ouverture aux nouvelles perspectives qu'offre le numérique à la santé[64]. Pour rappel, la loi bioéthique vise à élargir l'accès aux technologies, notamment en matière de procréation[65]. Le projet de loi assouplissait le régime de recherche des cellules souches embryonnaires, dans lequel certaines modifications apportées au génome pourront être ajoutées[66]. Cette loi a été la source d'un débat, dans la mesure où cela touchait à un embryon humain pour y apporter des modifications par l'intervention de technologies de pointe. La perspective de pouvoir modifier et toucher à la physionomie humaine n'est plus de l'ordre de la chimère, mais bien une réalité, qui fait l'objet d'un encadrement de la part du législateur.

Cette innovation du numérique dans le secteur de la santé marque également une profonde mutation dans le fonctionnement et l'évolution du fonctionnement des entreprises. En quelques années, le numérique a provoqué une importante mutation sociologique et économique et surtout juridique[67] avec un engagement

(61) D. Gruson, *Le numérique et l'intelligence artificielle en santé : Surveillance généralisée ou avancée majeure : Les Tribunes de la santé* 2019, info global santé média, p. 23.

(62) A. Labadie, *Effroi chez les scientifiques après la naissance en Chine de bébés génétiquement modifiés*, 27 nov. 2018 (www.letemps.ch).

(63) La loi bioéthique réglemente les activités médicales et de recherche qui utilisent des éléments du corps humain afin de répondre le mieux possible aux questions soulevées par le progrès scientifique et technique, au regard des valeurs de la société.

(64) D. Gruson, *Le numérique et intelligence artificielle en santé : Surveillance généralisée ou avancée majeure ? : Les Tribunes de la santé* 2019, info global santé média, p. 24.

(65) Projet de loi n° 343, relatif à la bioéthique, adopté par l'Assemblée nationale le 15 octobre 2019.

(66) Projet de loi relatif à la loi bioéthique (vie-publique.fr, 3 août 2020).

(67) L. de La Raudière, *La fabrique de la loi à l'ère du numérique : Enjeux numériques* 2018, n° 3, p. 40.

vers le tout numérique. Dans ce contexte, l'approche juridique est fondamentale dans une perspective d'utilisation des outils numériques permettant d'accélérer les opérations réglementaires. L'organisation juridique est désormais placée sous la domination des logiciels permettant d'améliorer et accélérer l'analyse juridique, d'avancer vers une justice prédictive, tout comme dans le domaine de la santé. Ainsi, les *LegalTech*(68) offrent des services juridiques innovants, entrant en concurrence avec ceux qui sont traditionnellement fournis par les professions juridiques. Ces innovations ont de multiples conséquences. Elles facilitent l'accès aux prestations juridiques dans le secteur de la santé à un coût réduit. Elles obligent ensuite les professionnels à modifier leur mode de travail, en investissant dans les nouvelles technologies, en élargissant leurs sources de financement et en se concentrant sur des services afin de s'adapter aux évolutions et mutations économiques(69). À titre d'exemple, la loi du 9 décembre 2020 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique(70) montre à quel point il est important de laisser une marge de manœuvre aux entreprises afin qu'elles puissent elles-mêmes mettre en place des actions pour limiter des pratiques anti-conformes et non éthiques. En effet, afin de garantir la réputation de l'entreprise et la sécurité des opérations, il est essentiel de respecter ces règles pour que l'entreprise soit pérenne et plus solide d'un point de vue éthique et institutionnel. L'Agence française anticorruption (AFA) a publié le 21 septembre 2020 une enquête précisant que 70 % des entreprises avaient mis en place des dispositifs de prévention. Cette enquête s'inscrit dans le plan national de lutte contre la corruption du 9 janvier 2020, et a pour principe d'aider les entreprises à mettre en œuvre des dispositifs anticorruption adaptés, notamment avec l'envoi de *guidelines*. Cette souplesse montre le succès de la loi anticorruption(71).

Bouleversant en profondeur les sources et la nature même du droit, les facteurs de cette transformation du numérique sont non seulement économiques et sociaux, mais également institutionnels, culturels, philosophiques, éthiques et politiques. Ils réunissent tous les éléments d'un véritable bouleversement de notre société(72). C'est toute la question de l'adaptation de l'innovation dans une vision du progrès de l'humanité qui est en cause. Les études dans tous les secteurs se multiplient à une vitesse phénoménale mais désordonnée sur l'impact du numérique dans la vie de la société et son avenir. La question de l'amélioration de l'humain grâce au numérique est un profond sujet qui anime tous les courants de pensée des plus innovants, utopistes, transhumanistes, aux plus conservateurs. La place du droit encadrant ce tournant dans l'évolution de la société est fondamentale(73).

(68) Les *LegalTech* représentent l'usage de la technologie pour développer, proposer ou fournir des produits ou des services relatifs au droit et à la justice, ou permettre l'accès des usagers du droit, à des professionnels ou non, à de tels produits ou services.

(69) G. Canivet, *Les facteurs de transformation du droit : Enjeux numériques* sept. 2018, p. 38.

(70) L. n° 2016-1691, 9 déc. 2016, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

(71) *Lutte contre la corruption : quelle prévention dans les entreprises ?*, vie-publique.fr, sept. 2020.

(72) J. Lucas, *Enjeux éthiques, réflexions déontologiques et recommandations du Conseil national de l'Ordre des médecins : Les Tribunes de la santé* 2019/1, n° 59, p. 85 à 97.

(73) A.-B. Caire, *L'immortalité numérique, entre fantasme et business : The Conversation* 16 janv. 2020 (https://theconversation.com/limmortalite-numerique-entre-fantasme-et-business-129384). – Rapp. AN n° 3190, *L'identité numérique*,

Les options qui seront adoptées dans l'encadrement des pratiques du numérique en santé seront déterminantes sur la préservation de l'équilibre fragile entre la protection de la santé publique et de la santé individuelle, ainsi que l'évolution scientifique et son impact économique(74).

Toutes ces problématiques sont clairement et précisément développées dans les nombreux rapports sur le numérique et la santé ou sur l'utilisation de l'intelligence artificielle dans ce secteur particulier, et plus généralement dans l'ensemble de la vie de la Cité(75).

## § 2. – Les nouveaux instruments générés dans la sphère de la santé numérique

L'émergence de nouveaux outils numériques a permis de nombreuses utilisations dans le domaine de la santé grâce au développement d'applications et d'objets connectés. Leur intégration dans le domaine de la médecine, de la formation et de la prévention, est de plus en plus présente au sein de notre société. À titre d'exemple, la montre connectée de la marque « Apple », nommée *Apple Watch*, est récemment devenue un dispositif médical surveillant les signes vitaux *via* son application(76). De ce fait, la distinction entre objets connectés en santé et ceux de la vie courante est de plus en plus difficile à établir. Toutefois, le principe pour les produits de santé, et notamment les produits connectés, est soumis à l'application de la réglementation en vigueur pour les dispositifs médicaux, comme mentionné *infra* dans le paragraphe 1.

La qualité et l'efficience du système de santé pourraient potentiellement être plus abordables pour tous avec la « m-santé »(77), mais le numérique pourrait aussi accentuer la rupture d'égalité avec les classes sociales les plus modestes, les séniors et plus largement toutes les personnes qui ont une difficulté d'accès à Internet. Son développement est très croissant, notamment au sein de l'administration publique, et cela montre l'effervescence de la société concernant les nouvelles technologies du numérique.

Le numérique intègre l'univers de la médecine en informant et en fournissant des sources d'informations viables concernant la santé et les outils en sont nombreux, à l'image de la télémédecine qui est l'un des piliers modernes du numérique en santé. Elle consiste à ce qu'un expert médical effectue sa consultation *via* l'outil numérique. Cet outil permettra potentiellement de lutter contre les déserts médicaux et

enregistré à la Présidence de l'Assemblée nationale le 8 juillet 2020 (www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information#_Toc256000142). – A. Berthe, S. Ferrari, R. Hétier, J.-P. Pierron, A. Theviot et N. Wallenhorst, *Quels fondements pour construire des politiques de l'anthropocène ? : Raisons politiques* 2020, 77.

(74) F. Becquart, *L'égal accès aux soins : mythe ou réalité ?*, Bordeaux, LEH, coll. « Mémoires numériques de la BNDS », 2011. – C. Krychowski (ss dir.), *Business models en e-santé*, Paris, Presses des Mines, coll. « Économie et gestion », 2020.

(75) CNNum, Rapport *Confiance, innovation, solidarité : pour une vision française du numérique en santé*, 2020. – PIPAME, *E-santé, Faire émerger l'offre française en répondant aux besoins présents et futurs des acteurs de santé*, 2016, 120 p.

(76) P. Renard, *Apple et le dispositif médical : une étude d'une « révolution » réglementaire*, 2018.

(77) Comm. UE, *Les pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que le téléphone portable, les systèmes de surveillance des patients, les assistants numériques personnels et autres appareils sans fil*. Cette définition est tirée du *Livre vert sur la santé mobile*, 10 avr. 2014, p. 1.

de rendre accessible la médecine à tous et partout, à la condition d'avoir un appareil numérique de type ordinateur ou smartphone. Le Code de la santé publique français définit la télémédecine à l'article L. 6316-1, comme « une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport un professionnel médical avec un ou plusieurs professionnels de santé, entre eux ou avec le patient et, le cas échéant, d'autres professionnels apportant leurs soins au patient »[(78)].

Cette pratique médicale est l'un des nouveaux visages que va prendre la médecine moderne. Son utilisation a été de plus en plus courante, le système étant plus abouti. D'une part, l'émergence de cet outil permet au patient d'être un acteur dans la reconnaissance de ses besoins et traitements. Les patients consommateurs de santé deviennent dès lors proactifs de ce système puisqu'ils s'informent, agissent et répondent à leurs besoins de santé. D'autre part, les bénéficiaires de santé disposent d'un outil qui permet un égal accès aux soins, quel que soit leur emplacement géographique ou leur aptitude physique. La télémédecine connaît un essor avec la crise de la Covid-19 qui a provoqué une distanciation physique des personnes. Dans cette période de crise, elle a été le meilleur moyen d'assurer la continuité des soins au public. La Covid-19 a permis, dans le malheur qu'elle a apporté, une véritable expansion de la culture numérique dans la réflexion médicale : « Le nombre des téléconsultations est passé de 40 000 actes facturés et remboursés par l'assurance maladie en février 2020 à 4,5 millions en avril, record absolu. Aujourd'hui, il se stabilise aux alentours de 150 000 par semaine »[(79)]. Ces consultations à distance semblent aussi rassurantes pour les médecins que pour leurs patients. Toutefois, si le numérique a envahi notre sphère médicale sans la moindre opposition, il se pose désormais les questions majeures de l'évolution du rapport de confiance entre le médecin et le patient, du consentement et de la responsabilité des professionnels de santé.

Durant la crise sanitaire, il y a eu une accentuation du phénomène de numérisation dans la santé pour permettre une continuité des soins. Toutefois, le numérique en santé est soumis aux mêmes contraintes que la médecine moderne. La question de l'étendue de la responsabilité des professionnels de santé dans le cadre des consultations en télémédecine se pose avec acuité. Les ordres professionnels, académies de médecine, experts médicaux s'interrogent sur le périmètre de la responsabilité des professionnels de santé. C'est le cas notamment pour les professionnels orthopédistes, qui doivent avoir un entretien physique avec le patient avant la décision d'intervention. À propos de la consultation préopératoire, la téléconsultation, régie par le décret 2010-1229 sur la télémédecine[(80)], pose une question majeure. En effet, la téléconsultation peut être la source d'un contentieux pour insuffisance ou erreur de diagnostic, et risque de perte de chance, défaut d'information du patient. La téléconsultation est donc possible pour les primo-consultants, mais le texte stipule « pour les patients infectés Covid-19 ou susceptibles de l'être ». Il n'est pas fait mention des autres cas. Il faut donc redoubler de prudence concernant

(78) L'article L. 6316-1 du Code de la santé publique définit la télémédecine.
(79) D. L. Étienne, *Comment le Covid-19 a « boosté » la e-santé ?*, Propos recueillis par A. Jeanblanc, lepoint.fr, 30 oct. 2020.
(80) D. n° 2010-1229, 19 oct. 2010, relatif à la télémédecine.

les primo-consultations et proposer au moindre doute une consultation présentielle au patient. Cette question de l'organisation de la relation avec le patient, de la confiance, du consentement libre et éclairé se posera désormais avec une force redoublée depuis la phase de pandémie. Concernant le recueil du consentement, les actes de télémédecine doivent être réalisés avec le consentement libre et éclairé de la personne (C. santé publ., art. R. 6316-2).

Le professionnel de santé doit recueillir le consentement du patient tant au niveau de l'acte médical de téléconsultation que sur les investigations ou traitements prescrits (C. santé publ., art. L. 1111-4). La Haute Autorité de santé (HAS), dans ses recommandations de juin 2019 sur la téléconsultation, prévoit que le consentement du patient doit être donné non seulement sur l'acte médical, mais aussi sur le recours à la consultation à distance avec les technologies de l'information et de la communication. Le professionnel de santé doit informer son patient sur les modalités pratiques de réalisation de la téléconsultation, la possibilité d'être accompagné d'une personne de son entourage, les mesures pour assurer la sécurité et la confidentialité des données de santé, le coût et le reste à charge le cas échéant. L'obligation d'information sur l'acte médical (C. santé publ., art. L. 1111-2) constitue une obligation de résultat et le médecin doit prouver par tout moyen qu'il a bien délivré l'information sur les investigations, traitements ou actes de prévention proposés, leur utilité, leurs conséquences et les risques fréquents ou graves, normalement prévisibles ainsi que les conséquences prévisibles en cas de refus et les autres solutions possibles. C'est au cas par cas que l'analyse devra être effectuée sur la faute éventuelle du professionnel de santé dans la gestion des consultations en télémédecine. Les assureurs et experts médicaux indiquent d'ailleurs une augmentation du niveau de contentieux depuis le début de la pandémie.

Au-delà de ces pratiques médicales, le numérique a développé de nouveaux outils tels que la e-santé et la santé connectée. L'application « Stop Covid », créée par l'État pour limiter la propagation du virus[(81)], en est une illustration. Toutefois, l'échec de cette application est notable, car elle n'a pas été utilisée à l'échelle escomptée. L'application a été considérée comme un empiétement sur les libertés individuelles et tout spécifiquement le respect à la vie privée. Ce constat permet de percevoir la défiance de la population française face aux mesures qui ont été instaurées. Afin de lutter contre cette défiance, et dans la mesure où l'épidémie est toujours active, une deuxième application a vu le jour par la suite : « Stop Covid » a ainsi été renommée « TousAntiCovid ».

Le numérique permet de transmettre des données de santé et l'intensité des échanges se fait plus facilement et librement, laissant place à des applications téléchargeables sur les e-boutiques. Cette libre circulation de l'information et des données de santé à destination des patients est néanmoins susceptible d'être contrôlée, afin d'apporter un maximum de véracité dans leurs contenus. C'est d'ailleurs l'un des piliers de la loi « Ma santé 2022 »[(82)].

(81) Ministère de l'Économie, des Finances et de la Relance, *L'application StopCovid est disponible au téléchargement dans les magasins d'applications*, communiqué de presse n° 2181-107, 2 juin 2020.

(82) J. Lucas, *Enjeux éthiques, réflexions déontologiques et recommandations du Conseil national de l'Ordre des médecins : Les Tribunes de la santé* 2019, n° 59, p. 92.

En France, une autre source d'innovation due au numérique est le dossier médical partagé (DMP), destiné initialement à offrir aux professionnels de santé des informations authentiques. Au sein du DMP sont inscrites les consultations, et les prescriptions dont le patient a fait l'objet. Pour les médecins, cela leur permet de se reposer sur une source d'informations fiables et valides. Il s'agit aussi d'éviter les examens redondants ou inutilement répétés. Cette option, créée en 2004, n'est donc pas novatrice, mais, tout comme la télémédecine, elle n'avait pas convaincu à cette époque[83]. Aujourd'hui, l'État a ajourné ce débat en n'imposant pas aux utilisateurs de l'assurance maladie la création d'un dossier médical partagé, mais ce projet revient en force en 2021. Le DMP demeure un outil prometteur de l'utilisation du numérique. En effet, il pourrait mettre fin à la désinformation concernant l'état de santé du patient. Ainsi, il pourrait permettre de poser un diagnostic en se basant sur des antécédents médicaux qui y auraient été déposés. Malgré cela, des doutes subsistent de la part de la population quant à son utilisation[84]. Qui du patient ou du professionnel de santé doit remplir le DMP ? Si le patient le remplit lui-même, cela ne risque-t-il pas de porter atteinte à l'authenticité du dossier ? Dans cette optique, comment s'assurer de la réelle fiabilité du dossier ? Autant de questions qu'il conviendra d'éclaircir.

Les innovations technologiques telles que l'intelligence artificielle[85], le *big data*[86] et la robotique sont désormais au cœur du système de santé. Ainsi, l'intelligence artificielle permettra à l'avenir de mieux soigner les populations notamment par l'incorporation de logiciel de santé. La qualité des soins et le suivi ne pourront qu'être améliorés.

Le numérique exige un effort de pédagogie, d'information et d'élargissement du débat public. Les citoyens doivent être mieux formés et avisés. En ce sens, la stratégie issue de « Ma santé 2022 » est basée sur la transmission de l'information de santé auprès de la population française.

Le monde numérique de la santé est désormais une réalité qui soulève une multitude de questionnements juridiques sur les usages et limites des pratiques.

SECTION 2

## LES ENJEUX DE LA RÉVOLUTION NUMÉRIQUE

De nouveaux enjeux économiques, humains, organisationnels sont apparus et démontrent que les données comportant des informations afférentes à la vie privée

(83) M. Fieschi, *Le DMP : leçons pour améliorer la gouvernance de projets de systèmes d'information nationaux*, in *I2D – Information, données & documents*, 2016/3, vol. 53.

(84) J. Lucas, *Enjeux éthiques, réflexions déontologiques et recommandations du Conseil national de l'Ordre des médecins : Les Tribunes de la santé* 2019, n° 59, p. 89.

(85) INSERM, *Intelligence artificielle et santé – des algorithmes au service de la médecine*, par J. Charlet, AP-HP et le laboratoire d'informatique médicale et ingénierie des connaissances pour la e-santé (LIMICS, unité 1142 Inserm/Sorbonne Université/Université Paris 13), Paris, 2018.

(86) Le *big data* est un gigantesque volume de données numériques produites et combinées, aux capacités sans cesse accrues de stockage et à des outils d'analyse en temps réel de plus en plus sophistiqués. Il offre aujourd'hui des possibilités inégalées d'exploitation des informations.

doivent faire l'objet d'une protection pertinente. Ceci est particulièrement vrai pour les données de santé au « cœur » de cette politique de santé (§ 1).

Le droit permet d'encadrer ces nouveaux outils ultra-connectés, mais ces derniers comportent, pour les utilisateurs, des risques indéniables, portés par le phénomène de la désinformation (§ 2).

## § 1. – La nécessité d'une protection des données de santé, une emprise sur les droits fondamentaux

En temps de crise sanitaire, il semble évident que la santé de la population est la principale préoccupation des représentants de l'État. Le Premier ministre Édouard Philippe, lors de son discours du 25 mai 2020 annonçant un « Ségur de la Santé »[87], en a fait l'un des principaux enjeux dans la rénovation du système de santé français. Face à la Covid-19, des outils ont dû être mis en place afin de permettre la protection de la santé, pas seulement d'un point de vue scientifique, mais également d'un point de vue juridique en tant que données de santé.

Depuis le 25 mai 2018, un règlement général sur la protection des données personnelles (RGPD)[88] est en vigueur au sein de l'Union européenne et permet d'apporter une sécurité juridique renforcée des données de santé. Ce nouveau texte européen s'apparente à une mise à jour de la loi Informatique et Libertés du 6 janvier 1978[89], pur produit français, qui est toujours en application dans le territoire aujourd'hui.

L'un des principaux fondements du RGPD est la transparence vis-à-vis des personnes concernées[90]. En effet, le médecin a l'obligation d'informer le patient sur les examens, soins ou traitements proposés. En plus d'une obligation réglementaire, il s'agit également d'une obligation déontologique[91]. Le défaut d'informations et le non-recueil du consentement sont régulièrement sanctionnés par les juridictions de droit commun et du droit disciplinaire. L'information du patient est donc le point de départ du processus et le préalable à son consentement ou à son opposition aux soins. Le RGPD en fait l'un de ses enjeux principaux, si ce n'est le plus important. Toute personne doit consentir par un acte positif, clair par lequel elle manifeste de façon « libre, spécifique, éclairée et univoque » son accord au traitement[92]. Il en va de même pour des données qui sont hébergées dans des bases informatisées. Les diverses applications de télémédecine, de télésurveillance ou encore l'assistance par des dispositifs médicaux intelligents sont également concernées par le recueil du consentement[93]. En somme, une donnée concernant la santé est caractérisée par la santé physique ou mentale d'une personne physique, y compris les prestations

(87) Discours du Premier ministre M. Édouard Philippe, Lancement du « Ségur de la Santé », 25 mai 2020.
(88) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016.
(89) L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés.
(90) RGPD, consid. 39 et art. 5.
(91) C. déont. méd., art. 35 et C. santé publ., art. R. 4127-35.
(92) RGPD, art. 4, pt 11.
(93) J. Lucas, *Enjeux éthiques, réflexions déontologiques et recommandations du Conseil national de l'Ordre des médecins : Les Tribunes de la santé* 2019, p. 85-97.

de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne[94].

Le groupe de travail « Article 29 »[95] précise que ces données de santé sont dites « sensibles ». Elles font partie des catégories particulières de données à caractère personnel visées à l'article 9. Les dispositions du règlement doivent être d'application stricte en ce qui les concerne, notamment lorsque leurs contenus sont partagés entre différents services et qu'ils sont étudiés par plusieurs personnes. C'est le cas pour les dossiers médicaux que peut conserver un hôpital général ou encore les informations sur des auteurs d'infractions que peut détenir un enquêteur privé. Une politique de sécurité informatique suffisamment fortifiée s'impose alors, et celle-ci est impérative dans le cadre des dispositifs médicaux, tels que les *pacemakers*, dispositifs médicaux à pression positive continue, pompes à insuline, *etc.* À défaut, les données de santé « sensibles » des patients risquent d'être rendues accessibles à des tiers. L'un des scénarios les plus catastrophiques serait de voir les dispositifs médicaux faire l'objet d'attaques informatiques visant à prendre leur contrôle à distance, pouvant potentiellement causer la mort des patients concernés.

Au-delà des dispositions du RGPD, certaines catégories de données peuvent augmenter le risque possible pour les droits et libertés des personnes, dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental, comme des données de localisation dont la collecte mettrait en cause la liberté de circulation. Il en va de même pour des données financières dont la violation aurait des incidences graves dans la vie quotidienne de la personne concernée, telle qu'un piratage à des fins de paiements frauduleux.

La menace de cette cybercriminalité va s'accentuer dans les années à venir par la numérisation croissante de l'économie et de la société qui constitue des opportunités pour les cybercriminels, comme l'a démontré la crise sanitaire de la Covid-19[96]. L'enjeu des réseaux informatiques sera d'autant plus stratégique avec l'arrivée de la 5G. L'Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité nationale compétente en matière de cybercriminalité, joue un rôle de détection et d'alerte quand une cyberattaque se produit. Ceci dit, la cybercriminalité étant de plus en plus sophistiquée et organisée, l'agence éprouve de réelles difficultés à recruter des agents ayant des compétences aussi pointues[97].

Cette forme de délinquance n'a pas de frontières et, afin de faire face à ce phénomène transnational, l'Union européenne s'est dotée d'un « dispositif d'ensemble pour lutter contre la cyberdélinquance », applicable par les États membres, qui mobilisent l'action de différentes agences telles qu'Europol, Eurojust et l'*European Union Agency for Cybersecurity* (ENISA). Les principales recommandations du rapport d'information sur la lutte contre la cybercriminalité du 9 juillet 2020 portent

(94) RGPD, art. 4, pt 15.

(95) Groupe de travail « art. 29 », 17/FR WP248 rév.01, « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement UE 2016/679 », adoptées le 4 avril 2017, p. 11.

(96) O. Cadic et R. Mazuir, Rapp. Sénat n° 502 (2019-2020) sur le suivi de la cybermenace pendant la crise sanitaire, au nom de la commission des affaires étrangères, de la défense et des forces armées, 10 juin 2020.

(97) S. Joissains et J. Bigot, Rapp. Sénat n° 613 (2019-2020) sur la lutte contre la cybercriminalité, fait au nom de la commission des affaires européennes et de la commission des lois, 9 juill. 2020.

sur la modernisation et le renforcement des moyens des services enquêteurs spécialisés dans la lutte contre la cybercriminalité et de la section du parquet de Paris spécialisée dans ce domaine, et l'élaboration dans les meilleurs délais d'un cadre réglementaire européen relatif à la preuve numérique compatible avec les dispositions concernant la protection des données personnelles tout en renforçant la coopération européenne.

Ainsi le risque de voir un établissement de santé se faire pirater est réel, et cela vient parfois de la « faille humaine » par laquelle les professionnels de santé, par négligence, ne respectent pas certaines procédures de sécurité. Une enquête a d'ailleurs permis de révéler que des centaines de données médicales confidentielles parmi lesquelles des prescriptions, des résultats d'analyses biologiques, voire des dossiers médicaux complets, se sont retrouvées facilement accessibles sur Google, à partir du nom du médecin ou du patient(98). Le Conseil national de l'Ordre des médecins soutient que tous les accès aux bases informatiques doivent faire l'objet d'un contrôle informatique par une politique d'habilitation des différents professionnels, d'un chiffrement de données rendant impossible la lecture par un tiers ne possédant pas la clé de déchiffrement, et d'une protection contre les attaques informatiques grâce notamment à l'antivirus(99). Cette assertion s'applique particulièrement au dossier médical partagé. En somme, tout accès non autorisé ou non justifié entraîne des sanctions pénales et disciplinaires.

De nouveaux appareils qui détectent certaines maladies ou symptômes sont très efficaces et sécurisants pour le patient. Leur suivi grâce au numérique et au pilotage par les données représente un enjeu essentiel pour assurer leur efficacité. À titre d'exemple, 42 % des patients diabétiques ont déjà téléchargé une application mobile de santé et plus de la moitié les considèrent comme incontournables pour gérer leur pathologie(100). Néanmoins, il ne faudrait pas pour autant négliger leur intrusion dans la vie privée. Certains dispositifs médicaux recueillent des informations sur l'état de santé du patient en temps réel, comme la montre connectée dotée d'un cardiofréquencemètre(101), d'une balance connectée, d'un micro, et de différents capteurs et applications permettant de suivre la consommation alimentaire de l'utilisateur et les activités physiques(102). Mais certains peuvent également déterminer l'état émotionnel de l'utilisateur qui servira aux médecins pour le suivi des traitements. De ce constat, il semble alors opportun de se demander où se situe la place de la sphère privée et des libertés individuelles si des appareils détectent les sentiments des individus pour contrôler et vérifier leur bonne santé et leurs besoins.

Il en va de même pour l'intelligence artificielle (IA), ces programmes informatiques capables d'imiter les fonctionnalités cognitives humaines, comme l'apprentissage et la résolution des problèmes(103). Ethik-IA, initiative citoyenne et académique

(98) G. Bonnaud, *Des données personnelles médicales sur Google : danger réel du numérique en santé ? : Hegel* 2013, p. 161-162.
(99) CNOM et CNIL, *Guide pratique sur la protection des données personnelles*, 2018.
(100) C. Chambard, *Comment accélérer le déploiement de l'e-santé en France ? : Les Tribunes de la santé* 2019, p. 51-61.
(101) Le cardiofréquencemètre permet de suivre le rythme cardiaque de l'utilisateur.
(102) X. Briffault et M. Morgiève, *Anticiper les usages et les conséquences des technologies connectées en santé mentale. Une étude de « cas fictif » : Droit, santé et société* 2017, p. 32-46.
(103) K. Gratzer, H. Servy et L. Chiche, *Des guidelines pour l'Intelligence artificielle ! : La Revue de médecine interne* mars 2020, vol. 41, Issue 3, p. 189-191.

française[104], a proposé au mois de février 2018 des principes de régulation de l'IA et de la robotisation en santé, dans le cadre de la révision des lois bioéthiques[105]. Parmi ces clés de régulation, l'information et le consentement du patient restent prioritaires, sur la base de l'article L. 1111-4 du Code de la santé publique qui dispose que « tout patient prend, avec le professionnel de santé (…) les décisions concernant sa santé ». Il doit être informé de manière claire et compréhensible du recours à un dispositif d'IA dans le processus de sa prise en charge. L'utilisation d'un tel dispositif suppose une évaluation sous l'angle bénéfice/risque qui servira au médecin et au patient dans la prise de décision. Ce rapport s'applique aux technologies de santé (médicaments, dispositifs médicaux, actes professionnels)[106] afin de valider de manière indépendante si un dispositif comporte suffisamment de sécurité et d'intérêt au regard des risques inhérents à son utilisation. À titre d'exemple, l'angle bénéfice/risque d'un logiciel associé à un scanner ou à un appareil d'IRM pour améliorer l'analyse d'images est effectué par l'intermédiaire d'une évaluation de l'acte professionnel d'imagerie correspondant.

Le patient étant par nature malade et fragile, le médecin est le seul à pouvoir alléger ses souffrances et le guérir. Qu'en est-il en l'absence de consentement du malade ? Si l'état du patient nécessite des soins urgents et appropriés, le médecin est autorisé à agir sans le consentement du malade et sans qu'il ait été informé. Il a, en effet, une obligation légale d'intervenir sous peine de sanctions pénales pour non-assistance à personne en danger[107]. Par ailleurs, la loi Kouchner du 4 mars 2002 prévoit que si le patient est dans l'incapacité d'exprimer sa volonté, une personne de confiance, ou de la famille, peut intervenir pour prendre les décisions à sa place. Ainsi, quels que soient les outils numériques mobilisés, le professionnel de santé doit rester maître de la décision finale[108]. L'article R. 4127-5 du Code de la santé publique appuie cette « indépendance professionnelle », ce qui suppose qu'il n'est pas tenu de suivre le diagnostic et les résultats issus d'un système intelligent et qu'il doit continuer à assumer ses décisions médicales[109]. De plus, étant donné qu'il s'engage personnellement à assurer les soins, la décision médicale finale lui incombe[110]. Cependant, l'évolution vers une utilisation de l'IA forte de plus en plus prégnante dans les outils numériques peut conduire à une prise de décision médicale dictée par l'IA, ce qui pose clairement la question de la responsabilité du médecin, sujet qui devrait être traité au sein du très attendu règlement sur l'intelligence artificielle.

(104) Ethik-IA, regroupant des enseignants, de chercheurs en droit numérique, en technologie de l'information et de la communication (TIC), et en sciences humaines et sociales, a pour but de « proposer une série d'outils et de notes de cadrage pour garantir un regard humain sur les algorithmes en santé ». Cette initiative académique et citoyenne présentée par David Gruson, ex-délégué général de la Fédération hospitalière de France (FHF) et membre du comité de direction de la chaire santé de Sciences Po Paris, entend défendre une « régulation positive » de l'intelligence artificielle et de la robotisation en santé, notamment dans le cadre des états généraux de la bioéthique.

(105) D. Gruson, *Le numérique et l'Intelligence artificielle en santé : surveillance généralisée ou avancée majeure ? : Les Tribunes de la santé* 2019, p. 23-29.

(106) Sénat, Proposition de résolution européenne sur l'évaluation des technologies de la santé, 2018.

(107) C. pén., art. 223-6.

(108) L. Morlet-Haïdara, *L'utilisation de l'intelligence artificielle en santé : contexte et focus sur l'engagement des responsabilités*, *op. cit.*, p. 102.

(109) CE, *Révision de la loi bioéthique : quelles options pour demain ?*, 2018, p. 207.

(110) L'article R. 4127-69 du CSP dispose que : « l'exercice de la médecine est personnel ».

Par ailleurs, l'accélération de l'utilisation des systèmes intelligents fait craindre au patient de ne pouvoir participer aux décisions et choix le concernant. Afin d'éviter ce risque, l'article 11 du projet de loi bioéthique, voté en première lecture par l'Assemblée nationale(111), prévoit que : « Lorsque, pour des actes à visée préventive, diagnostique ou thérapeutique, est utilisé un traitement algorithmique de données massives, le professionnel de santé qui communique les résultats de ces actes informe la personne de cette utilisation et des modalités d'action de ce traitement ». Il s'agit donc d'une obligation d'information *a posteriori* incombant au médecin. Étant donné que le professionnel de santé est tenu d'élaborer son diagnostic en s'aidant des méthodes scientifiques les mieux adaptées, au regard de l'article R. 4127-33 du Code de la santé publique, et qu'il y a une absence de risque lié à l'utilisation des systèmes intelligents(112), il doit utiliser les dispositifs IA dans la mesure du possible, dès lors qu'ils permettent d'apporter les meilleurs soins. Cela pourrait conduire à considérer que le médecin est dispensé d'obtenir le consentement préalable de son patient. Fort heureusement, la commission spéciale chargée d'examiner le projet de loi tel que voté par l'Assemblée nationale a proposé de subordonner le recours à un traitement algorithmique à une information préalable du patient par le professionnel de santé(113). Le Sénat a alors éclairci cette rédaction et a consacré le principe d'une information *a priori* du patient dans sa prise en charge par l'intermédiaire d'un système algorithmique. Il conviendrait de renforcer la notion de consentement, en précisant, du fait de l'asymétrie d'information entre le patient et le professionnel, les critères à rechercher dans la manifestation du consentement. En effet, une réponse positive ou négative est-elle toujours clairement décidée ; peut-elle être remise en cause par le patient ? Les manifestations du consentement éclairé sont encore plus complexes dans l'hypothèse du recours au numérique dans la relation de soins, ce qui impose en droit de la santé de repenser pour l'avenir le contenu de la notion de consentement du patient, en l'adaptant en fonction de la complexité des usages numériques dans une approche agile du droit.

En ce qui concerne la responsabilité du médecin, celle-ci se trouve-t-elle engagée s'il ne suit pas les prévisions du système intelligent ? En l'état actuel du droit positif, le professionnel de santé ne saurait voir sa responsabilité engagée au seul motif qu'il n'a pas suivi les résultats indiqués par l'intelligence artificielle, sur le fondement de l'article L. 1142-1 du Code de la santé publique. S'il s'engage personnellement à prodiguer les soins, il devra répondre de ses choix et de ses éventuelles fautes. Dans l'hypothèse où il suivrait aveuglément une décision d'IA qui a commis une erreur, la responsabilité du praticien sera engagée pour faute, car un médecin normalement diligent aurait écarté cette recommandation(114).

(111) Projet de loi n° 238 relatif à la bioéthique, adopté par l'Assemblée nationale, session ordinaire, enregistré à la Présidence du Sénat le 8 janvier 2020.

(112) Rapport fait au nom de la commission spéciale chargée d'examiner le projet de loi relatif à la bioéthique, t. II, 2019, p. 483.

(113) Rapp. AN n° 237 fait au nom de la commission spéciale sur le projet de loi relatif à la bioéthique, adopté par l'Assemblée nationale, 2020, p. 152.

(114) C. Lequillerier, *L'impact de l'IA sur la relation de soin : Journal du Droit de la Santé et de l'Assurance Maladie (JDSAM)* 2020, p. 84-91.

Au-delà des résultats issus d'une intelligence artificielle que le médecin suivrait, quelle est la signification pour l'homme de ces résultats, qui ne proviennent finalement pas du professionnel de santé ?

Cela pose la question de savoir si le robot intelligent dispose d'une personnalité morale, et donc d'être tenu responsable à l'instar d'une personne morale, mais aussi dispose de droits notamment lorsqu'il est la source d'une découverte ou d'une création nouvelle. Selon l'article 60 de la Convention sur le brevet européen (CBE), le droit au brevet appartient à l'inventeur ou à son ayant droit. Le processus créatif entraînant la brevetabilité n'appartiendrait donc plus à l'humain, mais à son inventeur, qui se présente comme une notion beaucoup plus large. Pour l'instant, l'IA s'est vu refuser la qualité d'inventeur par une première décision de l'Office européen des brevets (OEB)[(115)]. Si un inventeur, personne physique, met en place une IA qui d'elle-même crée un dommage à une personne physique ou morale, la question de l'attribution de la responsabilité se pose. Doit-on sanctionner l'IA qui, par son propre fait, a créé le dommage, ou bien l'inventeur personne physique qui a contribué indirectement à la création du dommage ? Faut-il donc prévoir un nouveau régime de responsabilité spécifique ? Ces questions soulèvent de véritables difficultés conceptuelles.

Le groupe européen d'éthique des sciences et des nouvelles technologies tente d'y apporter des réponses[(116)]. D'un point de vue scientifique, une intelligence artificielle a la faculté de prendre des décisions par elle-même, d'apprendre de manière continue, et est ainsi considérée comme étant « autonome ». À l'inverse, le groupe part d'un point de vue éthique et philosophique où l'autonomie est la capacité de l'homme à penser, à légiférer par et pour lui-même. De ce postulat, il ne serait pas possible d'accorder à un système intelligent un statut moral et une dignité de la personne humaine. Étant un fondement des droits de l'homme, le groupe explique que « la dignité humaine implique qu'une intervention et une participation humaines significatives doivent être possibles pour ce qui concerne les hommes et leur environnement ». Ainsi, une gestion des êtres humains par des entités « autonomes » serait contraire à l'éthique et porterait atteinte aux valeurs et à la Charte des droits fondamentaux de l'Union européenne. Le Conseil de l'Europe a déjà publié plusieurs lignes directrices et recommandations sur les responsabilités des États membres et des acteurs privés à l'égard des applications d'IA et des *big data*, ou « mégadonnées »[(117)].

(115) Les motifs de la décision de l'OEB relative à la demande EP 18 275 174 ont été publiés le 27 janvier 2020.

(116) Groupe européen d'éthique, des sciences et des nouvelles technologies, *L'intelligence artificielle, la robotique et les systèmes « autonomes »*, 2018, p. 10-11.

(117) Lignes directrices (Convention 108) sur l'intelligence artificielle et la protection des données, 2019, T-PD(2019)01 (Lignes directrices IA Convention 108) ; Lignes directrices (Convention 108) sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, 2017, T-PD(2017)01 (Lignes directrices Mégadonnées Convention 108) ; Recommandation du Comité des Ministres aux États membres sur les mégadonnées au service de la culture, du savoir et de la démocratie, 2017, CM/Rec(2017)8 (Recommandation sur les mégadonnées au service de la culture). Déclaration du Comité des Ministres sur les capacités de manipulation des processus algorithmiques, 2019, Decl(13/02/2019)1 (Déclaration sur les capacités de manipulation) ; Projet de recommandation du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme, 2018, MSI-AUT(2018)06 (Projet de recommandation sur les systèmes algorithmiques).

Jusqu'où le droit à la liberté d'expression protège-t-il l'« expression » d'applications d'IA entièrement autonomes ? Les gouvernements pourraient tenter de censurer les contenus indésirables produits par des applications d'IA, comme les *deep fakes* et autres types de contenus audiovisuels falsifiés pouvant être générés de façon automatique. Le débat sur la personnalité juridique et la responsabilité des systèmes automatiques est en cours, et n'a pas encore été tranché[118]. La Cour européenne des droits de l'homme estime que ces devoirs et responsabilités pèsent non seulement sur les journalistes, mais aussi sur d'autres acteurs contribuant au débat public, dont les propriétaires ou éditeurs de médias[119] et les portails d'actualité en ligne[120].

À cet égard, les acteurs du numérique sont aujourd'hui en quête, au-delà d'un régime réglementé, de nouvelles normes, de nouveaux principes à vocation éthique qui reposeraient sur l'autorégulation, l'implication et la responsabilisation de ces acteurs. Ils souhaitent que ces objectifs soient portés par des valeurs intangibles et universelles afin de créer un sentiment collectif de confiance et de responsabilité à tous les niveaux de la chaîne médicale[121]. Cependant, face à l'évolution de la science et des techniques qui deviennent de plus en plus complexes, les médecins ne doivent pas perdre de vue qu'ils soignent une personne malade et qu'ils ne combattent pas seulement la maladie dont un individu serait atteint. C'est en tout cas ce que rappelle le Conseil national de l'Ordre des médecins en leur demandant de dépasser la simple formation aux usages techniques : « La formation aux humanités, à la déontologie et à l'éthique, aux relations humaines doit être renforcée dans un monde qui se technicise de plus en plus. (...) »[122]. Des signes montrent cette évolution, comme le patient qui devient de plus en plus actif dans la prise en charge de ses soins. Ces mutations ne sont pas tellement d'ordre scientifique et médical, mais plutôt d'ordre sociologique, économique et politique. La situation d'une violation des données personnelles hébergées dans un pays hors UE en est un exemple.

Dans cette hypothèse, il faut se référer à la législation de l'État concerné par une atteinte aux données personnelles, ce qui n'est pas une chose aisée, d'autant plus que certains États n'ont pas une législation aussi protectrice que celle des États-Unis ou celles que l'on peut trouver en Europe. En effet, la judiciarisation des affaires pour des attaques provenant de pays étrangers est très complexe et longue, et n'aboutit généralement que très rarement[123]. Cependant, en matière de données de santé, les patients tout comme les professionnels de santé doivent recevoir la garantie que l'hébergement de leurs données comportera les mêmes exigences de sécurité et de disponibilité qu'en France s'il se réalise en dehors du territoire national[124].

(118) Comité d'experts sur les intermédiaires Internet, 2017, p. 25.
(119) *Sürek* c/ *Turquie* (n° 1), 1999, § 63 ; *Sürek* c/ *Turquie* (n° 3), 1999, § 41 ; *Öztürk* c/ *Turquie*, 1999, § 49 ; *Chauvy et a.*, 2004, § 79 ; *éd. Plon*, 2004, § 50.
(120) *Magyar Tartalomszolgáltatók Egyesülete et Index.hu Zrt* c/ *Hongrie*, 2016, § 62 ; bien que les responsabilités juridiques des « médias imprimés et audiovisuels classiques, d'une part », et « des médias sur Internet, d'autre part » puissent différer, en raison des différences fondamentales entre un exploitant de portail et un éditeur traditionnel. V. *Delfi AS* c/ *Estonie [GC]*, 2015, § 113.
(121) G. Canivet, *Les facteurs de transformation du droit : Enjeux numériques* 2018, n° 3.
(122) CNOM, *Médecins et patients dans le monde des data, des algorithmes et de l'intelligence artificielle*, 2018.
(123) F. Vidalo, *Les enjeux sécuritaires de l'entreprise mondialisée : Sécurité et stratégie* 2018, p. 5-12.
(124) CNOM et CNIL, *Guide pratique sur la protection des données personnelles*, éd. juin 2018.

Le secrétaire d'État chargé de la transition numérique et des communications électroniques, Cédric O, lors de l'ouverture du colloque « Données de santé et intelligence collective »[125], déclarait : « Il y a peu de secteurs en France qui sont aussi importants que la santé et le numérique. (…) Nous avons deux acteurs dominants dans le monde, qui sont les États-Unis et la Chine. (…) Ces deux acteurs, à la fois en termes d'investissements, en termes de maîtrise de la technologie, imposent leurs normes, imposent leur éthique. (…) C'est un problème économique, on le sent bien, mais c'est un problème également de souveraineté et d'indépendance (…) ».

Un autre risque lié aux données concerne l'ouverture des données aux bases publiques en santé. En effet, il existe un débat autour des relations entre ces données collectées dans les bases du *big data* et celles qui sont collectées dans les bases publiques. Le *big data* concerne le stockage et l'exploitation rapide de grandes quantités de données brutes souvent complexes, provenant de sources différentes (données cliniques, biologiques, sociales et environnementales)[126]. L'Ordre des médecins souhaite à ce sujet que ces débats soient publics et estime que leur accès doit être élargi avec une vision positive de leur traitement, sous l'angle bénéfice/risque pour le système de santé français et la recherche. Cela suppose une grande transparence auprès des citoyens et de savoir jusqu'où ils veulent protéger leurs données de santé et s'ils souhaitent les partager, notamment dans le cadre de la recherche. Nonobstant l'intérêt public majeur que cela représente, l'Ordre rappelle toutefois que la préservation du secret médical est primordiale et que l'exploitation des données personnelles de santé ne doit pas permettre l'identification d'une personne.

Cependant, l'attitude des citoyens vis-à-vis de cette collecte de données est assez déconcertante[127]. Dans la mesure où ils se soucient légitimement de l'usage qui serait opéré sur leurs propres données personnelles de santé au sein des bases publiques, ils semblent en revanche en contradiction avec l'usage qu'ils en font eux-mêmes dans les diverses applications en santé. Ils ne se soucient guère en effet de permettre à des gens, notamment sur les forums et les réseaux sociaux, de connaître leurs préoccupations, leur état de santé lorsque ce sont eux-mêmes qui les divulguent, croyant peut-être qu'il n'y aurait pas de risque porté à leur identité numérique, surtout sous pseudonyme. Mais il ne s'agit que d'un exemple parmi tant d'autres qui démontre la contradiction de l'essence humaine.

Les citoyens ont trouvé une manière d'extérioriser leurs émotions sans que cela n'ait de véritables conséquences sur leur train de vie. La plupart le font probablement pour combler un vide, à l'image d'une psychothérapie, et également d'une certaine façon, pour montrer qu'ils existent au milieu de toute cette foule numérique qui abonde aujourd'hui les réseaux[128]. Selon Laurent Saenko, « le plus curieux (et le plus dangereux) est sans doute que ces nouvelles sociétés virtuelles

(125) Ministère des Solidarités et de la Santé, Colloque « Données de Santé et Intelligence Collective », 18 nov. 2019.
(126) K. Gratzer, H. Servy et L. Chiche, *Des guidelines pour l'Intelligence artificielle ! : La Revue de médecine interne* mars 2020, vol. 41, Issue 3, p. 189-191.
(127) J. Lucas, *Enjeux éthiques, réflexions déontologiques et recommandations du Conseil national de l'Ordre des médecins : Les Tribunes de la santé* 2019, p. 85-97.
(128) J.-L. Manise, *Refuser d'être une fourmi numérique : La Revue Nouvelle* 2016, p. 58-61 : « Environ 1,71 milliard de personnes se muent en "fourmis numériques" ».

fonctionnent avec leurs propres codes, leurs propres règles : il faut y jouer un rôle actif pour ne pas être oublié ; il faut montrer qu'on aime pour pouvoir être aimé en retour..., *etc.* »[129]. Par ce comportement, ils prennent le risque de dévoiler directement ou indirectement des informations capitales sur leur train de vie et de faire naître ainsi des discriminations. De telles informations pourraient également se retourner contre eux si une personne malveillante souhaite les exploiter pour son propre compte. Se pose une nouvelle fois la question de la vie privée et des libertés individuelles. De plus, avec toutes les données qui circulent, les compagnies d'assurance seraient tentées de taxer davantage ceux qui auraient une moins bonne hygiène de vie.

Cette utilisation accrue des réseaux sociaux, et plus globalement d'Internet, amène une méfiance envers les informations qui y circulent, y compris celles issues de sources sûres, et certains comportements malveillants, par l'intermédiaire des *fake news* notamment, entraînent des situations nocives pour les utilisateurs.

## § 2. – Les risques de ces nouveaux enjeux par la manipulation de l'information

Le numérique est une arme à double tranchant. Elle permet, d'une part, de favoriser la diffusion des fausses informations, informations déformées, appelées notamment *fake news*[130] et, d'autre part, de réguler les comportements des utilisateurs devant leur écran. Face à leur montée en puissance exponentielle, la Commission européenne a annoncé le 26 septembre 2018[131] que les représentants des plateformes en ligne, des principaux réseaux sociaux, des annonceurs et de l'industrie de la publicité, se sont mis d'accord sur un code de pratique autoréglementé pour faire face à la propagation de la désinformation en ligne et des fausses informations. Il regroupe les géants du numérique, les GAFAM (Google, Apple, Facebook, Amazon et Microsoft), ainsi que Mozilla et TikTok. Ce code fixe plusieurs engagements allant de la transparence de la politique publicitaire à la fermeture de faux comptes et à la démonétisation des fournisseurs de fausses informations. Ces engagements conventionnels avec la Commission européenne et les États membres permettent de trouver une première arme contre le développement de l'« infodémie » telle que mentionnée par l'OMS, mais traduisent aussi la faiblesse des États membres dans leur capacité à traiter cette question. Cela pose la question de savoir quels sont les moyens à mettre en œuvre afin d'établir une réglementation ou régulation de l'information permettant d'établir une lutte efficace contre les fausses informations. Cette situation pourrait conduire à la reconnaissance de la responsabilité des auteurs de fausses informations sur les fondements du droit pénal

(129) L. Saenko, *Nouvelles technologies et liberté d'expression : le droit pénal (perdu) entre adaptation et innovation : Arch. pol. crim.* 2018/1.

(130) P. Troude-Chastenet, Fake news *et post-vérité. De l'extension de la propagande au Royaume-Uni, aux États-Unis et en France : Quaderni* 2018, 96 [en ligne].

(131) Comm. UE, Statement/18/5914, *« Déclaration de la Commissaire Gabriel sur le Code de pratique contre la désinformation en ligne »*, Bruxelles, 26 sept. 2018.

et civil, permettant d'assurer la protection de la liberté de la presse et de la liberté d'expression, dans le respect des libertés fondamentales de chacun. Le Conseil de l'Europe s'interroge sur cette question épineuse[132]. Cela pose aussi la question de savoir comment réguler au niveau international la circulation d'informations qui se déploient de manière instantanée à travers la planète. La question est donc de savoir comment sanctionner *a posteriori* l'auteur d'une fausse information sciemment diffusée, ou de son complice. Par ailleurs, une autorité indépendante nouvelle en charge du contrôle de l'information numérique pourrait être envisagée.

Tout au long de la crise de la Covid-19, la Commission européenne a mis en garde les citoyens sur la propagation du phénomène de la désinformation qui pourrait nuire à leur santé. En effet, les théories les plus folles et absurdes circulent et proviennent même de sources officielles ou des pouvoirs publics. Au niveau mondial, les propos relayant les théories du complot font florès. Les sites de contrôle de l'information journalistique, les GAFAM alertent quotidiennement sur ces *fake news* dangereuses. À titre d'exemple, le centre d'anti-poisons belge a relevé une augmentation de 15 % du nombre d'accidents liés à l'ingestion d'eau de Javel, suite à de fausses allégations portant sur la guérison du coronavirus grâce à ce produit ou même l'alcool[133].

M. Joseph Borelle, haut représentant et vice-président de la Commission européenne, a déclaré qu'« en ces temps de coronavirus, la désinformation peut tuer. Nous avons le devoir de protéger nos citoyens en les sensibilisant à l'existence de fausses informations et de pointer du doigt les acteurs responsables de telles pratiques. Dans le monde actuel, fondé sur la technologie, où les guerriers manient le clavier plutôt que l'épée et où les opérations d'influence ciblées et les campagnes de désinformation sont une arme reconnue utilisée par des acteurs étatiques et non étatiques, l'Union européenne augmente ses activités et ses capacités pour lutter contre ces pratiques »[134]. Les études pullulent sur la question des *fake news*. Cette contagiosité est un sujet majeur et complexe[135] abondamment étudié en sociologie, mais les analyses juridiques sont quasi inexistantes. Une étude portant sur la régulation juridique des *fake news* dans la phase pandémique et post-pandémique porte sur l'analyse de ce phénomène et sur les outils juridiques existants et à imaginer afin, d'une part, d'encadrer et de sanctionner les comportements à l'origine de cette propagation et, d'autre part, d'envisager les mesures permettant de prévenir en formant et en informant la population. Cette étude s'engage vers la nécessité d'une autorité indépendante, au niveau européen à tout le moins, renforçant le lien de confiance que les autorités nationales, européennes et internationales, tant au plan scientifique, que médical, ou numérique, ne parviennent plus à assurer.

(132) *Covid et la liberté d'expression. L'impact de la Covid-19 et des mesures qui en découlent sur la liberté d'expression dans les États membres du Conseil de l'Europe*, nov. 2020.

(133) Comm. UE, *Lutter contre la désinformation concernant la Covid-19*, communication, 10 juin 2020.

(134) Comm. UE, *Coronavirus : l'UE renforce son action contre la désinformation*, communication, 10 juin 2020.

(135) E. Jaubert et C. Dolbeau-Bandin, *Infox et Coronavirus Covid-19 : une relative contagiosité ?*, hal.archives-ouvertes.fr, 2020. – M. Tristan, « *Infodémie » autour du coronavirus*, entretien, vol. 2020, 2020. – G. Gamhewage, *A moving target in the fight against infectious hazards and epidemics/Une cible mouvante dans la lutte contre les risques infectieux et les épidémies*, in *Weekly Epidemiological Record* 2016, vol. 91, n° 7, p. 82 (consulté le 6 mars 2021).

Des chercheurs de l'Université d'État de Caroline du Nord située à Raleigh aux États-Unis ont mené une étude sur le « succès » de cette florissante circulation des fausses nouvelles parmi les internautes[136]. Les scientifiques ont interrogé 1 793 personnes d'origine américaine dans le but de savoir comment ils vivent personnellement la désinformation autour du coronavirus sur Internet. D'après leur recherche, deux éléments jouent un rôle déterminant dans cette diffusion malveillante. D'une part, la majorité des sondés pensent que les utilisateurs d'une manière générale sont trop vulnérables face à la désinformation. En revanche, ils ont répondu à titre personnel qu'ils faisaient preuve d'une grande vigilance. Les scientifiques ont alors estimé que les efforts d'éducation aux médias et la sensibilisation aux fausses informations restent difficiles, car personne ne pense en avoir vraiment besoin.

D'autre part, un aspect de cette recherche concerne les émotions. Les chercheurs ont constaté que les internautes ressentaient des émotions face à ce type de contenu, allant de la peur au dégoût, en passant par l'inquiétude, l'angoisse et d'autres formes de ressentiment. Ces états émotionnels les incitent indirectement à partager ces fausses informations avec leurs propres connaissances sur le sujet. Ainsi, cela peut vite devenir un cercle vicieux. À cet égard, l'Union européenne compte renforcer, sans toutefois porter atteinte à la liberté d'expression, ses mesures contre la désinformation et la haine en ligne provenant de sources étrangères au territoire européen, mais aussi de sources internes, à savoir divers médias d'information, des mouvements et organisations politiquement extrémistes présents dans des pays de l'Union européenne, qui ont tous l'ambition d'altérer la confiance des Européens[137]. Elle souhaite également un encadrement plus strict des publicités politiques et une plus grande protection des médias.

La Commission européenne invite dès lors les États européens à imposer des sanctions financières aux auteurs de telles actions, et compte améliorer son code de bonnes pratiques pour lutter contre la désinformation. Ces mesures s'inscrivent dans le projet de règlement européen *Digital Services Act*[138] (loi sur les services numériques) et également d'un *Digital Market Act* (loi sur le marché numérique) centré sur les questions de concurrence[139]. Ce texte semble arriver à point nommé au regard du contexte de la crise sanitaire et des élections américaines qui ont montré les effets nuisibles que les réseaux sociaux peuvent porter. De nombreux experts dénoncent l'enfermement des internautes dans des bulles de filtres, comme un cocon numérique où le partage d'opinions et le débat construit grâce à la contradiction n'ont pas de place. À titre d'exemple, la cellule StratCom de l'UE a identifié plus de 8 000 cas de désinformation sur la Covid-19 diffusés dans plus de vingt langues en seulement quatre mois, provenant de médias proches du Kremlin et répertoriés dans sa base de données EUvsDisinfo[140].

(136) Yunjuan Luo, *What makes COVID misinformation so tough to stop on social media* [Ce qui fait que la désinformation autour de la Covid est si difficile à arrêter sur les réseaux sociaux], Eurekalert.org, 7 déc. 2020.
(137) Procès-verbal de la 2 341e réunion de la Comm. UE à Bruxelles du 10 juin 2020, approuvé le 24 juin 2020.
(138) Comm. UE, *Proposal for a regulation on a single market For digital services « Digital Services Act »* (Proposition de règlement sur un marché unique des services numériques « loi sur les services numériques »), 15 déc. 2020.
(139) Comm. UE, *Shaping Europe's digital future : The Digital Services Act package* [Façonner l'avenir numérique de l'Europe : le paquet de la loi sur les services numériques], 16 déc. 2020.
(140) EUvsDISINFO, *Figure of the week : 8000*, 7 avr. 2020.

Dans la mesure où ils mettent en avant des contenus très engagés et remplis d'émotions négatives, ces types d'informations attirent malheureusement plus que le discours calme et rationnel. Laure de La Raudière, députée d'Eure-et-Loir, dans son article sur « la fabrique de la loi à l'ère du numérique »[141] explique qu'ils se nourrissent de la peur et diffusent des informations incomplètes ou totalement altérées pour arriver à leur fin. Il n'y a qu'à observer les mouvements anti-vaccins à la fin de l'année 2020. Il faut remonter à l'époque de la grippe aviaire pendant laquelle la peur au sein de la population autour des vaccins s'est accrue, par l'intermédiaire entre autres de nombreux forums en lignes. Les parents qui ont consulté ces forums deviennent de plus en plus craintifs vis-à-vis de la vaccination, même pour les vaccins obligatoires de leurs enfants, ce qui peut causer des répercussions catastrophiques pour la santé publique et conduire les pouvoirs publics à passer d'une politique de recommandation vaccinale à une politique de vaccination obligatoire afin d'assurer la sécurité et la santé publiques[142]. Une résistance croissante est alors observée contre la parole publique, notamment celle qui provient de l'État, et cela conduit à avoir une nouvelle société plus horizontale qui amène de nouvelles problématiques : « Pourquoi ceux qui nous gouvernent ou qui nous représentent seraient-ils plus crédibles que les autres ? », demande la députée. Il existe par ailleurs un renversement de la crédibilité de la parole politique qui est sans cesse remise en cause ou réinterprétée, et où tout est fait dans l'intérêt de l'État et non du citoyen. « Puisque la parole est officielle, elle est soupçonnée d'être manipulatrice. »

Cette fracture devient de plus en plus visible *via* Internet et les réseaux sociaux. Il s'agit d'une course dans laquelle les internautes dévoilent leurs opinions non pas pour débattre sur un point de vue, mais parce qu'ils pensent qu'ils détiennent la vérité sur fond de rumeurs[143], et qu'ils ont de ce fait la responsabilité de la divulguer. Mais, pour se faire entendre parmi cette foule numérique, il faut métaphoriquement « crier le plus fort » et tous les moyens sont utilisés. Cela passe surtout par une logique de plus en plus extrémiste où le sensationnel est omniprésent pour pouvoir attirer les internautes vers soi[144]. La protection des libertés fondamentales est une priorité pour le juge comme pour le législateur et par conséquent toute mesure, y compris en état d'urgence, doit préserver la liberté d'expression et liberté de pensée et communication des populations, et la liberté de la presse.

Ainsi que l'ont reconnu la Cour européenne des droits de l'homme et de nombreux organismes intergouvernementaux, y compris les Nations unies dans leur Plan d'action sur la sécurité des journalistes et la question de l'impunité ou le Comité des droits de l'homme dans son Observation générale n° 34, l'éventail des acteurs des médias s'est élargi avec l'apparition de nouvelles formes de médias à l'ère numérique. C'est pourquoi la notion d'acteur des médias comprend aussi toute personne qui contribue à alimenter le débat public, pratique des activités journalistiques ou

(141) L. de La Raudière, *La fabrique de la loi à l'ère du numérique : Enjeux numériques* 2018, n° 3.
(142) B. Espesson-Vergeat.
(143) P. Moliner, *Médias, relais et discussions sur Twitter. Proximités et distances lexicales à propos du Covid-19 : Communication et Organisation* 2020, p. 89-107.
(144) A. Chaves-Montero, F. Relinque-Medina, M.Á. Fernández-Borrero et O. Vázquez-Aguado, *Twitter, Social Services and Covid-19 : Analysis of Interactions between Political Parties and Citizens : Sustainability* 2021, 13, 2187.

joue un rôle de « chien de garde » dans la sphère publique. Le Conseil de l'Europe a émis une recommandation sur la protection des journalistes et acteurs de l'information contre les atteintes des pouvoirs publics et autres pouvoirs qui viennent porter atteinte aux droits des journalistes. Pour créer et maintenir un environnement favorable à la liberté d'expression garantie par l'article 10 de la Convention, les États doivent respecter un ensemble d'obligations positives, établies dans les arrêts pertinents de la Cour européenne des droits de l'homme et énoncées dans les principes figurant dans l'annexe à la présente recommandation. Ces obligations doivent être remplies par les pouvoirs exécutif, législatif et judiciaire, au sein des gouvernements ainsi que par toutes les autres autorités de l'État, y compris les services responsables du maintien de l'ordre public et de la sécurité nationale, à tous les niveaux : fédéral, national, régional et local. Les piliers des droits des journalistes sont la prévention, la protection, les poursuites (avec une attention particulière à l'impunité) et la promotion de l'information, l'éducation et la sensibilisation.

La lutte contre la désinformation dans la phase Covid passe par un renforcement des droits des journalistes et de leur liberté d'expression, avec un organe de contrôle indépendant et un engagement des États à soutenir ces mesures par des dispositions législatives fortes et une intervention judiciaire. L'attention est attirée sur les risques liés à l'utilisation de l'IA dans les médias, au regard de l'article 10 de la Convention européenne des droits de l'homme, mais aussi intégrant les différents risques et réglementations croisées à mettre en œuvre. Il faut garder à l'esprit que le recours aux applications d'IA se trouve à la croisée de la liberté d'expression et d'autres droits de l'homme, notamment le respect de la vie privée et l'interdiction de discrimination. De ce fait, les cadres réglementaires et la répartition des responsabilités entre les autorités régulatrices doivent tenir compte des relations entre les différents droits de l'homme.

L'épidémie de Covid-19 a amplifié ces défis auxquels sont confrontés les médias, les journalistes et l'espace de communication en général. Elle a également mis à nouveau l'accent sur certaines questions de longue date, telles que l'équilibre entre la liberté d'expression et la protection de la santé publique et d'autres intérêts énumérés à l'article 10-2 de la Convention européenne des droits de l'homme, mettant en évidence la nécessité de les traiter avec urgence et engagement.

La question de l'exploitation de l'IA forte dans la communication, source de *fake news*, est un vrai sujet de réflexion. L'article 10 de la Convention européenne des droits de l'homme interdit aux États membres de s'ingérer sans justification dans le droit à la liberté d'expression des journalistes et des responsables de médias. La Cour européenne des droits de l'homme a établi qu'« [o]utre la substance des idées et informations exprimées, l'article 10 (...) [protégeait] leur mode de diffusion ». Elle a également affirmé que l'article 10 de la Convention s'appliquait aux moyens de diffusion, « car toute restriction apportée à ceux-ci touche le droit de recevoir et communiquer des informations ». Par conséquent, il n'appartient ni aux juridictions internes ou supranationales, ni aux autorités de régulation de dire aux médias quelle technique de compte rendu les journalistes doivent adopter. Journalistes, médias, réseaux sociaux et moteurs de recherche sont donc libres d'utiliser des applications d'IA pour produire et diffuser des contenus.

Les 10 et 11 juin 2021, les ministres responsables des questions relatives aux médias et à la société de l'information se réunissent pour convenir des mesures nécessaires pour faire face aux changements radicaux de l'environnement des médias et de l'information provoqués par la numérisation massive, qui a des effets dramatiques sur l'exercice de la liberté d'expression et un impact important sur d'autres droits et libertés de l'homme. Ces instruments garantiront l'engagement politique du Conseil de l'Europe et de ses États membres pour un certain nombre d'actions prioritaires et contribueront au programme du Comité directeur sur les médias et la société de l'information du Conseil de l'Europe (CDMSI) pour les activités normatives et pour la mise en œuvre des normes existantes, pour les années à venir. Les résultats de ces travaux permettront d'avancer dans une démarche globale de protection et de traitement de l'« infodémie » tout aussi dangereuse que la pandémie elle-même.

L'individu désire avoir davantage de pouvoir et refuse que l'on décide à sa place, même dans le milieu médical[145]. François Stasse, économiste diplômé de l'Institut d'études politiques et docteur d'État en sciences économiques, a confié que l'autorité des médecins est souvent remise en cause et qu'ils sont tenus d'expliquer, voire de justifier les décisions qu'ils prennent. D'après lui, ce nouveau comportement provient de la retentissante affaire du Mediator[146] et celle du sang contaminé[147], qui ont donné un « coup de boutoir porté au prestige médical ». Par ailleurs, les lois bioéthiques sont certes considérées comme des avancées majeures, mais ne sont pas très bien perçues par une partie de la population, avec selon elle une absence d'éthique scandaleuse.

La société tolère certaines pratiques de la médecine qui paraissaient invraisemblables quelques dizaines d'années auparavant, ou bien au contraire, elle ne tolère plus certaines méthodes d'un ancien temps et qui sortent du cadre éthique et moral de notre société actuelle. Les mentalités ne cessent ainsi d'évoluer, et qui sait ce qui sera autorisé ou non, sous couvert de la morale et de l'éthique, dans les prochaines décennies. À cet égard, l'une des questions préoccupantes, explique François Stasse, est celle posée par le courant transhumaniste. « Quand les scientifiques sauront agir sur le cerveau pour rendre les hommes plus intelligents ou plus puissants, devrons-nous laisser faire ? Devrons-nous renoncer au principe de l'égalité républicaine puisque seuls les plus fortunés pourront recourir à ces techniques ? Le moins que l'on puisse dire est que cela ne va pas de soi. Nous ne pouvons pas laisser le calendrier scientifique dicter la loi de la société sans en débattre collectivement. Einstein et Camus s'inquiétaient déjà de cela au milieu du siècle dernier. » Ainsi, l'important est de savoir vers quoi la société tend. Les scientifiques ne peuvent prédire l'avenir, mais il est possible de faire une santé prédictible, en prévoyant certaines problématiques qui se poseront dans les années futures par

(145) F. Stasse, *Le savoir ne dit rien sur la morale : Les Tribunes de la santé* 2016, Propos recueillis par H. Delmotte, p. 99-104.
(146) P. Troude-Chastenet, *Santé publique et démocratie : l'affaire du Mediator : Études* 2011, p. 185-196.
(147) K. Ouldamar et A.-M. Gallerand, *La sécurité sanitaire en France : de l'affaire du sang contaminé à la réforme des vigilances : Santé publique* 2019, p. 517-526.

l'intermédiaire d'un débat construit et qui devront dans le même temps préserver notre libre arbitre.

Concilier l'innovation, l'information avec la protection des droits fondamentaux est donc une condition *sine qua non* pour assurer la pérennité d'un environnement juridique et éthique pour la vie de l'être humain dans un univers où l'intelligence artificielle est omniprésente, y compris dans la gestion des fausses ou vraies informations. Cette montée en puissance du numérique crée de plus en plus d'enjeux aux conséquences multiples, que ce soit au niveau de la création des produits de santé, de l'organisation de la fabrication, de l'organisation de la *supply chain*, de la distribution et de la traçabilité et surveillance des produits. Elle joue un rôle fondamental dans l'organisation des soins, la prise en charge du patient et la gestion de son parcours de santé. Elle est enfin centrale dans l'organisation et le contrôle de la communication et de l'information transmise par les acteurs de presse, mais aussi sur les réseaux sociaux. Cette question sera au cœur des échanges sur la protection de la presse et des journalistes, et devrait apporter des réponses à l'été 2021[(148)]. Il convient donc de suivre avec attention l'évolution de la relation de confiance tant du patient que du consommateur avec les acteurs de santé qui l'entourent, dont les acteurs du numérique qui tiennent une place déterminante dans la santé de demain.

(148) Conférence des ministres responsables des médias et de la société de l'information, *Intelligence artificielle – Une politique intelligente : défis et opportunités pour les médias et la démocratie*, Coorganisée par le Conseil de l'Europe et le gouvernement de la République de Chypre (10-11 juin 2021, en ligne).

CHAPITRE 2

# NOUVELLES TECHNOLOGIES CONNECTÉES ET INTELLIGENCE ARTIFICIELLE

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Manon BRUNON
Ela CAN
Silène COUTANSON

INTRODUCTION

## ENJEUX JURIDIQUES DE LA QUALIFICATION DES PRODUITS DE SANTÉ CONNECTÉS

Depuis une vingtaine d'années, les nouvelles technologies sont apparues et leur développement se base principalement sur l'utilisation de l'intelligence artificielle (IA). Aujourd'hui, un peu plus tardivement que pour d'autres secteurs, le monde de la santé a été influencé par ces nouvelles technologies à travers l'utilisation d'algorithmes dans les logiciels de santé et l'apparition d'objets et robots connectés (IoT) et d'objets médicaux connectés, dotés aussi d'une IA.

Ce développement de l'IA au cœur de la santé expose tous les acteurs du secteur à ces innovations : le fabricant qui met sur le marché un logiciel, dispositif médical connecté, ou produit de santé connecté, le professionnel de santé qui travaille à l'aide d'un robot intelligent ou encore le patient qui utilise ces produits dans son quotidien afin de gérer et surveiller sa pathologie et améliorer la prévention en santé grâce à des objets ou application de bien-être à la frontière des produits de santé tels que les montres connectées dotées de capteurs de données physiologiques. Sont également visés tous les médicaments dont l'évolution s'ouvre sur les biomédicaments, médicaments connectés qui embarquent des logiciels, ou dispositifs médicaux avec des nanocomposants. Ces produits

innovants dotés de numérique posent une difficulté quant à leurs qualification et classification juridiques.

Comme tous produits de santé mis sur le marché, ces nouveaux objets connectés doivent être qualifiés juridiquement au regard du *corpus* législatif et réglementaire existant au niveau européen et national, et dans une perspective d'innovation juridique concomitante à cette évolution numérique(1).

Ils entrent souvent dans le champ des produits dits « frontières », appelés également « produits complexes », soit parce qu'ils ne répondent à aucune qualification spécifique au domaine de la santé, soit parce qu'ils entrent dans le champ de plusieurs qualifications(2) relevant du droit de la réglementation santé, et de la réglementation des produits de consommation courante. L'évolution des produits de santé portant sur les médicaments, dispositifs médicaux, produits numériques s'inscrit dans le cadre d'une nouvelle approche de la santé largement décrite par différents rapports et études d'impact précédant les évolutions réglementaires préparées par la Commission européenne(3). Selon la Commission européenne, la santé et les soins numériques désignent les outils et les services qui utilisent les technologies de l'information et de la communication (TIC) pour améliorer la prévention, le diagnostic, le traitement, la surveillance et la gestion de problèmes liés à la santé et gérer les modes de vie ayant une incidence sur la santé. La santé et les soins numériques sont innovants et peuvent améliorer l'accès aux soins et leur qualité et renforcer l'efficacité globale du secteur de la santé.

Dans le travail de qualification du produit frontière, les entreprises vont mettre en place une stratégie d'analyse juridico-économique, qui peut s'apparenter à un comportement de *forum shopping*. En effet, puisque les règles de mise sur le marché diffèrent beaucoup en fonction de la qualification du produit, en termes d'exigence, de durée ou encore de coût, il convient de procéder à un effort de qualification afin de présenter le produit aux autorités en vue de l'obtention du statut juridique recherché, le moins contraignant n'étant pas nécessairement le plus pertinent. En effet, l'obtention du statut de dispositif médical (DM) connecté peut être préférable à celui de produit de bien-être, dans une perspective de pénétration du secteur de la santé, et d'obtention du remboursement du produit par l'assurance maladie. La qualification du produit est donc déterminante pour son avenir sur le marché économique. Par ailleurs, le statut de DM connecté soumis au nouveau règlement sur les DM permettra une meilleure circulation du produit au sein de l'Union européenne, et une protection du produit contre les risques de contrefaçon. Ainsi, l'entreprise doit réaliser des choix stratégiques pour orienter son produit, considéré au départ comme complexe, vers la qualification adéquate. Outre les conditions de mise sur le marché, sont également déterminants les conditions commerciales,

(1) E. Zerhouni, *Les grandes tendances de l'innovation biomédicale au XXIe siècle* : Leçon inaugurale prononcée le 20 janvier 2011. Chaire d'Innovation technologique Liliane Bettencourt, *Les grandes tendances de l'innovation biomédicale au XXIe siècle*, Paris, Collège de France, coll. « Leçons inaugurales », 2013. European Medicines Agency (EMA), Annual Report 2018, *The European Medicines Agency's contribution to science, medicines and health in 2018*, 2018.

(2) B. Espesson-Vergeat, *Les objets connectés de santé et l'apparition du « patient-consommateur »*, fasc. « Les nouvelles technologies et leur incidence en droit de la consommation » : *CDE* sept. 2019, p. 37.

(3) Institut Montaigne, *Médicaments innovants prévenir pour mieux guérir*, sept. 2019. – Institut Montaigne, *Innovation en santé : soignons nos talents*, 2018.

l'état du marché dans le secteur de la santé, l'impact concurrentiel, et surtout les critères de sécurité, transparence et vigilance vis-à-vis de l'utilisateur. En toile de fond, la responsabilité du fabricant ou concepteur est en cause.

À travers ce comportement, qualifié parfois de *benchmark* réglementaire[4], les fabricants utilisent les frontières, parfois floues, entre les différentes réglementations des produits de santé, afin de s'imposer sur un marché concurrentiel complexe du fait de la définition du marché pertinent dans le secteur spécifique de la santé[5]. Cependant, l'arrivée des nouvelles technologies ne laisse pas toujours la possibilité à l'entreprise d'opter pour telle ou telle stratégie.

Les enjeux juridiques qui découlent de la qualification du produit sont fondamentaux pour assurer le positionnement du produit sur le marché. Le fabricant ou concepteur doit se poser ces questions dès le commencement du projet, c'est-à-dire au moment où le bureau d'études va débuter le travail sur un prototype, par exemple. En effet, selon la qualification du produit, toute la suite du développement juridique et réglementaire du produit sera guidée par celle-ci. La coopération des équipes techniques et juridiques est alors indispensable afin de parvenir à une mise sur le marché rapide et efficace. La qualification du produit aura un impact sur tous les utilisateurs du produit, qu'il s'agisse des établissements de santé, professionnels de santé, auxiliaires ou du patient lui-même. Seront également impactées par la qualification du produit l'assurance maladie, dès lors que le remboursement du produit sera admis, mais aussi la Haute Autorité de santé (HAS), qui émet des avis et recommandations sur les conditions et modalités d'utilisation du produit[6], et enfin l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), qui viendra assurer le contrôle et la vigilance sur l'utilisation du produit, dès lors que sa qualification le place dans le périmètre de compétence de l'agence. Enfin, les pouvoirs publics auront un intérêt particulier dans la qualification du produit, notamment en raison des incitations financières sur les projets innovants en santé[7].

Afin d'aider les fabricants dans leur qualification face à ces nouveaux produits de santé innovants, au niveau national, la Haute Autorité de santé (HAS) propose des référentiels aux concepteurs de logiciels d'aide à la prescription. Ces guides leur permettent de savoir s'ils doivent prendre en compte la réglementation sur les dispositifs médicaux, ou non. Toute la question sera de savoir si ces avis, recommandations, référentiels s'imposent aux acteurs et dans quelles conditions[8]. Au niveau de l'Union européenne, la Commission européenne, consciente de l'arrivée de l'IA dans le secteur de la santé et des enjeux de la qualification des produits, propose

(4) N. Homobono et R. Bove, *Les produits frontières : Les Tribunes de la santé* 2017, vol. 55, n° 2, p. 29-36.

(5) B. Espesson-Vergeat, *La spécificité des produits de santé et l'identification complexe du marché pertinent en droit européen de la concurrence : RGDM* 2018, n° 26, p. 59-71 ; *Les produits de santé, synthèse de l'actualité juridique 2017, panorama de droit pharmaceutique* : journal de médecine légale, droit médical, victimologie, dommage corporel 2014, LEH, p. 65-79.

(6) HAS, *Référentiel de certification par essai de type des logiciels d'aide à la prescription en médecine ambulatoire*, nov. 2009.

(7) Comm. UE, *Manual on borderline and classification in the community regulatory framework for medical devices*, version 1, 22 mai 2019.

(8) B. Espesson-Vergeat, *La pratique médicale face aux avis et recommandations des autorités de santé : RGDM* 2009, n° 30.

régulièrement des manuels afin d'aider les fabricants dans le choix de réglementation pour leurs produits *borderline*[9].

Ces nouveaux enjeux juridiques, liés à l'utilisation de l'IA dans le monde de la santé, apportent de considérables avantages pour l'ensemble de la société, ainsi que pour les nombreux acteurs du numérique notamment qui interviennent activement dans ce domaine spécifique de la santé. Il va sans dire, et la multitude des études sur le sujet le démontre, qu'il y a un emballement de l'innovation scientifique et médicale avec et grâce au numérique entendu au sens large. Cette activité se caractérise notamment par la capacité à découvrir et mettre sur le marché en un an un nouveau vaccin contre la Covid-19. Les exemples sur les aspects positifs de l'utilisation du numérique dans le secteur de la santé, et plus particulièrement dans les produits de santé connectés (médicaments connectés, robots intelligents), pourraient être largement développés. L'innovation précède l'encadrement juridique et les questionnements liés à l'utilisation de ces produits surviennent au cours de l'approche de recherche et développement, puis de mise sur le marché et utilisation de ces produits, avec nécessairement un temps de retard, qu'il convient de réduire autant que faire se peut par l'intervention juridique au cours de l'activité d'innovation. En effet, l'IA, mal maîtrisée, peut entraîner des inconvénients pour les acteurs du secteur de la santé, notamment avec certaines dérives dans le comportement des acteurs du monde de la santé (Section 1).

Afin d'encadrer ces avantages et inconvénients, et pour qu'il n'y ait pas d'abus, le législateur s'engage vers l'élaboration d'un cadre juridique et réglementaire de l'IA en santé, mais se trouve confronté à des questionnements majeurs à la frontière de l'éthique et de la morale (Section 2).

SECTION 1

## AVANTAGES ET INCONVÉNIENTS DES NOUVELLES TECHNOLOGIES CONNECTÉES

Le numérique s'est considérablement imposé dans le domaine de la santé ces dernières années, suscitant un véritable débat sociétal. C'est notamment pour cela que la loi de 2016 sur l'économie numérique a confié à la CNIL la mission de conduire une réflexion sur les enjeux éthiques et les questions de société soulevées par l'évolution des technologies numériques. Cette mission est essentielle dans cette nouvelle ère, car le numérique représente depuis ces dernières années une réelle préoccupation citoyenne, comme le montre une étude réalisée en 2017 selon laquelle 72 % des Français estimaient que les algorithmes représentaient un enjeu de société.

Ce virage numérique, incontestablement révolutionnaire pour le domaine de la santé, fait jaillir des technologies de rupture qui bénéficient à tous ses acteurs

(9) L. n° 2016-1321, 7 oct. 2016, pour une République numérique.

sans exception (§ 1). Mais comme tout progrès, ce tournant dans l'approche scientifique et médicale s'accompagne de nombreuses dérives, obligeant le législateur à s'interroger et à se positionner sur diverses problématiques qui y sont liées (§ 2).

## § 1. – Des technologies de rupture au service de la santé

Alors que le secteur de la santé s'est ouvert tardivement au numérique, il est désormais au cœur des pratiques dans le domaine médical, en raison de la conception même de la médecine nécessairement en lien direct entre le professionnel de santé et le patient, ou encore dans le domaine pharmaceutique en raison de la complexité de la recherche fondamentale et appliquée portant sur les produits de santé innovants. L'émergence de ces nouvelles technologies a contribué à l'apparition d'une vision de la médecine « 4P » (prédictive, préventive, personnalisée, participative) puis « 6P » (preuve et parcours patient) qui s'accompagne du développement de nouveaux produits de santé, sous l'impulsion de la loi sur la modernisation du système de santé[10], poursuivie par la loi « Ma Santé 2022 ». Ces évolutions concomitantes des produits et techniques médicales représentent un formidable creuset d'innovation pour le monde scientifique et le secteur médical au bénéfice de tous les acteurs et usagers du système de santé (I).

Par ailleurs, dans une société marquée par le vieillissement de la population, par l'émergence de nouvelles pathologies, et par la progression inquiétante des dégradations de la santé liées aux facteurs environnementaux, les progrès technologiques représentent un immense vecteur de croissance économique, inscrit dans un véritable cercle vertueux de constante progression, dont bénéficient le patient à l'échelle individuelle, mais aussi plus largement l'ensemble du système de santé au niveau national, et contribuent plus largement à l'élévation générale du niveau de santé des populations au sein des territoires (II).

Parallèlement aux économies réalisées, ces différentes transformations ont, en conséquence, fortement impacté le système de santé en place, notamment son encadrement juridique et réglementaire. L'Union européenne s'engage dans une démarche active concernant le statut de l'IA et plus spécifiquement dans le secteur de la santé. Cette démarche initiée[11] depuis quelques années s'accélère avec la nécessité d'assurer une protection efficace des utilisateurs. L'initiative intitulée « Une Europe adaptée à l'ère numérique » fait partie des six priorités politiques de la Commission pour la période 2019-2024. S'appuyant sur des initiatives antérieures en faveur de la création d'un marché unique numérique, la transition numérique devrait profiter à tous, donner la priorité aux citoyens et ouvrir de nouvelles perspectives aux entreprises. La santé figure parmi les secteurs visés par cette initiative,

(10) L. n° 2016-41, 26 janv. 2016, de modernisation de notre système de santé.
(11) E. Van den Abeele, *La réglementation, « intelligente, affûtée et performante » de l'UE : une nouvelle bureaucratie au service de la compétitivité : Working Paper* 2014, 05, Bruxelles, ETUI.

étant donné les avantages potentiels que les services numériques peuvent offrir aux citoyens et aux entreprises dans ce domaine[12]. Depuis plus de vingt ans, l'Union européenne investit dans plusieurs projets et initiatives structurants en matière de numérique en santé au service des citoyens européens. L'objectif est de fluidifier le parcours de soin du patient au sein de l'Union européenne, et plus largement de favoriser les collaborations entre organisations qui délivrent les soins et organisations en charge de la recherche médicale. Un réseau européen des représentants de la stratégie du numérique en santé nationale anime les échanges sur les collaborations européennes en matière de e-santé, sous l'égide de la Commission européenne (DG Santé) : le réseau *eHealth Network*, créé en 2011 par la directive européenne des soins transfrontaliers[13].

La France participe au programme de mise en place des infrastructures d'échange de données entre les pays membres (CEF eHealth) et aux actions conjointes (eHAction, X-eHealth, TEHDaS)[14]. La déclinaison opérationnelle du Programme *EU4Health* a pour ambition de soutenir les actions en support de l'Europe de la santé pour 2021-2027. Au-delà de l'échelle européenne, la France est partie prenante de plusieurs initiatives internationales sur le déploiement du numérique en santé, *via* sa représentation et sa participation aux actions de l'Organisation mondiale de la santé (OMS) et de l'OCDE en matière de numérique en santé ou encore dans les organismes de normalisation tels que HL7 ou IHE.

L'intérêt de mettre en place une nouvelle réglementation est de plus en plus urgent.

## I. – Les acteurs du monde de la santé au cœur du processus d'innovation

Le droit à la santé est un enjeu essentiel au cœur des préoccupations des États, et désormais une priorité absolue révélée par la pandémie de Covid-19, avec la mise à l'arrêt de l'ensemble des activités économiques sur tous les territoires.

Cet enjeu apparaît dans la Déclaration universelle des droits de l'homme[15], qui dispose que « toute personne a droit à un niveau de vie suffisant pour assurer sa santé, son bien-être et ceux de sa famille, notamment pour l'alimentation, l'habillement, le logement, les soins médicaux ainsi que les services sociaux nécessaires… ».

Le Pacte international pour les droits économiques, sociaux et culturels précise que : « Les États parties au présent Pacte reconnaissent le droit qu'à toute personne de jouir du meilleur état de santé physique et mentale qu'elle soit capable d'atteindre ».

(12) Comm. UE, *eHealth Network Summary report*, 18th Meeting of the Health Network (Téléconférence), 12-13 nov. 2020. *Infrographic, Transformation of health and care in the digital Single Market – Harnessing the potential of data to empower citizens and build a healthier society.*

(13) Dir. (UE) 2011/24/EU en matière de soins de santé transfrontaliers.

(14) X-eHealth, projet qui développe les bases d'un format d'échange transfrontalier de dossier de santé électronique (résultat de laboratoire, compte-rendu d'imagerie médicale, document de sortie, intégration des maladies rares à la synthèse médicale). eHAction, action conjointe qui élabore les orientations stratégiques et les outils dans les domaines prioritaires comme autonomiser les personnes ou améliorer la continuité des soins.

(15) DUDH, art. 25.

Ce droit à la santé est créateur de droits et de libertés, qui concernent l'ensemble du système de santé. Ce dernier se compose de cinq blocs d'intérêt : le patient, usager central du système de santé, les professionnels de santé, les établissements de santé, les industries de santé et enfin les autorités de santé, tous impactés de manière positive par ce virage numérique.

L'essor numérique a premièrement vocation à servir les intérêts de l'usager, au cœur du système, car grâce à lui, de nombreuses avancées scientifiques et médicales ont été possibles et contribuent directement à la santé du patient.

Même si le volet scientifique est prépondérant dans l'essor de cette technologie, le volet médical et les usages pratiques sont eux aussi profondément nécessaires pour les acteurs du secteur sanitaire afin de pallier certaine carence de l'offre de soins(16). Ces technologies se déclinent par exemple en applications diverses pour la prise de rendez-vous, ou l'établissement de diagnostic par une intelligence artificielle (*chatbot*) et encore la consultation par vidéoconférence qui s'est fortement développée durant la pandémie de Covid-19. Cette pandémie, aussi dramatique soit-elle pour l'ensemble de la société, a néanmoins contribué à l'activation de la télémédecine en France, qui tardait à se développer. En seulement un an, la pratique de la télémédecine a explosé en France. Au cours du mois de mars 2020 (début du confinement), plus d'un million de téléconsultations a été décompté, avec une multiplication de la télémédecine par trois du côté des patients et par six pour les médecins généralistes. C'est la conclusion qui ressort du nouveau baromètre sur la télémédecine, commandé par l'Agence du numérique en santé (ANS) à Odoxa et au cabinet de conseil Care Insight. Cette croissance nécessite de lourds investissements et un accompagnement de l'État. Dans le cadre du Ségur de la Santé, le gouvernement a attribué une enveloppe de deux milliards d'euros au numérique en santé. Ces produits numériques répondent ainsi aux problématiques de gestion des déserts médicaux et participent à la réduction des inégalités face à l'accès aux soins, à la continuité des soins, à la bonne observance des traitements par les patients. Ces innovations, constantes et agiles, qui ont permis d'assurer la prise en charge des soins au cours de la phase Covid-19, ont nécessité un encadrement réglementaire adapté au fil de l'eau, notamment par l'adoption pendant l'état d'urgence sanitaire(17) de dispositions dérogatoires aux exigences réglementaires conditionnant la mise sur le marché des produits de santé (médicaments et dispositifs médicaux)(18), constatées tant au niveau national qu'au niveau européen, par la Commission européenne(19).

Nombreuses sont les prouesses techniques observées à tous les stades de la prise en charge du patient, et notamment dès la première phase des examens biologiques et radiologiques, puisque ces technologies, plus performantes que l'humain, permettent des diagnostics plus précis et plus rapides que ceux posés par la

(16) ANS, *Échange et partage de données de santé, Retours d'expérience des bonnes pratiques sur l'échange et le partage de données de santé*, nov. 2018.

(17) L. n° 2020-290, 23 mars 2020 d'urgence pour faire face à l'épidémie de Covid-19.

(18) A. 7 nov. 2020, modifiant l'arrêté du 10 juillet 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire.

(19) Dir. 2001/83/CE et Règl. (CE) n° 726/2004, définissent les règles d'établissement des procédures centralisées et décentralisées.

capacité d'analyse de l'être humain. Ainsi, les moyens de diagnostic de la maladie d'Alzheimer ne permettaient de déceler la maladie qu'à un stade tardif, mais l'utilisation d'un algorithme a démontré que la détection de la maladie peut intervenir en moyenne avec six ans d'avance. Toutefois, ces résultats donnés par une IA posent immédiatement la question de la responsabilité du concepteur, programmateur de l'IA, et celle du professionnel de santé, en cas d'erreur de diagnostic ou en cas d'erreur dans le mode et le contenu de l'information donnée au patient. Au-delà de la question juridique de la responsabilité juridique, c'est surtout en termes d'éthique et de déontologie que se pose la question de l'interprétation des résultats de l'IA par les professionnels de santé[20].

Cette vague numérique envahit l'ensemble du secteur de santé et touche notamment la gestion des informations de santé par les professionnels de santé, entre eux, à l'égard de l'assurance maladie et au sein des établissements de santé. Le sujet de la protection des données médicales véhiculées par ces outils numériques est crucial à l'heure du développement de la cybercriminalité et du piratage des données de santé. La création chaotique du dossier médical partagé (DMP) lancé par la loi n° 2004-810 du 13 août 2004[21] relative à l'assurance maladie continue de soulever des difficultés dans l'application de l'espace de santé numérique (ENS) du patient prévu par la loi de 2019 et visant à rendre actif en 2021 le dossier pour tout patient. L'hébergement des données chez un opérateur numérique européen est souhaité afin d'assurer un encadrement juridique plus efficace[22]. L'objectif de ce DMP est d'assurer le suivi médical des patients par les professionnels de santé de façon coordonnée, mais le chemin reste long quant à la sécurisation de ces données. Enfin, il convient d'observer l'impact positif de ces technologies numériques dans le processus de soin, et la phase curative. En effet, ces innovations de pointe permettent aux patients de bénéficier de soins de qualité inégalable et auparavant inatteignable, comme dans la détection et le traitement de la maladie d'Alzheimer[23].

Peut également être cité le recours au premier cœur artificiel qui vient d'obtenir sa certification européenne pour être commercialisé et pris en charge par la sécurité sociale[24]. Le numérique offre la possibilité d'interventions chirurgicales de précision grâce à des robots dotés d'IA, permettant l'obtention de résultats impossibles par la main humaine. Là encore, se pose avec difficulté la question de la responsabilité du professionnel de santé, dans la décision médicale adaptée à la situation critique du patient, indépendamment du choix de l'IA, ou dans son obligation de formation à de nouvelles techniques opératoires et notamment par l'apprentissage de la commande des robots intelligents. Les premiers cas de mise en cause de la responsabilité des professionnels apparaissent aux USA, et ne manqueront pas de se manifester

(20) Cass., Colloque sur L'IA et l'expertise judiciaire, 26 nov. 2018.
(21) L. n° 2004-810, 13 août 2004, relative à l'assurance maladie.
(22) Comm. UE, *Projet sur les données numériques*, obtenu par Euractiv, 9 mars 2020.
(23) Radiology, *Un modèle d'apprentissage approfondi pour prédire le diagnostic de la maladie d'Alzheimer à l'aide de la TEP 18F-FDG du cerveau*, 6 nov. 2018.
(24) Collège de la HAS, avis n° 2020.0023/AC/SED, relatif à la prise en charge dérogatoire du dispositif CARMAT TAH en application de l'article L. 165-1-1 du Code de la sécurité sociale, 1er avr. 2020. – A. 28 sept. 2020, relatif à la prise en charge au titre de l'article L. 165-1-1 du Code de la sécurité sociale du dispositif CARMAT TAH.

sur le territoire national. Les questionnements se multiplient pendant la période de pandémie quant aux obligations du professionnel de santé lors de l'utilisation des technologies numériques dans leur exercice professionnel, et notamment la responsabilité liée aux consultations en visioconférence par la télémédecine, qui n'est pas adaptée à tous les cas.

Une analyse précise au cas par cas du respect des règles déontologiques dans l'utilisation d'une technologie numérique au cours de l'exercice médical s'imposera, afin d'identifier si les notions de consentement libre et éclairé, d'information doivent évoluer afin de s'adapter au contexte numérique. Vastes sont les problématiques juridiques soulevées par ces usages nouveaux dans l'activité scientifique et médicale. Mais incontestablement, le progrès en marche est déjà très avancé et génère des perspectives économiques qui devront être appréciées au regard de questions éthiques et déontologiques brûlantes qui trouveront dans l'encadrement juridique et réglementaire un périmètre de protection.

Ces sujets déterminants pour l'avenir de la science et de la médecine sont au cœur des politiques de santé et du numérique. La création de l'Agence du numérique en santé (ANS) a pour vocation d'accompagner cet épanouissement en le cadrant. L'ANS apporte un soutien juridique aux projets de numérique en santé en constatant la difficulté d'application des règles dans un contexte mouvant. Tout projet de système d'information de santé doit faire l'objet d'un cadrage en amont de sa mise en œuvre en tenant compte des problématiques juridiques propres. La réflexion doit être mise à jour en fonction de l'avancement du projet jusqu'au déploiement du système d'information sur le terrain, qui peut susciter de nouvelles interrogations juridiques. S'agissant de systèmes d'information de santé, les principales problématiques juridiques ont trait à la protection des données personnelles, la protection des données de santé, la propriété intellectuelle, la commande publique et le droit de la concurrence, le droit du numérique.

La feuille de route de l'ANS pour 2022 présente trente actions fortes visant à renforcer à tous les niveaux, et vis-à-vis de tous les acteurs, le numérique en santé, incluant l'encadrement juridique, réglementaire et déontologique indispensable, lequel passe par une révision des codes en vigueur.

Cet accompagnement des entreprises en amont permet de sécuriser juridiquement les projets. Toutefois le récent rapport du Conseil national du numérique fait état des propositions à mettre en œuvre pour implanter efficacement le numérique en santé, en insistant notamment sur l'encadrement juridique permettant de sécuriser les acteurs, entreprises, établissements de santé et professionnels de santé. Les propositions du rapport s'enracinent dans un plaidoyer pour une dynamique française et européenne du numérique en santé et poursuivent trois objectifs : lever les freins à l'innovation, faire de l'Espace numérique de santé (ENS) l'épicentre du système de santé, acculturer, former et accompagner les utilisateurs des plateformes nationales de santé[25].

(25) ANS, *L'ANS publie la 3e vague du baromètre sur la télémédecine*, 13 janv. 2021.

## II. – Un vecteur d'économies à destination de la recherche et des innovations

Ces avancées technologiques représentent des performances scientifiques impactant le patient, son bien-être et finalement son espérance de vie. Ces avancées du numérique en santé, outre les intérêts individuels pour le patient et l'organisation de l'ensemble du système de santé, contribuent à la croissance économique en favorisant le maintien ou le retour à une bonne santé pour une population qui reste active et source de croissance. Cet essor du numérique en santé génère par ailleurs la croissance de nouvelles entreprises du numérique qui deviennent des intermédiaires cruciaux dans le fonctionnement du système de valeur, allant jusqu'à renverser l'équilibre entre les acteurs de santé. La place occupée par les entreprises du numérique devient déterminante, ce qui représente tout à la fois un avantage et un risque considérable quant à la sécurisation des données et systèmes. Aussi avancé soit-il en termes d'innovation numérique, le système de santé est à la merci des piratages et n'a jamais été aussi fragile et dépendant. Aussi l'impact économique recherché, s'il s'avère très profitable pour tous les acteurs de santé et pour les acteurs du numérique spécialiste en santé, et plus généralement pour l'ensemble de l'économie, représente un risque majeur pour la sécurité des personnes et de leurs données. Il est donc fondamental d'assurer un appui technique, technologique solide, accompagné d'un encadrement juridique puissant et agile permettant, au fil de l'évolution, d'anticiper et de traiter les nouvelles problématiques avant leur survenance, et non pas seulement en aval en réparation des risques survenus. La croissance économique attendue est donc interdépendante de la solidité de son encadrement, et de la confiance qui peut être accordée aux innovations numériques.

Dès lors que ce périmètre de sécurité est assuré concernant le numérique en santé qui permet de produire de nouveaux modes d'organisation du système de santé, il convient de remarquer l'enjeu économique que ce marché représente, avec les conséquences concurrentielles qui en découlent[(26)]. Ces économies sont évidentes à l'échelle individuelle pour le patient, acteur central du système de santé. Ce dernier va pouvoir améliorer sa façon de se soigner, et prévenir les risques. Le recours au numérique en santé doit permettre au patient de se soigner de façon plus régulière, ce qui devrait avoir pour effet de prévenir les maladies et éviter l'aggravation des pathologies déjà présentes.

Cette projection économique de la croissance du numérique en santé devrait avoir pour conséquence de réduire les différences face aux soins, traduction directe des inégalités sociales et problématiques encore trop présentes aujourd'hui, comme le met en évidence la récente étude de l'Observatoire de la Mutualité française démontrant qu'un Français sur dix vit dans une commune où l'accès à un médecin généraliste est limité, et que le nombre de généralistes aura baissé de 13 % entre 2010 et 2025, rendant les inégalités dans l'accès aux soins de plus en plus criantes[(27)]. Par ailleurs, cette étude indique que ces situations ne sont pas définitives

(26) Autorité de la concurrence, Rapport annuel, 2018.
(27) L'Observatoire, *Accès territorial aux soins*, oct. 2020.

et que le succès de la télémédecine permet d'améliorer cet accès aux soins. Le sondage publié par l'ANS dans le baromètre télémédecine, lors de la troisième vague de la pandémie en janvier 2021, démontre l'impact croissant de la télémédecine auprès du corps médical et des patients, mais pointe également les failles du système.

Le développement massif du numérique en santé touche aussi les établissements de santé, publics et privés, restés très en retard en dépit du programme « Hôpital numérique », et devrait leur permettre de trouver une source d'économies dans la réorganisation de leurs services et des fonctions des professionnels de santé. L'investissement dans les technologies de pointe devrait permettre d'établir un diagnostic de façon autonome et rapide, avec pour effet de réduire le temps de consultation et le temps de séjour dans l'établissement. Le recours au numérique en santé devrait permettre de s'engager activement vers un système ambulatoire, dont les effets économiques s'accompagnent d'avantage au plan sanitaire avec une réduction des infections nosocomiales et des risques liés à l'hospitalisation. L'amélioration de ces services de santé devrait avoir pour conséquence directe la réduction des risques médicaux et opératoires et la diminution du contentieux. Toutefois, ces points devront être appréciés dans les années à venir afin d'identifier la réalité de ces progrès liés au numérique et à l'ensemble des nouvelles technologies en médecine.

Enfin, l'assurance maladie représente le principal bénéficiaire des économies liées à l'intégration du numérique en santé et des nouvelles technologies dans la pratique médicale. L'anticipation dans la survenance d'une pathologie, l'amélioration dans le suivi et le traitement de celle-ci grâce aux outils numériques, l'amélioration des méthodes d'intervention et la réduction du temps d'hospitalisation, sans compter l'efficacité des produits de santé connectés, devraient conduire à une réduction du coût global de la santé.

Ces questions sont prégnantes et impliquent une position plus engagée vers la prise en charge et le remboursement des produits de santé connectés. Les recommandations de la HAS sur la prise en charge et le remboursement des produits vont en ce sens[28].

Enfin, les industries de santé sont fortement touchées par cette révolution technologique qu'elles ont certes intégrée tardivement. Ces innovations influent sur l'organisation de leurs secteurs de recherche et développement avec une accélération des pratiques et des résultats, ce qui permet de réduire les coûts de mise sur le marché des produits. La période Covid-19 a permis de démontrer l'efficacité de ces méthodes dans la recherche. Toutefois, ce contexte aggrave et déplace les questions de concurrence entre les industries de santé. Les produits deviennent complexes et numériques, et se créent eux-mêmes grâce à l'intervention des technologies numériques et notamment de l'intelligence artificielle autonome. Cela propulse les industries dans une nouvelle forme de compétition, basée sur l'exploitation des algorithmes dans la phase de recherche et *in vivo*. Cette concurrence change de fondements et d'objectifs. Cela conduit à de nouvelles formes de marchés et de nouvelles problématiques portant sur l'organisation des coopérations entre les acteurs,

(28) HAS, *Évaluer les dispositifs médicaux connectés, y compris ceux faisant appel à l'intelligence artificielle*, 19 févr. 2019.

les restructurations et la réorganisation du marché des produits de santé. Ce sont toutes les questions liées à la protection de la propriété industrielle, et intellectuelle, à la protection des données de l'entreprise et des secrets d'affaires, à la protection des données de santé collectées par l'entreprise et qui constituent sa valeur désormais, mais aussi toutes les questions liées à l'encadrement de la responsabilité des acteurs dans cet univers nouveau qu'il convient de résoudre.

En conséquence, bien au-delà de l'enjeu concurrentiel phénoménal que représentent les technologies numériques en santé et les économies qu'elles permettent de générer, ces technologies impliquent de nouvelles responsabilités pour l'ensemble des acteurs du système de santé, et notamment celles de garantir la protection des données personnelles et données de santé du patient qui représentent l'or brut et la valeur des entreprises. L'intérêt de renforcer la protection du traitement des données personnelles, préoccupation du règlement général sur la protection des données (RGPD)[29] est patent, et explique l'implication de la Commission européenne sur cette question, notamment par le *Digital Act*[30] dans la gestion des plateformes numériques qui visent aussi les produits de santé.

## § 2. – Les points négatifs et les dérives des technologies connectées

Le monde du numérique en santé présente une face cachée sombre. Au-delà des questions relatives à l'impact environnemental lié à l'utilisation exponentielle des nouvelles technologies, et à l'usage intensif des outils de communication par Internet, celles relatives à la protection des droits, au respect des libertés fondamentales, sont de plus en plus difficiles à appréhender. L'extension tentaculaire du numérique en santé apporte autant de bienfaits qu'il exacerbe de risques. Il convient d'envisager toutes les possibilités permettant au droit d'anticiper et traiter ces risques en organisant en amont une approche par la *compliance*[31] et les méthodes agiles.

Dans l'ensemble des difficultés soulevées par le numérique en santé, il convient de s'intéresser tout particulièrement aux catégories d'acteurs les plus exposées et notamment les plus vulnérables et les moins informées, les patients (I), puis aux utilisateurs de ces technologies qui portent la responsabilité de la décision médicale face aux patients : les professionnels de santé (II).

### I. – Les impacts négatifs sur le patient

Le droit ne peut pas évoluer et s'adapter aussi vite que les technologies apprenantes le peuvent de leurs erreurs. L'un des enjeux est de prouver ou du moins de

(29) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 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) ».

(30) Comm. UE, *Une Europe adaptée à l'ère du numérique : la Commission propose de nouvelles règles pour les plateformes numériques*, 15 déc. 2020.

(31) M.-A. Frison Roche, *Le droit de la Compliance au-delà du droit de la régulation : D.* 2018, p. 1561.

s'assurer de la stabilité et de la fiabilité de ces technologies numériques[32]. Selon la programmation initiale des *deep learning*, les évolutions et l'apprentissage de la technologie peuvent s'orienter vers une trop grande captation des données, une discrimination dans le traitement de données ou des personnes, et plus grave encore une discrimination dans la possibilité d'accéder à ces technologies qui améliorent et prolongent la vie humaine. L'accès à ces nouvelles technologies conduit à s'interroger sur le renforcement du droit à l'information du patient, sur l'expression du consentement libre et éclairé, sur l'accès pour tous à la santé. Ces questions trouvent une expression amplifiée lorsqu'elles sont examinées à l'échelle de la planète, marquant une fracture profonde entre les pays selon leur niveau d'accès à la santé. L'OMS alerte sur ces situations et invite les États à s'engager sur ces questions.

Au niveau national, la question centrale est celle de l'information et du consentement du patient à l'utilisation de ces nouvelles technologies et des données qui en sont issues[33]. L'analyse des modalités d'information et de recueil du consentement lors de l'utilisation des outils numériques doit permettre de préciser les points d'attention sur le contrôle de la bonne compréhension du patient. La participation de la personne de confiance doit être systématisée. La notion de « proches » du patient devrait également être définie afin de préciser clairement quelles sont les personnes ayant la capacité juridique à donner le consentement aux soins avec ou pour le patient. Le professionnel de santé voit son obligation d'information renforcée avec toutes les conséquences en termes de responsabilité[34]. Au-delà du recueil du consentement éclairé, et de l'information sur les techniques médicales grâce et au travers du numérique, l'information doit porter précisément sur le traitement des données qui seront recueillies, dans un mode de présentation compréhensible, et lisible, notamment par un public non averti. Le traitement de l'information du public senior et grand senior est un sujet à appréhender avec beaucoup d'attention, dans une société qui s'engage dans l'innovation numérique à destination d'une population vieillissante. Il convient de rappeler que le patient, parmi tous ses droits[35], a un droit à la vie privée[36], et que le traitement ou l'utilisation des données peut porter atteinte à ce droit. Le déploiement sans limite des produits de santé numérique dans la vie du patient, du matériel connecté en passant par les médicaments connectés ou encore les dispositifs médicaux implantables connectés, tous ces produits dotés de logiciels et d'intelligence artificielle rendent transparente la vie du patient dont les données de santé et données personnelles sont exposées au risque d'être piratées et utilisées publiquement.

En effet, de nombreuses technologies connectées permettent d'améliorer la santé, entraînant constamment une perfectibilité de l'être humain, pour repousser ses limites allant de l'homme réparé à l'homme transformé confronté à des robots quant à eux de plus en plus humanisés. Au titre de ces nouveaux produits,

(32) Défenseur des droits, *Algorithmes et discriminations : le Défenseur des droits, avec la CNIL, appelle à une mobilisation collective*, communiqué de presse, 31 mai 2020.
(33) Section 1 : « Principes généraux », C. santé publ., art. L. 1111-1 à L. 1111-9.
(34) L. Mazeau, *Responsabilité : Cahiers Droit, Sciences & Technologies* 11-2020, 227-234.
(35) C. Lantero, *Télémédecine et droits des patients : RD sanit. soc.* 2020, n° 1, p. 61 (halshs-02497544).
(36) C. civ., art. 9 ; Conv. EDH, art. 8.

les exosquelettes qui sont connectés au cerveau et permettent à des personnes tétraplégiques de pouvoir remarcher. Des dispositifs d'enregistrement contenant des électrodes sont implantés entre le cerveau et la peau, pour collecter et transmettre à un algorithme les signaux du cerveau. Au-delà des risques que présentent ces produits dans leur mise en œuvre et leur efficacité, nombre de questionnements surviennent concernant la fiabilité de ces technologies qui repoussent les lois de la nature, pour augmenter l'Homme, corriger ses imperfections.

L'un des risques de l'augmentation de l'Homme à l'infini est sa déshumanisation. L'Homme « naturel » a une identité, des valeurs, des droits acquis, qu'il pourrait perdre en étant transformé et augmenté. Les travaux sur l'évolution des soins et le transhumanisme sont très importants et se développent, posant la question éthique, juridique et philosophique de la protection de l'être humain dans sa spécificité[37], et plus spécifiquement l'analyse des droits et différences juridiques qui pourraient exister entre un patient normal et un patient « augmenté ».

Un homme « augmenté » aura certainement plus de facilités dans la société qu'un homme « classique »[38]. Une augmentation des performances du corps humain aura pour conséquence un meilleur accès à des emplois, au milieu politique ou sportif, et à une qualité de vie plus élevée. Un patient classique, qui refusera ces technologies, verra sa situation rétrogradée. Il y aura une rupture d'égalité. Cette situation hypothétique devrait être corrigée et évitée par l'élaboration de règles spécifiques portant sur la protection des droits du patient et des populations en prévention. Toutefois, la question de la mise en place d'un carnet vaccinal dans la phase de pandémie, afin de permettre la circulation libre au sein de l'Union européenne aux personnes vaccinées, conduit à s'interroger sur la privation de liberté des personnes non vaccinées, par impossibilité d'accès au produit, ou par recommandation médicale de ne pas avoir d'inoculation. Cette interrogation sur les risques de rupture d'égalité entre les patients devrait être prolongée pour le cas des patients « augmentés » ou non. L'inégalité d'accès aux nouvelles technologies améliorant le corps humain pourrait dépendre de plusieurs facteurs portant sur la nécessité de l'intervention médicale ou de confort, sur le financement de l'intervention pris en charge par l'assurance maladie ou supportée par le patient, sur le lieu d'intervention créant une rupture entre les régions dotées de services de santé innovants ou non. Loin d'élever le niveau de santé pour tous les citoyens, en conformité avec les objectifs du Traité sur le fonctionnement de l'Union européenne, l'innovation numérique pourrait conduire, si elle n'est pas précisément encadrée, à de profondes ruptures d'égalité et à des failles dans l'accès aux soins et droit à la santé des citoyens.

Ceci pose question au regard de la Déclaration des droits de l'homme et du citoyen en son article 1er : « Les hommes naissent et demeurent libres et égaux en droits ». En effet, dans ce contexte des nouvelles technologies, les hommes ne vivront plus égaux en droit. Le droit de se faire augmenter/soigner dépendra des ressources financières. Il serait possible d'aller jusqu'à s'interroger sur une violation de l'article 14 de la Convention européenne de sauvegarde des droits de l'homme

(37) J. Carbonnier, *Le transhumanisme face au droit et à l'éthique : Éthique & Santé* éd 2018 publié par Elsevier Masson SAS.
(38) X. Labbée, *L'homme augmenté face au droit*, PU du Septentrion, août 2015.

et des libertés fondamentales[39], portant sur le principe de non-discrimination, et complété par le Protocole additionnel n° 12[40]. En vertu de cet article, les distinctions ne peuvent pas être faites sur l'origine ou les caractéristiques du citoyen. Or, les ressources financières constituent une caractéristique des citoyens.

Par ailleurs, des algorithmes contenus dans les produits de santé innovants pourraient, de manière biaisée, et non plus objectivement, identifier et viser des catégories de personnes sur d'autres critères, comme le genre, l'ethnie, la religion, la couleur de peau, l'appartenance sexuelle, *etc.* Les discriminations peuvent être nombreuses pour les patients. L'Union européenne, à travers sa Charte des droits fondamentaux, prohibe également les discriminations[41], basées sur quelques causes que ce soit.

Si l'utilisation d'un dispositif ou d'un médicament connecté est nécessaire pour maintenir la personne en vie, le sujet du dépassement de son refus pour intégrer les nouvelles technologies dans sa vie se pose[42]. La question des soins sans consentement lorsque celui-ci ne peut être recueilli, et de l'emploi de technologies innovantes pour mettre en place ces soins se posera nécessairement au corps médical dans les années à venir. Les juristes devront alors s'interroger sur les limites dans l'utilisation des produits et la responsabilité des professionnels de santé. De même, si un patient manifeste ou défend des positions anti-technologies, il conviendrait de s'interroger sur la possibilité pour lui de disposer d'un droit d'opposition et sur sa responsabilité dans l'hypothèse où l'usage de ces technologies serait déterminant pour sauver sa vie ou celle de la personne qu'il a sous sa responsabilité (mineur ou majeur protégé)[43]. Le débat sur la fin de vie[44] conduit à s'interroger sur la volonté et le droit de l'humain sur sa propre vie[45].

Cela amène à des discussions sur les dérives potentielles entraînées par les professionnels de santé dans l'exercice de leur pratique médicale améliorée par l'innovation scientifique et numérique afin d'éviter toute dérive d'eugénisme. Mais le recours à l'IA dans les soins et notamment dans la fin de vie peut conduire à des dérives, au choix qu'exercera l'IA forte de sauver ou non un patient en fonction des paramètres de l'algorithme de base de la machine. Au final, l'étendue de la responsabilité humaine porte sur la construction de la machine intelligente autonome. C'est la limite fixée et rappelée par Dunja Mijatović, commissaire aux droits de l'homme, dans son intervention du 3 juillet 2018 au Conseil de l'Europe :

« Les États devraient veiller à ce que le secteur privé, qui est responsable de la conception, de la programmation et de la mise en œuvre de l'IA, respecte les normes des droits de l'homme. La Recommandation sur les droits de l'homme et les entreprises et sur les rôles et les responsabilités des intermédiaires d'Internet, adoptée par le Comité des Ministres du Conseil de l'Europe, les Principes

(39) Conv. EDH 4 nov. 1950, entrée en vigueur le 3 sept. 1953.
(40) Protocole n° 12 à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 2000, entré en vigueur le 1er avril 2005.
(41) Charte des droits fondamentaux, art. 21, adoptée le 7 déc. 2000.
(42) C. Salas Toquero, *Le patient face à la technologie : Étude des déterminants de l'acceptabilité des technologies en santé*, thèse en psychologie clinique et psychopathologique, Université Grenoble Alpes, déc. 2018.
(43) Village de la Justice, *Procès du transhumanisme : la justice fait un bond dans l'avenir*, 8 juin 2020.
(44) Prop. de loi n° 131 (2020-2021) visant à établir le droit à mourir dans la dignité.
(45) Rapport fait au nom de la commission des affaires sociales sur la proposition de loi visant à établir le droit à mourir dans la dignité, par Mme Michelle Meunier.

directeurs relatifs aux entreprises et aux droits de l'homme, qui émanent de l'ONU, et le rapport sur la réglementation des contenus, élaboré par le Rapporteur spécial de l'ONU sur la promotion et la protection du droit à la liberté d'opinion et d'expression, devraient tous être pris en compte dans le cadre des efforts visant à faire en sorte que cette nouvelle technologie améliore notre quotidien. Il faudrait aussi augmenter la transparence des processus décisionnels utilisant des algorithmes, de manière que le raisonnement qui les sous-tend soit plus compréhensible, à ce que la responsabilité de ces décisions puisse être imputée à quelqu'un et à ce qu'elles puissent être contestées efficacement ».

## II. – Les dérives pour les professionnels de santé

Le droit met très souvent du temps à se saisir des questions complexes, et les nouvelles technologies connectées ne font pas exception. Un flottement juridique est inévitable pendant leur phase d'émergence, et permet de fixer les contours d'une future réglementation. En ce sens, le rôle des études d'impact préalables à l'adoption d'une nouvelle réglementation européenne n'est plus à démontrer[46].

Les établissements de santé, laboratoires de biologie et professionnels de santé sont particulièrement exposés à l'utilisation de nouveaux produits dotés de numérique et d'IA. L'évolution du secteur de la santé passe désormais incontestablement par l'utilisation d'outils dotés d'intelligences artificielles fondées sur des algorithmes capables d'analyser avec une extrême précision, et sur la base de considérables bases de données patients, l'évolution des pathologies. Toutefois, l'utilisation et le recours à ces outils peuvent conduire à d'importantes dérives lorsque la science va au-delà des limites acceptables au regard de l'éthique et de la déontologie médicale. Les longs débats sur la loi bioéthique en France en sont la représentation[47]. Les concepteurs d'intelligences artificielles (IA) peuvent être amenés à accepter de s'engager dans des études déraisonnables, ou des situations qu'ils savent contestables au plan éthique et juridique au regard des réglementations en cours de discussion. Cette question préoccupe l'Union européenne qui produit de nombreux rapports et études sur la question de la protection des droits fondamentaux de l'homme face à l'utilisation de l'IA[48].

En effet, en l'absence de tout texte ou jurisprudence, les concepteurs d'IA peuvent profiter de cet espace juridique pour collecter des données sensibles autres que celles qu'ils auraient dû recueillir, ou tester des dispositifs médicaux-médicaments connectés dans – ou sur – le corps humain. C'est la raison pour laquelle un projet de réglementation de l'intelligence artificielle (IA) a été présenté par les commissaires européens à Bruxelles le 21 avril 2021. Ce projet combine un « premier cadre juridique sur l'IA » et un « nouveau plan coordonné avec les États membres ». Dans son communiqué de presse, la Commission européenne annonce vouloir « garantir la sécurité et les droits fondamentaux des citoyens et des entreprises, tout en renforçant l'adoption de l'IA, les investissements et l'innovation dans l'ensemble de l'UE ». Ce règlement se fonde principalement sur les risques, créant

(46) É. Van den Abeele, *L'UE à l'épreuve du Mieux légiférer ; de l'urgence de changer de logique pour sauver le projet européen*, Bruxelles, ETUI, 2019.02 ; *Mieux légiférer : une simplification bureaucratique à visée politique*, Bruxelles, ETUI, Working Paper, 2015.04.

(47) L. n° 2011-814, 7 juill. 2011, relative à la bioéthique.

(48) Cons. UE, *Algorithmes et droits humains. Étude sur les dimensions des droits humains dans les techniques de traitement automatisé des données et éventuelles implications réglementaires*, 2017.

les catégories de risques inacceptables, élevés, limités et minimes. Les utilisations dans le secteur de la santé relevant des risques élevés, qu'il convient d'encadrer.

La situation est d'autant plus inquiétante que même s'il existe une réglementation, certaines entreprises tentent de la contourner soit en modifiant la présentation de leur produit, soit en délocalisant leur activité sur d'autres territoires soumis à des réglementations plus souples ou extensives[49].

Ces situations peuvent conduire les entreprises à se localiser sur des territoires à partir desquels seront déployées les activités du numérique en santé. Sans qu'il y ait là une pratique illicite, il n'en demeure pas moins que cette habileté juridique soulève des questionnements.

La captation des données est le plus gros risque, car elle représente une valeur considérable pour les entreprises, qui peuvent être tentées de les revendre pour augmenter leurs bénéfices. Les données représentent l'or actuel ; toutefois elles n'ont de réelle valeur que si l'entreprise a la capacité de les retraiter et de les analyser dans un objectif défini. Cette transformation représente la véritable valeur ajoutée des données de santé. La collecte des données par les professionnels de santé, au cours de leur exercice au profit de l'industrie dans le cadre de conventions de recherche ou d'études *in vivo*, représente un vecteur déterminant dans le succès du numérique en santé. Ainsi, les données captées par les plateformes de prise en ligne de rendez-vous médicaux sont considérables et contribuent au développement exponentiel des plateformes au point de les rendre indispensables et incontournables. Tel est par exemple le cas de Doctolib qui a joué un rôle déterminant dans la phase Covid-19, permettant la réalisation des actes de télémédecine, en accord avec les pouvoirs publics. Dès lors, les plateformes deviennent des partenaires des pouvoirs publics dans l'organisation du système de santé numérique[50]. Les médecins, et plus généralement les praticiens dans les établissements de santé publics et privés, sont donc particulièrement exposés aux nouvelles technologies dans l'exercice de leur activité. Non seulement les algorithmes collectent des données, mais ils les synthétisent également, pour aider le professionnel à prendre une décision sur un traitement, ou une opération[51]. Ils permettent aussi aux plateformes et industries des produits de santé de se développer dans l'offre de nouveaux services aux patients, créant de la valeur numérique en exploitant les données des patients qui eux-mêmes chercheront à valoriser leurs données. Cette question ouvre le débat sur la nature des données considérées comme des biens incessibles entrant dans le patrimoine de la personne.

Au-delà des questions relatives à la nature juridique des données de santé, notamment au niveau du droit européen, il convient de préciser que la méthode de collecte des données de santé et données personnelles du patient, au cours de l'acte de consultation et de diagnostic, implique une nouvelle approche de la relation entre le médecin et le professionnel. La méthode de collecte des informations permet de gagner du temps et d'être en principe plus efficace.

(49) Ministère de l'Économie, des Finances et de la Relance, avis, *Objets connectés santé et bien-être : sont-ils fiables ?*, 7 juill. 2017.
(50) France TV, *Covid : l'État s'associe à Doctolib pour la vaccination*, 1er janv. 2021.
(51) HAS, *Étude des systèmes d'aide à la décision médicale*, 12 juill. 2010.

Toutefois, la question est de savoir si l'information collectée au cours de l'entretien physique doit présenter les mêmes caractéristiques que celles collectées par la voie numérique. L'exemple de la vente par Internet de médicaments et du rôle du pharmacien dans l'acte de délivrance du médicament soulève des sujets de réflexion posés par l'Autorité de la concurrence considérant que les lourdeurs dans les questionnaires numériques représentent un déséquilibre économique et concurrentiel entre la vente en ligne et la vente sur site[52]. L'organisation de la collecte des informations du patient par Internet afin d'assurer au mieux l'acte de diagnostic ou de délivrance dans le respect des dispositions des codes de déontologie médicale ou pharmaceutique est un sujet lourd de conséquences pour le professionnel de santé.

Le véritable professionnel pourrait devenir l'algorithme ou le robot chirurgical[53] chargé de la décision de l'acte médical ou pharmaceutique. La télémédecine accroît ce phénomène de distance entre le patient et le professionnel[54]. Il pourrait y avoir un risque de déshumanisation du patient, qui ne serait pour l'algorithme qu'un numéro ou un ensemble de données. Une dérive que l'on pourrait également retrouver serait relative à la publicité ciblée[55]. En effet, une technologie qui aide un médecin à prescrire un traitement peut proposer les noms de certains médicaments en particulier. Il convient de s'assurer que ce médicament a été choisi par l'algorithme en toute objectivité, et non pas par une programmation bien définie du fabricant qui a des liens avec un laboratoire pharmaceutique. Cette preuve semble très difficile à rapporter, et la notion de confiance vis-à-vis de ces technologies devra être entière. Les industries de santé sont particulièrement vigilantes sur cette question de la promotion du produit et de l'incitation des professionnels de santé à la prescription des produits de santé, et se conforment strictement aux dispositions de la loi anti-cadeaux[56] et de la loi anticorruption[57] afin d'éviter les risques de sanctions financières et pénales. L'organisation de la promotion des produits de santé et produits connectés au sein des industries de santé représente un risque important, dans un contexte d'innovation mouvant. Le respect de ces dispositions vaut aussi pour les professionnels de santé soumis au risque de voir prononcer des sanctions lourdes financières et pénales.

L'impact fort et irréversible du numérique en santé, et donc des produits de santé connectés, des technologies numériques en santé, intelligences artificielles et algorithmes, implique inévitablement une révision des principes fondamentaux de la relation entre les acteurs de santé et les patients. L'information, le consentement libre et éclairé, la confiance sont des notions à redéfinir au fil

(52) Aut. conc., avis n° 19-A-D8, 4 avr. 2019, relatif aux secteurs de la distribution du médicament en ville et de la biologie médicale privée, reprises dans le projet de loi « ASAP ».

(53) A.-S. Fabas-Serlooten, *La responsabilité des robots : le médecin est-il remplaçable ?*, in *Le numérique et l'être humain*, Université Toulouse 1 Capitole, 13 oct. 2016.

(54) L. Tranthimy, *Déshumanisation, problèmes techniques, erreurs : la télémédecine ne fait pas carton plein : Le Quotidien du médecin* 27 janv. 2020.

(55) Sans Limites Marketing, *Publicité ciblée : le profilage algorithmique*, 11 août 2017.

(56) D. n° 2020-730, 15 juin 2020, relatif aux avantages offerts par les personnes fabriquant ou commercialisant des produits ou des prestations de santé.

(57) L. n° 2016-1691, 9 déc. 2016, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

de l'évolution numérique dans une conception agile du droit qui permet une adaptation constante des critères, tout en gardant fortement ancrés les principes fondamentaux de protection des libertés fondamentales, dont la protection de la vie privée, des données de santé et personnelles, du secret et de la confidentialité.

La redéfinition de ces notions permettra de répondre à la question de la valorisation des données et de leur exploitation par le patient lui-même. Le droit est une solution, et doit se présenter comme assez malléable pour prendre en compte la réalité au plus près, en intégrant comme périmètre les enjeux éthiques et moraux.

SECTION 2

## LES DIFFICULTÉS RELATIONNELLES ENTRE LE DROIT, L'ÉTHIQUE ET LA MORALE

L'état actuel de notre droit est très riche, permettant de s'adapter, de comprendre la majorité de notre environnement et de connaître les conséquences des actions de chacun. Cependant, dans des domaines très récents, notamment le numérique couplé à la santé, il convient de remarquer un manque d'encadrement. L'OMS, au travers de divers rapports, précise les objectifs à atteindre par les États et, notamment, de construire un environnement juridique et réglementaire efficace permettant d'assurer le développement du progrès, dans le respect des droits des utilisateurs. Cet équilibre délicat est fragilisé par les divergences d'approche qui se dégageront des analyses nationales des États signataires. Au sein de l'Union européenne, une approche harmonisée de la santé numérique a pour ambition de permettre, d'associer la vision de l'innovation et la protection des patients dans un objectif de progrès de la société autour du respect de l'éthique et de la déontologie. Ces objectifs sont en permanence bousculés. Il ne suffit pas de les affirmer *a priori*, il convient de les redéfinir et de les faire évoluer au rythme de l'avancée scientifique et numérique. Or, le décalage entre la rapidité fulgurante du développement numérique et le temps de la loi est patent. Bien que le législateur européen, ou national, accélère le temps d'adoption des dispositions législatives et réglementaires, il n'en demeure pas moins une analyse du temps relative entre les secteurs d'innovations et juridiques. Le temps de la loi n'est pas le temps de la science, et c'est en vue d'assurer une réduction de ce fossé que l'approche du droit agile intégrant la relativité de ces dimensions peut apporter une réponse favorable.

En effet, en raison de ces décalages, de nombreuses difficultés se posent dans toutes les hypothèses d'encadrement juridique, notamment lorsqu'une IA est présente (§ 1). Des propositions visent à insérer dans le droit des notions d'éthique et de moralité, pour avoir une approche la plus réaliste possible (§ 2).

## § 1. – Une réglementation difficile des intelligences artificielles

Les médicaments[58], les dispositifs médicaux[59], les dispositifs médicaux connectés, dotés d'une IA, les robots intelligents ou *Internet of Things* (Iot)[60], la collecte des données de santé et données personnelles[61] sont réglementés par le droit de l'Union européenne, au travers de directives ou règlements. Plus généralement, le droit de l'Union européenne encadre le développement sectoriel de la santé, la vie des produits de santé, et leur exploitation. La confrontation des réglementations sectorielles et du droit primaire de l'Union européenne issu des traités, mais aussi la confrontation de ce droit dérivé sectoriel avec les principes de droit des affaires dans ses différentes branches traduisent une complexité importante dans l'analyse juridique du secteur de la santé. Cette difficulté s'accroît lorsque les produits sont liés ou intègrent une IA. Un flou juridique peut apparaître, si les réglementations sont complexes à combiner, contradictoires ou ambiguës.

Pour résoudre cette problématique, des propositions et des recommandations de l'Union européenne ont été émises pour réglementer l'IA. En ce sens, les députés européens ont adopté trois résolutions pour guider la Commission européenne dans sa rédaction de futures réglementations relatives à l'IA[62]. Les préconisations sont fondamentalement de placer l'humain au cœur du système d'IA.

De plus, l'Agence des droits fondamentaux de l'Union européenne a rendu un rapport[63] ou elle essaye de proposer des solutions pour réglementer les IA et limiter leurs dérives, notamment celles relatives aux discriminations imputables aux IA.

Toutes les nouvelles technologies, en particulier celles connectées, ont des enjeux bien spécifiques que la réglementation se doit d'aborder. En revanche, certaines catégories parmi ces technologies soulèvent de nombreuses interrogations quant à leur encadrement juridique[64].

C'est notamment le cas des IA et des *deep learning* associées. L'un des enjeux est de savoir comment réglementer l'IA, alors qu'il semble très difficile d'encadrer une réalité abstraite, en particulier s'il s'agit d'une IA *deep learning*. Ces nouvelles technologies dotées d'IA, sous un format numérique, évoluent en permanence en s'appuyant sur leurs propres erreurs pour ne plus les reproduire ensuite. Il s'agit ici d'IA forte qui va prendre des décisions par elle-même. Toutefois, bien qu'auto-apprenante, cette IA a, à l'origine, été conçue sur la base d'un algorithme dont les critères ont été choisis par les concepteurs humains. La question de la responsabilité de l'IA et de l'humain est la problématique à résoudre d'ores et déjà pour les années à venir. En effet, ces décisions de l'IA peuvent engendrer des erreurs particulièrement

(58) Code communautaire du médicament, PE et Cons. UE, dir. 2001/83CE, 6 nov. 2001.
(59) *Cybersécurité : de nouvelles exigences pour les fabricants de DM connectés : Devicemed* 9 janv. 2018.
(60) PE et Cons. UE, règl. n° 2017/45, 5 avr. 2017.
(61) Règl. (UE) n° 2016/679, 27 avr. 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.
(62) PE, « Résolution contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes », 20 oct. 2020.
(63) Agence des droits fondamentaux de l'UE, *Bien préparer l'avenir : l'IA et les droits fondamentaux*, 13 déc. 2020.
(64) B. Bévière et D. Dibie, *Cour de cassation, Numérique : Droit et société* 23 janv. 2020.

dommageables pour les utilisateurs et les patients. Il est, en conséquence, indispensable que le droit prévoie des règles précises, prévisibles, mais évolutives permettant d'assurer une réparation efficace du préjudice subi par les victimes.

Les IA dites « faibles », appelées aussi *machine learning*, comme les suggestions proposées par des moteurs de recherche selon les termes utilisés ou les sites visités par les utilisateurs, ne posent en pratique quasiment pas de problème juridique nouveau[65]. Les IA faibles sont développées depuis de longues années dans de nombreux domaines, et notamment sont omniprésentes dans l'organisation de l'utilisation d'Internet, et le e-commerce. Les smartphones, tablettes, robots sont chargés d'applications fondées sur l'IA faible. Dans le secteur de la santé, ces outils numériques sont largement utilisés et permettent d'améliorer considérablement la relation de santé et la qualité des soins. La plupart des questions juridiques ont été approchées concernant l'IA faible, mais il reste néanmoins celle de la protection des données de santé dans un contexte de risque renforcé de piratage et cybercriminalité.

La vraie problématique actuelle repose sur les IA fortes, *deep learning*, autoapprenantes, qui évoluent et progressent à un rythme exponentiel. Il serait donc intéressant de se concentrer sur les potentielles approches juridiques envisageables pour réglementer les IA apprenantes, ayant un pouvoir décisionnel autonome.

En ce sens, il conviendra d'analyser les différentes possibilités d'encadrement juridique des IA (I), pour ensuite se pencher sur les éventuelles responsabilités invocables par la victime pour être indemnisée (II).

## I. – Les propositions d'encadrement juridique des intelligences artificielles fortes

Le nouveau livre blanc de l'Union européenne trace des lignes directrices pour réglementer les intelligences artificielles[66]. L'un des objectifs est de rendre assez maniable ce livre blanc, d'essayer de rendre sa modification assez malléable pour l'adapter aux évolutions permanentes des IA. Cet objectif doit être couplé à la structure même de l'Union européenne, à savoir vingt-sept États membres qui prennent ensemble des décisions. Il faut donc parvenir à une réglementation applicable, modulable rapidement pour prendre en compte en temps réel les besoins d'encadrement concernant les intelligences artificielles.

Le transhumanisme, courant de pensée philosophique promouvant l'amélioration de l'être humain, tant sur ses capacités physiques, qu'intellectuelles, est évidemment favorable au recours accru des intelligences artificielles fortes[67]. Selon ce mouvement, un *corpus* juridique peut être un rempart contre les atteintes à la dignité, et à l'inviolabilité du corps humain par les nouvelles technologies connectées. Il est cependant possible d'émettre des doutes sur ce *corpus* juridique. L'une des questions soulevées est de savoir comment le mettre en œuvre, être sûr qu'il

(65) Étude du Conseil de l'Europe DGI (2019)05, *Responsabilité et IA*, 2019.
(66) Comm. UE, Livre blanc *Intelligence artificielle*, 19 févr. 2020.
(67) Haas-avocats, *Le Transhumanisme : futur de l'Homme ?*, 19 avr. 2017.

soit complet, ou l'adapter dans une temporalité la plus faible possible par rapport aux innovations ou risques présentés par les intelligences artificielles.

La réglementation des IA apparaît extrêmement compliquée, mais elle est indispensable[68]. Cette nécessité s'impose d'autant plus en cas de survenance d'un dommage, lié d'une façon ou d'une autre à une IA. La victime doit avoir un droit à réparation et à indemnisation.

L'une des réponses pourrait être de réglementer l'IA en tant que nouvelle catégorie juridique, avec une personnalité juridique distincte de toutes celles existantes. La création d'une nouvelle entité juridique avec la personnalité juridique, pour réglementer les intelligences artificielles, peut être une solution à la difficile réglementation de ces nouvelles technologies.

L'une des idées avancées serait de créer une troisième catégorie ayant la personnalité juridique[69] : les personnes physiques, les personnes morales et la nouvelle catégorie de « personne » regroupant les intelligences artificielles et robotiques. Il faudrait alors se pencher sur la dénomination de cette troisième catégorie : personne artificielle, robotique, intelligente… De nombreuses possibilités sont admissibles. Néanmoins, certains auteurs de la doctrine considèrent cela comme un dédouanement des fabricants, qui verraient leurs responsabilités hors de portée[70].

D'un autre côté, il est aussi possible de se pencher sur une solution moins contraignante que la création d'une troisième catégorie de personnes ayant la personnalité juridique. En ce sens, il est possible de s'interroger sur la création d'un statut spécifique ou hybride entre les personnes et les biens pour intégrer les intelligences artificielles[71]. Cette situation existe pour les animaux, bien qu'elle soit, dans les faits, symbolique, l'animal restant pour son régime juridique un bien[72]. Évidemment, si une telle option est choisie pour réglementer les IA, la création de ce statut devra être optimale et permettre une véritable différenciation entre le régime juridique des personnes et celui des biens[73].

Une solution a été avancée dans une proposition de résolution du Parlement européen pour que soit créée une personnalité juridique spécifique aux robots[74], pour que les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques dotées de droits et de devoirs, et qu'ils puissent réparer tout dommage causé à un tiers. En ce sens, serait considéré comme une personne électronique tout robot qui aurait la capacité de prendre des décisions de manière autonome et intelligente ou qui interagirait de manière indépendante avec des tiers.

(68) T. Doh-Djanhoundy, *Le statut juridique de l'intelligence artificielle en question*, University Félix Houphouët-Boigny, nov. 2019.
(69) *Faut-il une personnalité juridique propre au robot*, Master 1 IP/IT, Faculté Jean Monnet, Université Paris Saclay, 2 mars 2018.
(70) *Il faut prendre l'humanoïde pour ce qu'il est : une machine*, Entretien avec N. Nevejans, Maîtresse de conférences en droit privé à l'Université d'Artois : Philonomist.com, 17 sept. 2019.
(71) G. d'Arcy et C. Martin, *Quand l'intelligence artificielle vous soigne : quelle(s) responsabilité(s) ?*, EDHEC Business School, LL.M. Law & Tax Management, 7 juin 2019.
(72) Déclaration universelle des droits de l'animal, 15 oct. 1978.
(73) Village Justice, *La protection juridique des œuvres créées par l'IA*, 23 juin 2020.
(74) Parlement européen, rés. 16 févr. 2007.

L'interaction entre la personne robot et le professionnel de santé devra donc être analysée afin d'identifier la répartition de responsabilité. Le médecin ayant recours aux outils numériques sera tenu par des obligations dont la violation entraînera sa responsabilité. La responsabilité des médecins du service public, des médecins salariés d'établissement privé ou des médecins libéraux est analysée sous l'angle des responsabilités contractuelle et délictuelle selon les actes réalisés.

La loi n° 2002-303 du 4 mars 2002 pose le fondement de la responsabilité médicale qui est devenue délictuelle selon l'article L. 1142-1 du Code de la santé publique :

« I. – Hors le cas où leur responsabilité est encourue en raison d'un défaut d'un produit de santé, les professionnels de santé mentionnés à la quatrième partie du présent code, ainsi que tout établissement, service ou organisme dans lesquels sont réalisés des actes individuels de prévention, de diagnostic ou de soins ne sont responsables des conséquences dommageables d'actes de prévention, de diagnostic ou de soins qu'en cas de faute… ».

Cet article renvoie à la faute délictuelle, nous permettant d'appliquer au domaine médical les articles 1240 et suivent du Code civil.

Les médecins et les infirmiers ont l'obligation déontologique de s'assurer de la fiabilité du matériel qu'ils utilisent. Ils sont tenus par une obligation de sécurité de résultat en ce qui concerne le matériel utilisé.

La première chambre civile de la Cour de cassation, dans un arrêt n° 98-10.010 du 9 novembre 1999, précise que « le contrat formé entre le patient et son médecin met à la charge de ce dernier une obligation de sécurité de résultat en ce qui concerne les matériels qu'il utilise pour l'exécution d'un acte médical d'investigation ou de soins ». Il faut savoir qu'il appartient au patient de prouver que ces matériels sont à l'origine de son dommage.

Lorsqu'est en cause une défectuosité du matériel, la responsabilité du fournisseur sera engagée dans le cadre d'une obligation de sécurité de résultat. Il appartient à ce dernier d'exercer une action récursoire contre le producteur. Ces recours sont gérés par le biais des assureurs en responsabilité civile. Le régime, lié à la qualité du matériel, permet d'engager la responsabilité personnelle de toutes les personnes intervenant dans la chaîne des outils informatiques et des technologies. Le professionnel de santé doit aussi s'assurer d'une maîtrise de l'outil qu'il manœuvre, et il doit pouvoir disposer de contacts permettant de joindre des informations professionnelles en cas de défaillance. Enfin il doit, dans le cadre des soins effectués, s'assurer de la compétence et de la disponibilité des professionnels. Le patient peut invoquer la perte de chance sur le fondement de l'obligation de solliciter l'avis de tiers compétents en cas de doute sur le diagnostic médical ; cette obligation est instaurée par le Code de déontologie médicale[(75)].

Lorsque le professionnel médical dispose du moyen de la télémédecine, il doit s'en servir et la proposer pour faciliter l'accès aux soins, et notamment pour pratiquer une téléconsultation chez des patients handicapés se trouvant en difficulté pour effectuer un déplacement jusqu'à son cabinet, au nom de l'éthique de bienfaisance et de justice. Lorsqu'une organisation professionnelle et des moyens

(75) C. santé publ., art. R. 4127-60.

technologiques le permettent, une télésurveillance médicale au domicile du patient atteint de maladie chronique peut être organisée. Le médecin doit participer et se coordonner avec les autres professionnels de santé impliqués dans la pratique de la télémédecine afin de prévenir les hospitalisations et les venues aux urgences, souvent génératrices d'aggravation de la maladie et de perte de chance pour le patient(76).

Selon les hypothèses envisagées, les actions en responsabilité pourront différer. En effet, si aucune personnalité juridique n'est reconnue à l'IA qui a causé un dommage, aucune action contre cette même entité n'est envisageable. Il convient donc de s'interroger sur les diverses responsabilités qui pourraient être envisageables pour la victime ayant subi un dommage du fait d'une action ou décision d'une IA contre le fabricant, le concepteur du programme, le titulaire de la plateforme numérique, ou encore l'utilisateur, professionnel de santé en charge de la surveillance et de l'évaluation des résultats proposés par l'IA. Un régime de responsabilité conjointe ou solidaire pourrait être envisagé entre ces acteurs. Cela pose très clairement la question de la capacité des professionnels de santé à détecter les risques d'erreur fondés notamment sur la conception biaisée de l'algorithme de départ. Le sujet de la responsabilité ne fait que commencer avec l'évolution et la complexité des IA apprenantes, et la croissance du *deep learning*. Le recours aux IA dopées par les ordinateurs quantiques avec une capacité d'analyse démultipliée rendra d'autant plus complexe la question de l'identification des responsabilités. Elle pose en amont la question fondamentale de la formation du professionnel de santé à l'utilisation de l'IA, à son maniement et à la connaissance de ses limites dans l'organisation de la prise en charge du patient. L'évolution vers la médecine « 6P » suppose donc une formation des professionnels sur les risques et responsabilités qu'ils encourent.

## II. – Les diverses responsabilités envisageables

Il y a une question primordiale sur la responsabilité qui se pose en cas de préjudice causé par une intelligence artificielle, à savoir qui est le responsable du préjudice si un utilisateur ou un tiers subit un préjudice du fait de l'utilisation ou de la prise de décision d'une nouvelle technologie apprenante.

Une IA, tel un robot chirurgical, ou un algorithme prenant des décisions à la place des praticiens, peut commettre une faute qui pourra entraîner un effet indésirable grave, très grave, voire le décès d'un patient.

La question de la responsabilité des IA est très ardue, à tel point que la cour d'appel de Paris, dans un rapport du 25 juin 2019, a écarté l'hypothèse d'une régulation des intelligences artificielles dans le cadre de la réforme de la responsabilité civile(77).

En premier lieu, la responsabilité de l'IA elle-même semble difficile à déterminer. Il faudrait pouvoir reconnaître la personnalité juridique à l'IA, ou créer un régime juridique hybride correspondant aux IA.

(76) P. Simon, *Télémédecine, santé connectée, éthique numérique : enjeux de la médecine au XXIe siècle*, in *Santé, numérique et droit-s* (ss dir. I. Poirot-Mazères), PU Toulouse 1 Capitole, 2019, p. 143 à 144.
(77) CA Paris, Rapport *Réforme de la responsabilité de et intelligence artificielle*, Lamyline, 25 juin 2019.

Mais, une fois levé cet obstacle de l'identification du régime de responsabilité de l'IA, reste la question centrale de l'application des sanctions. En effet, en l'état actuel du droit positif, les sanctions financières sur le plan civil ou administratif, les sanctions pénales impliquant une amende ou une peine d'emprisonnement ne sont pas adaptées pour une IA. Celle-ci n'a pas de personnalité juridique, et, en conséquence, n'a pas de patrimoine propre, et ne peut pas être détenue physiquement, sauf s'il s'agit d'un robot intelligent. Le régime de la responsabilité du propriétaire de la chose, du gardien de la chose au sens du droit des obligations générales ne saurait s'appliquer sans adaptation à la spécificité de l'IA dès lors qu'elle dispose d'une autonomie d'analyse et de déduction au-delà de la volonté humaine du concepteur, et dès lors qu'elle dépasse les capacités d'analyse humaine, voire emprunte des chemins d'analyse et d'expression entre IA qui sont incompréhensibles par les concepteurs et utilisateurs. La capacité des IA à échanger entre elles, à partir des données auto-apprises hors de la compréhension humaine, pose une grave question concernant l'identification du responsable et l'application du régime de responsabilité. En tant que telle, l'IA ne saurait être sanctionnée ; quant aux concepteurs et utilisateurs, il est illusoire de pouvoir engager leur responsabilité dès lors que la décision autonome de l'IA qui a porté préjudice au patient est hors de leur champ de connaissance et compréhension. Il serait possible d'envisager une coupure temporaire ou un arrêt définitif de l'IA en question, avec tous les risques que cela pourrait entraîner pour l'ensemble des utilisateurs patients et professionnels dès lors que l'IA s'est imposée comme centrale dans l'accompagnement, la prévention et le traitement du patient. La technologie numérique pourrait alors être débranchée, mise hors service. Ceci apporterait une solution technique et permettrait de rétablir l'identification des responsabilités des concepteurs ou titulaires des plateformes numériques ou utilisateurs, portant sur la maîtrise de la mise en fonctionnement de l'IA. Toutefois, cette solution radicale n'est pas satisfaisante, ni pertinente. Elle n'apporte, par ailleurs, pas de réelle possibilité de réparation ou indemnisation de la victime faute de démonstration de la faute commise par l'IA.

La seule solution possible pour obtenir une réparation financière du dommage est la création d'un fonds d'indemnisation pour les victimes. En ce sens, si la responsabilité d'une IA est retenue, en raison d'une faute matérielle ou dans sa prise de décision, la victime sera indemnisée par le fonds d'indemnisation. Ce régime d'indemnisation par l'Office national d'indemnisation des accidents médicaux (ONIAM) est calqué sur celui existant concernant les affections nosocomiales et aléas thérapeutiques. Il permet d'indemniser le patient alors même qu'aucune responsabilité ne peut être identifiée de la part des différents acteurs de santé.

Avant la loi du 4 mars 2002, les assureurs étaient amenés à indemniser des préjudices de plus en plus nombreux. Il fallait trouver un moyen d'indemnisation au titre de la solidarité nationale pour certaines maladies et pour certaines situations. L'article L. 3122-2 du Code de la santé publique pose un régime favorable à la victime. Une fois l'ONIAM saisie d'un dossier, elle va constituer un collège d'experts, qui a pour rôle de déterminer si le demandeur est en droit d'obtenir une indemnisation par l'ONIAM.

L'analyse de la responsabilité des acteurs, à savoir l'utilisateur, le patient ou le professionnel, doit être décortiquée afin d'identifier les éléments qui ont pu être à l'origine du dommage. La situation la plus fréquente est celle où un médecin utilise, ou a recours à un appareil robot, ou logiciel doté d'IA auto-apprenante, qui va causer un dommage à un patient du fait de la décision qu'il aura prise. Le patient sera la victime et le professionnel de santé sera extérieur à la décision prise par l'IA d'utiliser la technologie dans l'indication thérapeutique pour ce patient. Il convient alors de décortiquer les phases de la prise de décision et d'identifier le moment à partir duquel le professionnel de santé cède la décision à l'IA, hors de son contrôle. Sur ce point, la jurisprudence portant sur la réparation des préjudices liés à l'utilisation d'un véhicule autonome dotée d'une IA est intéressante à explorer. Il convient d'ajouter à cette analyse concernant l'autonomie des véhicules le rôle du professionnel de santé qui doit demeurer libre de sa décision à l'égard du patient, et l'on ne peut en aucune manière soumettre sa décision à une influence extérieure. Il conviendra donc de vérifier la capacité du professionnel de santé à maîtriser la décision prise par l'IA dans un bon état de compréhension des critères de la décision, ce qui suppose pour le professionnel une formation suffisante pour comprendre les modalités de la décision algorithmique selon sa conception, et donc à détecter les risques de biais d'interprétation.

En conséquence, la responsabilité du professionnel de santé pourra porter sur un défaut ou une insuffisance de formation dans l'apprentissage et l'utilisation de l'IA. C'est ce défaut de formation qui constituera le fondement de la mise en cause de sa responsabilité, en se basant sur la jurisprudence existante en la matière tant sur le plan civil et pénal en cas de mise en danger de la personne, qu'au plan déontologique devant le Conseil de l'Ordre des médecins[78].

Par ailleurs, la responsabilité du professionnel de santé pourra dépendre des modalités d'utilisation de l'objet connecté ou robot doté d'une IA. Par utilisation correcte de la technologie numérique, il convient d'entendre un usage conforme à la destination prévue par le fabricant et le concepteur de l'IA. Il convient alors de s'appuyer sur un régime de responsabilité pour faute, et d'identifier la faute, le préjudice et le lien de causalité, avec toutes les difficultés portant sur la caractérisation de ce lien. La jurisprudence sur le sujet est extrêmement abondante, notamment concernant les produits de santé tels que les médicaments ou dispositifs médicaux. Il est alors tout à fait possible d'étendre ce régime de responsabilité aux seules situations concernant les revendications d'utilisation du produit et précautions par le fabricant. Dans ce cas, il conviendra d'identifier les cas d'utilisation du robot, l'opportunité du choix thérapeutique, mais non les décisions adoptées par l'IA. Il est aussi possible de se fonder sur un régime de responsabilité sans faute tel que prévu à l'encontre des établissements de santé, utilisateurs de dispositifs médicaux[79]. Dans cette hypothèse, l'établissement de santé ou le professionnel de santé verra sa responsabilité engagée dès lors qu'une IA est en cause et qu'un préjudice peut être relevé pour le patient. Ce régime permet une indemnisation rapide

(78) C. santé publ., art. L. 4121-2.
(79) CE, 29 mai 1995, n° 143238, *N'Guyen*.

du patient et les acteurs de santé pourront agir contre le fabricant ou le concepteur du produit doté d'IA, mais avec le risque qui pourrait leur être opposé de non-conformité dans l'utilisation du produit.

En effet, en application du droit commun des obligations et de la responsabilité, s'il y a une mauvaise utilisation par l'utilisateur, professionnel de santé, non conforme aux prescriptions du fabricant et qu'un dommage est causé, alors la faute de l'utilisateur doit pouvoir être retenue. En conséquence, le tiers à l'utilisation, le patient victime, aura droit à exercer une action en réparation afin d'obtenir une indemnisation.

Dans ces hypothèses, la démonstration de la non-conformité ou de la faute dans l'utilisation du produit sera particulièrement complexe à définir, et visera principalement les aspects matériels et techniques dans la mise en œuvre ou l'interruption d'utilisation du produit ou robot intelligent. Elle ne pourra pas porter sur la décision prise par l'IA qui reste hors de sa capacité de contrôle, sauf à retenir une responsabilité sans faute de tous les utilisateurs de robots dotés d'IA[(80)].

Le règlement « DM » prévoit les conditions et modalités de mise en cause de la responsabilité du fabricant et du fournisseur des produits dotés de l'IA ayant requis la qualification de DM. Le règlement va permettre de traiter l'ensemble de ces situations sur le plan réglementaire, ce qui n'exclut pas l'action en responsabilité contre le fabricant sur le fondement du droit commun.

D'autres scénarios peuvent survenir, par exemple si le dommage est causé par des produits dotés d'IA à l'utilisateur lui-même. Cela peut survenir dans le cas où, par exemple, un chirurgien aidé par un robot intelligent va être blessé par ce dernier, passé hors de son contrôle ; l'application du régime de responsabilité devrait conduire à rechercher la responsabilité du fabricant ou du concepteur de l'IA afin d'appliquer le régime de responsabilité prévu notamment dans la directive sur les dispositifs médicaux logiciels. Le fabricant porte l'entière responsabilité[(81)].

Sur le plan du droit commun en France, la responsabilité du gardien de la chose pourra être recherchée.

Il est possible d'invoquer la responsabilité extracontractuelle sur le fondement des articles (C. civ., art. 1242 et s.), la responsabilité du gardien de la chose pourra toujours être mobilisée.

Cependant, lorsque la décision du produit doté de l'IA est autonome et hors du contrôle du gardien de la chose, il sera difficile d'invoquer la responsabilité du fabricant ou du fournisseur dès lors que le dommage commis provient d'un apprentissage autonome de l'objet intelligent. Dans ce cas de figure, pourra être invoquée la défectuosité du produit (C. civ., art. 1245).

Dans tous les cas, il convient de s'intéresser à la responsabilité du fabricant/inventeur de l'IA en question. Plusieurs responsabilités relatives au fabricant sont envisageables.

(80) Comm. UE, *Rapport sur les conséquences de l'intelligence artificielle, de l'Internet des objets et de la robotique sur la sécurité et la responsabilité*, 19 févr. 2020.

(81) F. Charlet, *Que se passera-t-il si un robot commet un crime ?* : https://francoischarlet.ch/categories/droit/, 24 juill. 2017.

Tout d'abord la responsabilité du fabricant du fait des choses (C. civ., art. 1242)[82]. Conformément à cette disposition, il y aurait bien un dommage, celui qui est subi par la victime, ou l'utilisateur.

Concernant la deuxième condition, la présence d'une chose, il s'agirait de l'IA *deep learning* ou d'un robot intelligent. Dans cette hypothèse, l'IA est assimilée à une chose, du moins pour son régime juridique. Si cette technologie acquiert un régime juridique propre, de par un nouvel encadrement juridique, alors l'assimilation à une chose devient inenvisageable et en conséquence la responsabilité du fait des choses est automatiquement exclue. En revanche, en l'absence de régime juridique distinct, ce qui est le cas dans l'état actuel du droit, alors l'IA peut être considérée comme une chose d'où l'application de l'article (C. civ., art. 1243).

La troisième condition est que la chose soit l'instrument du dommage. En pratique, cela est assez simple à concevoir. Il suffit que l'IA prenne une décision dommageable, ou blesse physiquement une personne s'il s'agit d'une entité physique.

Ces trois conditions pourraient être remplies. Le problème est relatif à la dernière condition : le fabricant doit être le gardien de la chose, soit de la nouvelle technologie intelligente. Pour cela, il doit en avoir l'usage, le contrôle et la direction[83]. Le fabricant de l'IA peut en avoir la direction, c'est-à-dire qu'il décide de la finalité de la chose. Cela peut encore être discuté puisque s'il s'agit d'une IA autonome, l'apprentissage est continu et perpétuel, et la finalité de la technologie peut tendre vers des résultats qui n'étaient pas prévus par le fabricant. En effet, l'IA autonome va peut-être orienter son apprentissage sur d'autres domaines que ceux initialement programmés. La notion de contrôle de la chose, qui correspond à la capacité du fabricant à prévenir le fonctionnement anormal de la chose, soulève des difficultés. Le fabricant est supposé savoir ce qu'il a créé, et doit être capable de l'arrêter en cas de problème. On peut estimer que le fabricant d'une IA autonome est capable de reprogrammer son invention, de l'arrêter si elle a un fonctionnement anormal, ou en dehors des finalités qui lui ont été assignées. Mais il faut pouvoir savoir quand l'IA a un comportement anormal. L'objectif de ce type de technologie est continuellement à apprendre, au-delà de la compréhension humaine. La question sera alors de savoir si l'intervention humaine est justifiée dans la décision d'interrompre ou modifier l'usage de l'IA. Cela suppose de définir avec clarté les objectifs à atteindre par l'IA, et renvoie à des questions éthiques et déontologiques. Ce sujet a notamment été soulevé dans le cas d'utilisation de robots intelligents dans les conflits armés ou encore dans la mise en circulation des véhicules intelligents. Toute la question sera de savoir comment limiter son invention quand celle-ci va trop loin au regard de ces limites éthiques, ou parvenir à le reprogrammer sans perdre tout l'apprentissage déjà réalisé.

Enfin, se pose la question de l'application du régime de la responsabilité du fabricant du fait des produits défectueux (C. civ., art. 1245 et s.)[84]. Cependant, afin de pouvoir mobiliser ce fondement juridique, il faut être en présence d'un produit. Or,

(82) C. civ., art. 1242 ; Ord. n° 2016-131, 10 févr. 2016, art. 2.
(83) Cass. ch. réunies, 2 déc. 1941, *Franck*, publié au bulletin.
(84) C. civ., art. 1245 à 1245-17 ; Ord. n° 2016-131, 10 févr. 2016, art. 2.

un produit ne correspond pas à la définition d'une chose. Le produit doit être un bien meuble, ce qui n'est pas le cas d'une IA autonome. Si l'on est en présence d'un robot, effectivement il s'agit d'un meuble. En revanche, concernant un algorithme auto-apprenant, la réponse est moins évidente, il pourrait entrer dans la définition de meuble incorporel[85].

Le point conflictuel repose sur la sécurité à laquelle on peut légitimement s'attendre. Les IA autonomes apprennent de toutes les situations auxquelles elles sont confrontées, notamment de leurs propres erreurs. Elles peuvent donc très probablement faire au minimum une erreur. Une erreur qui pourrait causer un dommage à une personne. Mais cette erreur n'entraîne pas forcément la défectuosité de l'IA. Cette dernière sera seulement dans son usage normal : un apprentissage permanent. Bien que l'on puisse considérer que les IA sont dangereuses sur ce point, il faut rappeler que la dangerosité n'induit pas nécessairement le défaut. La dangerosité ne s'apparente pas à la défectuosité du produit. En ce sens, il est tout à fait possible, au sens des dispositions du règlement sur les dispositifs médicaux contenant un logiciel, d'appliquer les règles relatives à la précaution concernant la matériovigilance, fondée sur la notion de risques du produit liés à sa dangerosité, sans pour autant considérer le produit comme défectueux. En revanche, la défectuosité du produit suppose de démontrer le vice dans la construction de l'IA. La responsabilité du fait des produits défectueux semble donc difficilement envisageable.

La dernière hypothèse, et la plus probable, réside dans la mobilisation des dispositions issues du règlement sur les dispositifs médicaux implantables (DMI) ou non implantables contenant une IA. Le règlement « DM » met en avant la responsabilité du fabricant[86].

En cas de défectuosité du matériel, la personne lésée peut mettre en cause la responsabilité du fabricant des DM, implantables ou non implantables, dotés d'une IA. En cas d'une défaillance du DMI qui aurait causé un accident sur la personne du patient, c'est sur le terrain de la défectuosité d'un appareil, et donc un recours à la responsabilité du fait des produits défectueux serait envisageable sur le fondement de l'article (C. civ., art. 1245-17). Le patient victime de la défectuosité du DMI doit prouver l'existence du dommage, le défaut du produit et le lien de causalité entre les deux. Il est préconisé pour le patient victime de la défectuosité du DMI de conserver ce dernier pour le cas où une expertise serait nécessaire, et de faire une alerte matériovigilance, mais de ne jamais retourner au fabricant le DMI mis en cause. Il s'agit d'une faveur pour la victime d'un défaut de produit de santé qui pourra agir à l'encontre du producteur ou du distributeur. La défectuosité permet de mettre en cause la responsabilité de toute personne intervenant dans la chaîne de fabrication jusqu'à la distribution des produits de santé dotés de l'IA.

Cela étant, afin d'assurer une réparation du préjudice subi par le patient, il conviendrait de créer une responsabilité spécifique aux IA, permettant une indemnisation des victimes. La création d'un fonds d'indemnisation semble être une bonne piste, mais ne peut pas être l'unique solution. Il faudra à l'avenir songer à instaurer

(85) J. et A. Besoussan, *IA, robots et droit*, éd. Lexing, 2019.
(86) Règl. (UE) n° 2017/745, relatif aux dispositifs médicaux.

un véritable cadre juridique pour ces nouvelles technologies dotées d'IA. Les avancées de la Commission européenne sur ce sujet devraient permettre l'adoption d'une réglementation européenne portant sur l'IA et les responsabilités y afférentes.

L'insertion de l'éthique et de la morale[87] pourraient potentiellement être associées pour faciliter la création d'un cadre juridique.

## § 2. – Une réglementation incluant l'éthique pour une meilleure protection des données de santé

Le numérique a révolutionné notre société, en basant l'ensemble des relations sur des interactions virtuelles. L'ennemi n'est plus une personne visible, mais est devenu invisible, insaisissable, imprévisible. Dans ce contexte totalement insécurisant, la redéfinition des contours de la confiance et du consentement est fondamentale. Les bases éthiques et morales qui sont à l'origine de ces notions devront, dans ce nouvel univers, à l'échelle planétaire, être repensées[88]. Or, l'approche éthique du consentement et de la confiance diffèrent profondément d'un territoire à un autre et impliquent une harmonisation, à tout le moins au niveau de l'Union européenne, afin d'assurer un niveau minimal élevé de protection des droits des citoyens européens, notamment le domaine de la santé révélé comme un point fondamental depuis le début de la crise Covid-19. Bien qu'il ait permis une avancée considérable, et place la société entière à l'aube d'une nouvelle ère assurant une considérable amélioration de la santé individuelle et collective, le numérique est aussi source de risques en ce qu'il permet un traçage permanent et une identification complète de la personne, de son mode de vie, ses fréquentations, ses activités, ses pathologies et permet la captation de l'ensemble de ses données de santé et personnelles. Les objets connectés de bien-être, de santé, de traitement ou de soins sont exposés de plus en plus fortement aux risques de piratage et cybercriminalité posant la question de la protection des données et de la vie privée des citoyens.

En conséquence, les gouvernements se doivent de prévoir une législation protectrice des patients (I).

Cette protection juridique doit également s'étendre à la problématique du secret médical dans le partage de ces données et à celle de la neutralité des intelligences artificielles, afin d'éviter les formes d'exclusions (II).

### I. – Une protection juridique nécessaire au patient

Le règlement général sur la protection des données (RGPD) du 27 avril 2016[89] définit le consentement comme étant : « toute manifestation de volonté, libre,

(87) Version abrégée de J.-P. Cobbaut et P. Boitte, *Pour une éthique de l'allocation des ressources en santé : les enjeux de l'accès aux soins*, in *Éthique publique* 2003, vol. 5, n° 1, p. 15-34.

(88) J. Béranger, *La valeur éthique de la donnée de santé à caractère personnel : vers un nouveau paradigme de l'écosystème médical dématérialisé : Sciences de la société* 95-2015, 91-105.

(89) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 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, dit « règlement général sur la protection des données ».

spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[90]. Cette disposition n'a fait que confirmer la position adoptée par la loi Informatique et Libertés du 6 janvier 1978[91].

Selon la Commission nationale de l'informatique et des libertés (CNIL), pour qu'un consentement puisse être valablement recueilli, quatre critères cumulatifs doivent être remplis. L'un des critères essentiels est le consentement éclairé qui oblige le responsable du traitement des données à une obligation de transparence[92].

Le développement des technologies de santé s'est accompagné de nombreuses demandes d'accès aux données de santé des utilisateurs. Pour autant, l'utilisateur doit faire preuve de vigilance, car ce sont des données sensibles qui relèvent de sa vie privée. Les données de santé sont devenues « l'or noir du numérique ».

Comme le rappelle le Comité consultatif national d'éthique (CCNE), dans un avis de 2019, l'enjeu principal est de trouver « le bon équilibre entre le risque d'une sous-exploitation des données limitant des recherches menées dans l'intérêt général et celui d'un partage des données trop large et insuffisamment contrôlé mettant en cause les droits fondamentaux de la personne »[93]. Par ailleurs, ce comité n'a pas hésité à rappeler que l'utilisation de technologies types hors soins revêt un risque en matière de protection des personnes. C'est pourquoi une démarche de responsabilisation des acteurs est nécessaire.

Pour autant, l'utilisateur peut revenir sur le consentement qu'il a émis. Un droit à l'effacement est prévu par le RGPD[94]. Dès le retrait de son consentement, l'utilisateur peut faire valoir ce droit à l'oubli[95]. Encore faut-il qu'il comprenne et ait conscience de cette possibilité d'exercer ce droit. Ceci sera d'autant plus difficile que le produit en question est un dispositif médical doté d'une IA qui lui est essentiel dans le cadre du traitement de sa pathologie. La difficulté est accrue lorsque ledit dispositif est implanté et collecte des données ou lorsque le produit est un médicament connecté. C'est à ce stade que la confrontation des réglementations relevant des produits de santé, et celles relevant du régime général de la protection des données doit être bien analysée afin de savoir quelle est la règle applicable à tels ou tels produits. Ces produits spécifiques seront soumis à un encadrement réglementaire strict visant la protection de la personne et la sécurité du produit, des règles visant les objectifs des logiciels contenus dans les produits de santé.

Malgré toutes ces dispositions préventives, la responsabilisation des acteurs n'est pas gage de respect des dispositions légales[96]. C'est pourquoi la collecte des

(90) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016, consid. 11, 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 (RGPD), applicable depuis le 25 mai 2018.

(91) Loi Informatique et Libertés, 6 janv. 1978 mod. par L. n° 2018-493, 20 juin 2018, relative à la protection des données personnelles.

(92) PE et Cons. UE, règl. n° 2016/679, 27 avr. 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, art. 12, 13 et 14.

(93) CCNE, avis n° 130, 29 mai 2019, pour les sciences de la vie et de la santé.

(94) RGPD, art. 17.

(95) Treize décisions du 6 décembre 2019 ont été adoptées à la lumière de l'arrêt de la CJUE rendu le 24 septembre 2019.

(96) La loi de modernisation de notre système de santé du 26 janvier 2016 et la loi sur une République numérique du 7 octobre 2016.

données doit faire l'objet de contrôles. Le Conseil national de l'Ordre des médecins et la CNIL ont d'ailleurs publié un guide pratique sur le sujet en 2018[97], suivi de la publication de trois référentiels par la CNIL en 2020[98] et d'un guide pratique de conservation des données[99]. En outre, la valorisation excessive des données n'arrange en rien ce phénomène. En effet, non seulement la collecte des données représente un marché économique considérable pour les acteurs de santé ou du numérique dans le secteur de la santé, mais elle constitue aussi pour le patient lui-même une source d'enrichissement. En l'état actuel du droit de l'Union européenne, le patient ne peut négocier et valoriser ses données de santé, afin d'en assurer une activité lucrative source de revenus. Toutefois, dans les territoires hors UE, la valorisation des données par le patient est déjà un sujet en route. Hors UE, essentiellement aux États-Unis et en Chine, la problématique de la richesse et la valorisation de la donnée ne se posent donc même pas. En France, la question posée est centrale[100] et le législateur, dans les lois successives sur la santé, cherche à encadrer la maîtrise des données par la création du *hub* santé, qui permet de centraliser les données du patient et d'assurer leur protection sous le sceau du RGPD. L'État tente de se positionner comme acteur principal du recueil et de la valorisation des données de santé. En effet, hors de l'intervention de l'État, les acteurs seront dans l'incertitude sur les pratiques à mettre en œuvre pour capter et valoriser les données des patients. Ceci pourrait inciter les patients à expérimenter individuellement des pratiques d'utilisation des données par le rachat de données ou la capitalisation dans des entrepôts de données afin de pouvoir disposer de quantité suffisante pour la réalisation des phases de recherche et développement pharmaceutique par exemple. Les enjeux vertueux consistant à effectuer la recherche et les essais à partir de banques de données colossales, et donc de réduire les risques sur les cohortes vivantes, pourraient aussi être détournés dans des usages non éthiques. Cette prise de conscience des pouvoirs publics sur le risque de la manipulation des bases de données s'illustre dans le rapport publié par Cédric Villani sur l'intelligence artificielle et sur le *big data*[101]. La médecine algorithmique se développe très vite à partir du traitement massif des données et suppose un encadrement construit, mais agile, permettant à l'Union européenne et à la France de rester dynamiques sur le marché sans interdire totalement ces transferts et utilisation de données, mais en les encadrant. L'élaboration d'une réglementation trop stricte conduirait à une fuite de ces activités sur des territoires plus complaisants et, au final, à un retour de leur exploitation sur le territoire de l'UE. La compétitivité suppose donc d'assurer un réel encadrement agile permettant la protection dans la dynamique de l'innovation.

L'élaboration de ce *hub* santé pose la question de savoir s'il convient de prévoir un droit d'entrée pour accéder au *Health Data Hub* pour les acteurs qui souhaitent

(97) CNOM et CNIL, *Guide pratique sur la protection des données personnelles*, éd. juin 2018.
(98) Référentiel des durées de conservation dans le domaine de la santé hors recherche. Référentiel des durées de conservation dans le domaine de la recherche en santé. Référentiel relatif aux traitements de données personnelles pour les cabinets médicaux et paramédicaux.
(99) CNIL, *Guide pratique sur les durées de conservation*.
(100) L. Dusserre, *La commercialisation des informations médicales est-elle « déontologiquement correcte » ?*, Ordre national des médecins, Conseil national de l'Ordre, 29-30 juin 2000, 1-7.
(101) C. Villani, Rapport *Donner un sens à l'intelligence artificielle*, 28 mars 2018.

exploiter les données, s'il conviendra d'instaurer un caractère contraignant au recueil des données de santé auprès de tous les praticiens de santé et de toutes les structures de santé dont les hôpitaux. Plus généralement, la question posée est celle du rôle joué par l'État dans la création de ce *Health Data Hub*, dans sa relation notamment avec les acteurs économiques, en vue de la transformation et de la valorisation de ces données. Une vraie réflexion doit être aussi engagée sur le périmètre de l'action publique qui doit se cantonner à la régulation de l'écosystème. Selon une étude du Boston Consulting Group(102), les données personnelles représenteraient la valeur de 1 000 milliards d'euros. Preuve en est que les données sont devenues la source de revenus la plus importante. Il n'en demeure pas moins que ces dernières sont sensibles et se doivent d'être protégées. Cela passe notamment par la sensibilisation des acteurs de la santé quant à l'importance de la préservation de ces données.

Cela pose la question de la « patrimonialité des données ». Il convient donc de se demander si un utilisateur peut vendre ses données. Le RGPD prévoit qu'un traitement des données est licite à condition d'avoir obtenu le consentement de l'utilisateur « pour une ou plusieurs finalités spécifiques »(103). Juridiquement, la vente implique un transfert de propriété. En l'espèce, il ne s'agit pas d'un transfert à proprement parler puisqu'une finalité spécifique y est attribuée. À ce sujet, la France est très réticente. L'éthique en matière de protection des données tend plutôt à considérer que les données sont un élément de la vie privée et sont, par nature, inaliénables. La revente de données représente un vide juridique et provoque des risques de dérives, notamment en matière d'éthique. Deux conceptions s'affichent : d'une part, les pouvoirs publics, adversaires de la patrimonialité des données, s'emparent du nouvel or blanc au bénéfice de la recherche et des patients. D'autre part, des voix plus libérales prônent un commerce libre de données dans le mécanisme de la *blockchain*, selon les choix des patients. Ainsi, la *startup* Embleema, fondée en 2017, qui compte parmi ses partenaires la Fondation Linux, l'Université Harvard et les laboratoires Pierre Fabre, veut créer le premier carnet de santé en *blockchain* en France. Se pose avec acuité la question de la patrimonialité des données collectées. La discussion porte sur la question de savoir si les données sont une émanation de la personnalité depuis la loi Informatique et Libertés (1978) et protégées par le principe d'indisponibilité du Code civil. Toutefois, le droit devra vraisemblablement s'adapter à une évolution des mentalités et des comportements des citoyens vis-à-vis de leurs données, soit en considérant que les personnes doivent être protégées contre elles-mêmes en assurant l'indisponibilité des données, soit en accompagnant le mouvement de valorisation des données. Selon une enquête de CSA Research pour le laboratoire pharmaceutique Roche de novembre 2018, 78 % des Français interrogés estiment que le partage de données de santé (avec des scientifiques) est un acte citoyen qui peut faire progresser la recherche dans le cadre de l'*open science*, 20 % sont prêts à aller plus loin que le simple partage, et à les vendre. Cette proportion augmente à l'horizon 2045, où la santé numérique sera quasiment totalement

(102) J. Rose, O. Rehse et B. Röber, *The value of our digital identity*, 20 nov. 2012.
(103) RGPD, art. 6.

intégrée aux pratiques médicales[104]. Dans vingt-cinq ans, les jeunes d'aujourd'hui considéreront que la médecine numérique basée sur la téléconsultation et la télémédecine[105] sera la norme, et que la question de la protection des données de santé aura évolué dans un sens favorable à la valorisation des données au profit des patients afin d'assurer un indispensable progrès pharmaceutique[106].

Ces évolutions incontournables, qui s'inscrivent dans une dynamique de digitalisation de la société, conduisent à s'interroger sur l'évolution du périmètre des responsabilités des acteurs en charge de la collecte, de la surveillance, de la protection, de l'exploitation et de la valorisation des données de santé collectées par les outils numériques en santé.

## II. – Une responsabilité pesant sur les acteurs de la santé

Bienfaisance, non-malfaisance, autonomie et justice, tels sont les enjeux éthiques dégagés notamment par le Conseil national de l'Ordre des médecins (CNOM) en matière de numérique en santé. Il est indispensable de penser une évolution des règles déontologiques applicables aux professionnels de santé, médecins, pharmaciens et autres professionnels, dans un monde porté par une innovation fulgurante. Ce serait un véritable frein, voire une source de contournement des dispositifs législatifs et réglementaires, que de continuer à penser et maintenir les règles déontologiques en l'état. Le droit doit donc s'adapter[107] avec agilité à ces évolutions qui restent encore, pour une grande partie, inconnues, et fixant des normes sur des bases éthiques, qui elles demeurent des principes fondamentaux intangibles de l'homme. La quadrature du cercle consiste donc à innover dans le respect des principes, à anticiper un monde inconnu en déterminant la marge acceptable d'évolution des droits du patient.

Le CNOM a publié un bulletin de réflexion[108] au sujet de la place du médecin dans le monde du numérique, où il ressort qu'il serait peut-être nécessaire de faire évoluer certains aspects du Code de déontologie afin de s'adapter aux nouveaux enjeux[109]. À ce titre, le CNOM a publié, en 2018, un livre blanc[110] prévoyant des recommandations pour favoriser la pérennité de la santé dans le monde numérique. Ces réflexions font suite à la publication d'un livre blanc en décembre 2011[111] sur la déontologie médicale sur le web. L'un des aspects les plus sensibles en matière d'éthique reste le secret médical. Comment peut-il être convenablement garanti dans un monde ultraconnecté ? La numérisation de la santé a pour effet positif

(104) Observatoire Roche/CSA Research, *Les Français et la recherche en santé*, 1er févr. 2019.
(105) J.-F. Nys, *La télémédecine, simple évolution ou véritable révolution des usages dans le système de santé français ? : Marché et organisations* 2020, vol. 38, n° 2, p. 15-36.
(106) C. Chambard, *Comment accélérer le déploiement de l'e-santé en France ? Rôle des principaux acteurs dans le diabète : Les Tribunes de la santé* 2019, vol. 60, n° 2, p. 51-61.
(107) CE, Étude annuelle 2013, *Le droit souple*, p. 6.
(108) CNOM, *Enjeux éthiques : la place du médecin*, 9 mars 2020.
(109) CNOM, *La télémédecine face au risque d'ubérisation des prestations médicales*, 14 févr. 2018. – R. Cuvillier *et al.*, *En quoi la transformation numérique peut-elle se révéler un levier pour l'accès aux droits et l'inclusion sociale ?*, Groupe de travail EN3S, 2017.
(110) Livre blanc, *Médecins & patients dans le monde des data, des algorithmes et de l'intelligence artificielle, Analyses et recommandations du CNOM*, 26 janv. 2018, Recomm. 29, p. 61.
(111) CNOM, Livre blanc, *Déontologie médicale sur le web*, déc. 2011.

de favoriser les échanges entre les professionnels de santé et, ainsi, d'améliorer la prise en charge du patient. Cependant, ce bénéfice n'aura de la valeur que s'il est accompagné du respect des valeurs d'éthique comme la confidentialité.

À ce sujet, le Conseil a rappelé que la préservation du secret médical couvrant les données personnelles de santé doit être appliquée aux traitements des données massives et que leur exploitation ne doit pas permettre l'identification d'une personne au risque de la conduire à des discriminations. Cet enjeu de protection du secret et de la confidentialité qui s'impose aux professionnels de santé porte sur l'ensemble du parcours de santé du patient, entre médecine de ville et hôpital, entre médecins généralistes et spécialistes, et ce tout au long de la vie du patient. Les appétits pour la récolte de données sensibles permettant de faire des études sur des bases considérables de données du patient, tout au long de leur vie, permettent d'identifier des voies de traitement et des pistes d'innovation pharmaceutiques nouvelles, qui déclencheront des sources de profits. L'encadrement tout au long du parcours de soins, et notamment au sein des établissements de santé, s'impose, ce qui signifie une confidentialité des données vis-à-vis des acteurs tels que l'assurance maladie, mais aussi et surtout les assurances, banques et organismes. Les nouvelles technologies appliquées à la santé constituent un atout majeur pour améliorer la qualité de la prise en charge des patients et pallier certaines carences de l'offre de soins. Elles permettent de développer de nouvelles pratiques professionnelles, notamment grâce à la mobilité, pour améliorer la qualité de la prise en charge ou la coordination des différentes interventions au profit d'un même patient. Ces nouvelles pratiques répondent en particulier aux besoins induits par des parcours de soins de plus en plus complexes. Le parcours de santé est dit « complexe » lorsque l'état de santé, le handicap ou la situation sociale du patient rend nécessaire l'intervention de plusieurs catégories de professionnels de santé, sociaux ou médico-sociaux. Enfin, les technologies numériques représentent également une opportunité de croissance économique pour la France avec le développement d'une filière industrielle d'excellence. Le régime d'échange et de partage des données de santé est fondé sur le respect du secret professionnel qui s'impose à tous les professionnels intervenant dans le système de santé, sur un socle de conditions légales d'échange et de partage des données de santé[(112)] (la loi prévoit le partage de certaines données de santé à caractère personnel et non le partage de toutes ces données) et sur la notion d'équipe de soins et le couple information/droit d'opposition. Dans cet environnement juridique dense et nécessairement évolutif, il est de la responsabilité de chaque acteur participant à l'exploitation, l'échange et le partage des données de santé, de prendre des mesures spécifiques pour garantir le respect du cadre juridique de la santé numérique. Il relève de la mission de l'ASIP-Santé de contribuer à créer les conditions d'un « espace national de confiance » : en facilitant l'orientation et le parcours des patients dans le cadre des grands chantiers nationaux qui lui sont confiés (MSSanté, SI-Samu, PSIG, *etc.*), mais également au travers de son rôle dans la définition des prérequis au développement des systèmes

(112) C. santé publ., art. L. 1110-4-1.

d'information partagés de santé (cadre fonctionnel d'interopérabilité et de sécurité, infrastructures techniques, confidentialité et usages).

Cet enjeu doit permettre justement de pallier les inégalités. Comme l'a précisé la Conférence nationale de santé dans un avis[113], l'objectif est d'assurer l'accès pour tous, et cela suppose de former tous les acteurs[114]. La question du partage d'informations médicales au sujet du patient concerne aussi les établissements de santé. En effet, ces établissements, publics ou privés, doivent contribuer à l'enjeu de la sécurisation des données qui va de pair avec l'éthique. Au-delà de la divulgation d'informations à caractère personnel non consentie, se pose le risque de la discrimination en raison de l'état de santé par les assureurs, que la loi française prohibe. De plus, le Code de la santé publique[115] interdit d'utiliser des données de santé à cette fin.

Il est essentiel que le développement du numérique en santé profite à tous, au risque de creuser les fractures sociales, économiques, mais aussi culturelles. Les enjeux éthiques voudraient une régulation stricte ; or, un environnement aussi contraignant ne serait pas en faveur de l'innovation. En effet, ne pas s'ouvrir à ces nouvelles technologies expose à un risque de voir arriver sur le territoire français des algorithmes étrangers qui ne respectent pas la législation française[116]. Les risques éthiques seraient plus importants. De plus, l'éthique évolue en même temps que les changements sociaux, et se doit de s'adapter. Le numérique ne devrait pas être un frein, mais de nombreux points de vigilance sont à anticiper par une législation agile qui protégerait les intérêts des utilisateurs, tout en préservant le développement des nouvelles technologies.

## CONCLUSION

La pandémie de Covid-19 a permis de donner de multiples illustrations de ces problématiques concernant l'amplification dans l'utilisation des outils numériques dans une préservation maximale des droits du patient. La question notamment du traçage des populations touchées par la Covid-19 pose d'énormes difficultés. Plusieurs applications ont été proposées par le ministère, permettant de suivre les patients et les *clusters* afin d'éviter la propagation du virus[117], avec toutefois de très sérieuses réserves sur la sécurité de ces outils créés dans l'urgence, et sur la confiance accordée par la population.

(113) Conférence nationale de santé, avis, *Faire en sorte que les applications et objets connectés en santé bénéficient à tous*, 8 févr. 2018.

(114) R. Brasselet, *La circulation de la donnée à caractère personnel relative à la santé : disponibilité de l'information et protection des droits de la personne*, thèse Droit, Université de Lorraine, 2018.

(115) C. santé publ., art. L. 1461-1.

(116) C. Villani et G. Longuet, *L'intelligence artificielle et les données de santé*, Rapp. Sénat n° 401 (2018-2019), 21 mars 2019.

(117) La loi n° 2020-546 du 21 mars 2019, prorogeant l'état d'urgence sanitaire et complétant ses dispositions, contient en effet deux ensembles de dispositions destinées à assurer le repérage des patients potentiellement infectés et leur isolement plus ou moins strict, afin de « rompre les chaînes de contamination ».

Le chapitre II de la loi d'urgence précitée est spécifiquement consacré à la « création d'un système d'information aux seules fins de lutter contre l'épidémie de Covid-19 ». Il annonce d'emblée de nouvelles dérogations au secret médical puisqu'il débute par la formule suivante : « Par dérogation à l'article L. 1110-4 du Code de la santé publique (…) ». Il indique toutefois que ces dérogations ont pour « seules fins de lutter contre la propagation de l'épidémie de Covid-19 » et ont une durée limitée : celle strictement nécessaire à cet objectif ou, au plus, une durée de six mois à compter de la fin de l'état d'urgence sanitaire.

Il n'en demeure pas moins que, comme l'a souligné la CNIL dans sa délibération du 8 mai 2020 sur le projet de décret d'application, « l'aménagement d'une nouvelle dérogation au principe du secret médical entraîne le partage de données d'une très grande sensibilité susceptibles de concerner l'ensemble de la population, caractérisant ainsi une situation inédite ».

Comme l'a souligné le Conseil constitutionnel dans sa décision n° 2020-800 DC du 11 mai 2020 :

> « Si les dispositions contestées de l'article 11 exemptent la collecte, le traitement et le partage des données de santé de l'obligation d'obtenir le consentement des intéressés, elles n'exemptent pas ces mêmes opérations du respect des dispositions du règlement du 27 avril 2016 [RGPD] et de la loi du 6 janvier 1978 [Loi "Informatique et Libertés"] relatives aux principes régissant les traitements des données à caractère personnel et aux droits reconnus aux personnes dont les données sont collectées, notamment leurs droits d'accès, d'information et de rectification ».

Par ailleurs, il faut constater pendant toute la période Covid-19 un relâchement certain de la sécurisation des données au sein des établissements de santé et entre professionnels de santé, confrontés aux urgences médicales. Ces constats alarmants ont été dressés par toutes les autorités, et notamment, la CNIL pointe du doigt la communication entre les acteurs sur les plateformes numériques, par mails et autres outils de communication.

C'est donc tout l'équilibre du RGPD qui flanche pendant cette crise Covid-19, qui démontre ses limites avec des applications basées sur des plateformes hors UE et dépendantes des systèmes américains notamment, ou encore des piratages et actes de cybercriminalité dans les établissements de santé. L'édifice est fragile et menace les droits des patients.

Il est donc plus que jamais indispensable de revoir l'équilibre entre protection et valorisation des données, entre confidentialité et partage, entre secret médical et ouverture des données à l'innovation. Il est certain que la configuration des problématiques changera dès lors que le droit intégrera la possibilité d'évoluer agilement autour d'une protection des droits du patient associée à l'innovation numérique. C'est la mise à l'écart du patient, considéré comme un sujet de protection et non comme un acteur actif dans l'organisation de sa protection, qui peut en partie expliquer les risques de surévaluation des données et de piratages associés.

Dès lors que le patient pourra s'exprimer sur ce qu'il entend protéger parmi ses droits et comment il entend protéger ses droits, à l'instar du régime assurantiel sur son habitation notamment, la question de la confidentialité ou encore du secret médical sera résolue. Cela impliquera toutefois une part de responsabilité à assumer par le patient utilisateur des outils numériques et applications de santé.

Cette part de responsabilité correspondrait au risque qu'il prend lui-même en permettant l'accès à ses données personnelles et de santé, notamment parce qu'il s'expose ou transmet ses données sur les réseaux sociaux.

Une évolution dans ce sens alliant les droits et obligations du patient à une révision du Code de déontologie permettrait d'avancer vers une innovation juridique dans l'innovation numérique.

CHAPITRE 3

# L'IMPACT DU NUMÉRIQUE DANS LA RECHERCHE ET DÉVELOPPEMENT DES PRODUITS DE SANTÉ

Stéphanie CHABIN

*Coauteurs :*
Agnès AUDOIN
Aurélien BIECHY
Laëtitia GAILLARD
Daniel KADAR
Deogratias NGABONZIZA
Klervi SIMON

## INTRODUCTION

Les solutions digitales dans le domaine de la santé, appelées également e-santé (ou santé du numérique), peuvent revêtir des formes variées. Certaines sont désormais connues et maîtrisées, pour ne pas dire standardisées, mais les solutions digitales innovantes requièrent la compréhension de modèles économiques et de technologies éloignés des corps de métiers traditionnels de l'industrie pharmaceutique. L'e-santé se développe de manière exponentielle et concerne l'intégralité des domaines d'activité et des acteurs du monde de la santé.

Les projets digitaux innovants sont au croisement d'enjeux multiples, tel celui de la conformité, de la protection des données personnelles et de l'intégrité scientifique ainsi que de la maîtrise des systèmes de technologies de l'information et de la communication (TIC), intégrant parfois de l'intelligence artificielle (IA).

L'enjeu essentiel, pour les acteurs de la santé numérique, est de comprendre cet environnement complexe et son évolution exponentielle, tout en assurant l'intégrité scientifique fondamentale à son activité. Cette compréhension, encore timide, est la seule à pouvoir permettre aux acteurs de la santé numérique d'investir dans

les compétences, le développement de leurs collaborateurs, mais également des partenariats d'une nature différente.

La complexité de mise en œuvre de ces projets vient souvent de la difficulté à maîtriser les considérations techniques en jeu et à intégrer de nouveaux risques associés. Dans un cadre juridique existant, et en perpétuelle évolution, comment appréhender ces innovations et comprendre leur impact dans la recherche et le développement des produits de santé ?

Nous proposons une analyse axée sur la compréhension des technologies de l'information et de la communication ainsi que sur le parcours des données, essentielles à l'ensemble des solutions digitales innovantes, et si vitales aux acteurs de la santé numérique. Ces derniers doivent opérer dans un environnement concurrentiel et mouvant, tout en répondant aux exigences d'un changement de paradigme tendant vers une responsabilisation accrue des intervenants sur le parcours des données.

Les acteurs dans l'industrie de la santé doivent désormais aborder les données et les expertises associées au-delà des enjeux strictement médicaux, scientifiques et réglementaires, en développant une approche holistique et stratégique. Les données apparaissent peu à peu comme une nouvelle classe d'actifs et la course au développement de solutions digitales innovantes provoque des mutations profondes dans l'organisation des entreprises ainsi qu'une réflexion nouvelle sur la stratégie de valorisation de ces nouveaux actifs. La transformation des entreprises pharmaceutiques et de biotechnologies tend notamment à la création d'une gouvernance globale autour de la donnée afin de maximiser le potentiel des utilisations des données de santé. Les flux des données doivent être maîtrisés et sécurisés, notamment par une connaissance des systèmes de technologies de l'information, mais également des réglementations relatives aux données personnelles qui se sont multipliées à travers le monde.

Les projets digitaux, et *a fortiori* les plus innovants, sont dépendants d'une parfaite maîtrise de ces différents enjeux. D'autant que lesdits projets ne doivent plus être compris en isolation mais de manière intégrée, afin d'anticiper les connectivités entre solutions digitales. Cela laisse augurer de l'importance de solutions technologiques telle que la *blockchain*.

Une fois cette étape maîtrisée, le potentiel d'impact du numérique dans la recherche et le développement des produits de santé peut véritablement produire des effets, notamment par l'accélération donnée aux programmes de recherche. Toutefois, cela n'est pas sans risque si les acteurs de la santé numérique s'engagent sans conduire les diligences nécessaires et maîtriser parfaitement l'environnement dans lequel ils opèrent. La crise de la Covid-19, que nous traversons alors que nous rédigeons cet article, a notamment révélé les opportunités mais aussi les risques bien réels que rencontrent l'ensemble des acteurs du système de santé et le patient acteur de sa santé. C'est tout le paradigme d'organisation du système de santé et d'actions des acteurs industriels, établissements et professionnels de santé qui est modifié.

Quels que soient les outils utilisés, la recherche scientifique est guidée par la notion d'objectivité. Elle se doit donc d'obéir à une parfaite compréhension et

maîtrise des méthodologies utilisées pour être en capacité d'expliquer et reproduire le résultat innovant et passer les fourches caudines des autorités de santé.

SECTION 1

# L'ADAPTATION DES ACTEURS DE LA SANTÉ À LA DIGITALISATION, DE LA DONNÉE À L'INTELLIGENCE ARTIFICIELLE

## § 1. – Une nouvelle place pour les technologies de l'information, au « cœur du réacteur » des acteurs de la santé numérique

Pourquoi s'intéresser à l'IT en matière de santé ?

*IT* est la contraction de *Information Technology* en anglais, une expression communément utilisée pour se référer aux nouvelles technologies de l'information et de la communication, au numérique, à l'informatique et à l'utilisation des logiciels. La démocratisation de l'industrie logicielle a permis aux entreprises d'entamer une transformation sans précédent dans leurs modes de fonctionnement, et si l'avantage premier était l'automatisation de tâches répétitives pour un gain de productivité, un autre avantage a rapidement émergé : une opportunité d'innovation et de nouvelles perspectives de développement. Le secteur de la santé ne fait pas exception, toute entreprise qui souhaite se développer durablement et accéder à de nouveaux marchés investit massivement dans l'innovation et tend à confier à l'IT une place de plus en plus importante autant au travers de partenariats que de recrutements ou de rachats – ce qui n'a pas les mêmes conséquences en termes de propriété ou de protection des résultats.

Bien que présent partout, l'IT reste tout de même une matière invisible. Autant le résultat produit par un logiciel est visible (un tableau d'affichage numérique, le déblocage d'une barrière, le fonctionnement automatique d'une machine), autant le fait qu'un logiciel soit à l'origine de ce résultat n'est pas immédiatement évident à l'œil nu, ce qui est probablement dû à une incompréhension de l'environnement IT qui, pour l'usager, apparaît souvent complexe ou opaque.

Afin de comprendre cette évolution actuelle dans l'industrie pharmaceutique, il devient nécessaire de prendre en compte la complexité technique et l'environnement dans lequel l'IT évolue. La recherche et le développement de produits de santé comportent en effet un grand nombre de projets informatiques, qui font aussi évoluer la manière d'envisager la chaîne de production et l'accès des produits au marché. C'est notamment le cas de logiciels qui permettront de gérer des essais cliniques, de couvrir des obligations réglementaires, qui permettront de faire dialoguer des formats très différents de données, de les analyser en vue d'identifier certaines données spécifiques qui feront avancer la recherche, ou qui permettront de créer

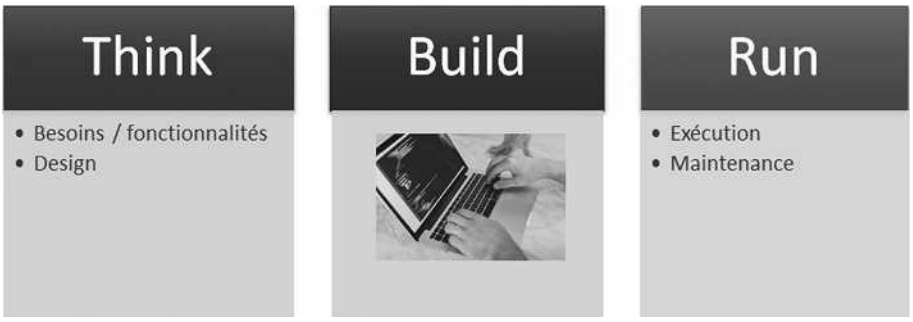
des dispositifs médicaux. Grâce à l'automatisation, au *machine learning* et à l'intelligence artificielle, les outils technologiques de R&D peuvent aussi aller jusqu'à proposer des résultats qui n'auraient pas été envisagés auparavant.

Les aspects technologiques ne pourront pas être dissociés du projet qu'ils vont permettre de créer, ce qui fait qu'un juriste souhaitant sécuriser des projets numériques de santé doit s'assurer une compréhension minimale du contexte et des principaux modes de fonctionnement de l'IT. Par ailleurs, rappelons qu'à la base de l'IT, il est nécessairement question de données et d'algorithmes.

## I. – L'IT, un environnement complexe

Si les systèmes informatiques ne sont qu'à la base du traitement de données et des algorithmes d'intelligence artificielle, ils relèvent déjà en eux-mêmes d'un écosystème complexe. La définition des fonctionnalités nécessaires à l'usager y est une notion clé, tout autant que la méthode de développement, le choix de l'éditeur ou l'environnement d'intégration et de configuration. Il existe nombre de métiers et de spécialités très différents dans l'univers IT, et il est facile de se perdre dans les différentes strates de ces projets d'investissement à acteurs multiples qui aboutiront *in fine* à l'utilisation d'un seul logiciel. On peut par exemple compter des activités d'assistance à maîtrise d'ouvrage qui aideront les usagers à définir leurs besoins fonctionnels et donneront instruction à d'autres spécialistes de transformer ces besoins en fonctionnalités techniques, des activités d'architecture IT qui permettent de valider la conception globale du logiciel en lui-même et sa cohérence technologique avec le paysage numérique de l'entreprise, des activités de développement dans plusieurs langues, de test, de configuration, sans oublier les activités de gestion de projet pour coordonner autant d'acteurs multiples (y compris des juristes).

La technologie n'existant pas pour elle-même, nous pouvons en déduire que chaque logiciel poursuit un objectif utile à l'activité commerciale de l'entreprise qui l'a acquis ou le fait développer. De plus, un logiciel fonctionnera rarement seul : il doit composer avec son écosystème et n'atteindra l'utilité voulue que s'il a été correctement « pensé », autant dans ses fonctionnalités que dans son environnement. La méthode fréquemment proposée dans les projets numériques est celle du « *Think – Build – Run* » :




*Source : auteur*

**Logiciel et algorithme :** dans la pratique, on ne pourra pas sécuriser entièrement un projet numérique sur des produits de santé si l'on s'intéresse uniquement à l'algorithme d'IA ou de *machine learning*. En effet, l'algorithme pose dans ce cas essentiellement la question de la production du résultat attendu, ce qui prend généralement en compte des considérations de droit de la santé mais ne s'intéresse que peu à l'aspect technologique et au logiciel en lui-même (qui reste toujours la base de l'algorithme d'un projet numérique). Il devient nécessaire de mettre en perspective le domaine du numérique tout autant celui de la santé, et notamment de garder à l'esprit quelques-uns des éléments suivants :

– le système d'information et son environnement : le logiciel et sa documentation, le matériel connecté au logiciel, son hébergement, les données qu'il traite, les interfaces nécessaires avec les autres systèmes, le paysage applicatif de l'entreprise et les personnes gérant le logiciel ;

– l'aspect évolutif du logiciel, dont certaines fonctionnalités seront forcément ajoutées ou supprimées au fil du temps ;

– les différentes étapes de développement du logiciel, qui n'auront pas les mêmes impacts selon que l'on part d'un résultat attendu (développement par un cycle en V) ou que l'on crée un résultat au fur et à mesure (développement par la méthode Agile) ;

– les aspects réglementaires de qualité, de sécurité, de traçabilité et d'audit liés aux logiciels pouvant avoir un effet sur les patients ;

– les problématiques de droit d'utilisation et d'exploitation accrues par la multiplicité d'acteurs et de produits interfacés dans le cadre d'un même projet.

Ce sont tout autant d'éléments qui pourront avoir de l'influence sur la bonne exécution du logiciel, la production du résultat attendu et même la possibilité technique d'exploitation de ce résultat pour le projet R&D.

## II. – Du *Privacy by design* à l'*IT by design*, vers le nouveau rôle de l'IT

L'essor des technologies a nécessairement des conséquences sur le rôle des départements informatiques et la stratégie de conformité des acteurs de la santé numérique. La révolution numérique, qui a bouleversé non seulement la recherche médicale mais également la prise en charge et l'accompagnement des patients, a permis d'intégrer les technologies de l'information et de la communication « au cœur du réacteur » des acteurs de la santé numérique.

Selon les lignes directrices de la CNIL, la logique de responsabilisation (*accountability*) des acteurs, instaurée récemment par la réglementation en matière de protection des données (V. *infra*, Section 2, § 1), se traduit par la prise en compte des problématiques de protection des données en amont, dès la conception du service ou du produit. Ce principe, plus connu sous le nom de *Privacy by design*, est ainsi une exigence à intégrer en amont de tout projet numérique. Ceci implique que les acteurs de la santé numérique adaptent leurs procédures internes, afin de penser la conformité en amont, puis tout au long de la vie d'un projet.

Les services informatiques doivent au contraire être capables de penser en amont la sécurisation de tout projet digital, notamment en assurant la mise en place de mesures techniques et organisationnelles appropriées prévues par le RGPD. Ainsi, les responsables IT doivent avoir de nouvelles responsabilités et se doter d'un rôle plus stratégique dans la mise en place des projets innovants. Ceci implique par exemple que les départements IT soient formés, ou du moins sensibilisés, aux exigences de la réglementation européenne en matière de protection des données. Plus généralement, l'entreprise se doit d'entamer une nouvelle stratégie numérique fondée sur la conformité, ce qui peut passer par une restructuration des départements, mais aussi la nécessaire obtention de moyens et d'un budget nécessaire pour sensibiliser les acteurs de l'IT aux nouvelles problématiques de conformité. De plus, ce changement de paradigme nécessite une consultation préalable des départements informatiques, ce qui implique de modifier, en interne, les process et le *business model* de la société, autour de l'IT.

Ainsi, l'approche *Privacy by design* induite par le RGPD doit aller de pair avec celle de l'*IT by design*, qui consiste à donner aux départements IT un rôle central dans la stratégie de conformité de l'entreprise. Ce n'est pas encore le cas aujourd'hui pour la plupart des entreprises. Or, il s'agit d'un enjeu essentiel : comment maintenir les flux de données et avoir confiance dans des systèmes informatiques que l'on ne comprend pas ? Connaître les flux de données, c'est bien. Mais connaître les systèmes qui permettent et mettent en œuvre ces flux, c'est beaucoup mieux. Une meilleure maîtrise, en amont, des flux de données et des problématiques de gestion des données en général, permettra aux départements IT de passer moins de temps à gérer de potentiels incidents, afin de se concentrer enfin sur l'innovation et la digitalisation de l'entreprise.

Le grand hiatus dans ce contexte est que seules les données ont été considérées comme devant faire partie du « cœur du réacteur », mais pas les systèmes qui les génèrent, les collectent ou les traitent. Contenant et contenu ont été séparés dans le traitement réglementaire, le contenant n'étant régulé que sous l'aspect sécurité/inviolabilité. C'est un peu comme si on voulait sanctionner les émissions des véhicules automobiles sans s'intéresser aux causes desdits rejets. En d'autres termes, il est illusoire de chercher à mettre la protection des données au cœur du réacteur si les technologies de l'information ne le sont pas, et restent « au bout du couloir ».

L'*IT by design* doit donc permettre de véritablement inclure les technologies de l'information « au cœur du réacteur » des acteurs de la santé numérique. Les technologies de l'information prennent une nouvelle place, centrale, chez ces acteurs. Cette logique, cependant, se heurte encore à de nombreux risques et réticences, et doit notamment faire face à un mouvement d'externalisation des compétences.

## III. – L'externalisation des compétences, un facteur de risque pour l'*IT by design* ?

Dans une situation idéale, il est beaucoup plus avantageux de créer un système d'information ou d'acquérir un logiciel dont la configuration et les droits d'utilisation correspondent exactement aux besoins du projet ou du produit (selon la logique de l'*IT by design* décrite ci-dessus). Toutefois, l'évolution de nos *business models* qui tendent vers l'externalisation des compétences peut rendre cette tâche extrêmement difficile.

En effet, avec l'explosion de l'industrie technologique, la diversification des activités et des spécialités, l'IT qui était traditionnellement créé et géré à l'intérieur de l'entreprise est aujourd'hui de plus en plus externalisé, surtout lorsque la technologie n'est pas le cœur de l'activité commerciale de l'entreprise. Nous le voyons d'ailleurs, nombreux sont les partenariats actuels en R&D entre laboratoires pharmaceutiques (propriétaires de données) et sociétés de développement logiciel ou *startups* ayant développé des modèles d'intelligence artificielle, autant de compétences que les laboratoires n'ont pas (ou pas encore) recruté.

Mais cela n'est pas tout. Même pour des logiciels plus classiques, on observe l'émergence de solutions SaaS (*Software as a Service*) « clés en main », développées, hébergées et maintenues directement par l'éditeur du logiciel, alors qu'auparavant les entreprises les installaient et les contrôlaient sur leurs propres serveurs. Les principales conséquences de ce phénomène sont que les entreprises perdent peu à peu leurs connaissances techniques, leurs capacités de développement et donc leur autonomie, ce qui les rend de plus en plus dépendantes de leurs fournisseurs IT (des GAFAM aux *startups*), sans lesquels elles ne peuvent plus fonctionner aujourd'hui, autant pour leurs activités bureautiques que pour leurs activités commerciales. La négociation contractuelle avec les prestataires évolue dans cette même logique, où un déséquilibre de plus en plus profond peut se créer avec un acheteur qui n'aurait pas connaissance de l'environnement IT. Dans ce cas de figure, il est par exemple bien plus difficile de tracer et de démontrer ce qui a été mis en place, surtout lorsque la communication du code source ne fait pas partie des engagements contractuels, ou qu'il faut encore faire appel à un autre prestataire IT pour l'analyser. Il est également plus difficile de démontrer qu'une partie de développement en *open source* n'est pas contagieuse pour prouver que le produit garde toute sa valeur commerciale.

Enfin, nombreux sont les cas où les entreprises sont confrontées à un prestataire IT qui souhaite vendre uniquement un résultat tout en conservant le moyen d'obtenir ce résultat (le logiciel), alors même que ce moyen est financé par l'entreprise tant en termes de développement logiciel que d'apport de données. Une des difficultés notables de l'*IT by design* est que la plupart des logiciels proposés sur le marché sont « sur étagère » ou vendus comme un service « sur étagère ».

Mais il faut également garder à l'esprit que tous les produits innovants basés sur des logiciels sont évolutifs et reposent sur l'analyse de données. Un logiciel auquel on ne fournit pas de données ne peut fonctionner. *A fortiori*, un algorithme (de *machine learning* ou d'IA) ne devient vraiment efficace que s'il a accumulé

une quantité de données suffisante qui lui a permis d'analyser ou « d'apprendre » de la situation : plus l'algorithme aura analysé d'essais cliniques différents, meilleur sera le résultat attendu. Les données que les entreprises de santé mettent sur la table ont donc autant de valeur que le service proposé par les prestataires IT, même si l'argumentaire commercial de ces derniers peut tendre à écarter cette question.

## IV. – Une course à l'appropriation des données par les entreprises IT

L'émergence des acteurs de l'industrie informatique a provoqué une amplification du traitement des données, qui sont désormais monétisées, cédées, transférées et revendues au sein et en dehors de l'Union européenne. Ce phénomène a par la suite été accentué avec l'apparition de nouveaux acteurs dans l'économie numérique, tels que les *dataminers*, *databrokers* ou encore algorithmeur.

La traque aux données personnelles est devenue un véritable *business model* pour les entreprises. En ce sens, dans son rapport de mai 2014, la *Federal Trade Commission* a évalué à environ 426 millions de dollars les revenus annuels en 2012 des neuf courtiers en données personnelles les plus importants. Il s'agit ici de profits considérables auxquels les individus, producteurs primaires des données, ne participent pas.

S'agissant des données de santé, l'article L. 1111-8, IV du Code de la santé publique dispose que : « Tout acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions ». De plus, l'article L. 4113-7 interdit l'exploitation commerciale des données de santé.

Néanmoins, on peut souligner l'exemple de l'entreprise Embleema qui permet aux individus d'héberger gratuitement leurs données relatives à la santé sur leur plateforme, afin de pouvoir par la suite les céder aux plus offrants. Dans un rapport, l'Assemblée nationale parle d'« une sorte "d'ubérisation" de la collecte de données, où chacun est son propre vendeur de données. Dès lors que les données de santé peuvent être revendues, la question du consentement libre et éclairé est brouillée »[(1)].

(1) J.-L. Touraine, Rapport d'information de M. Jean-Louis Touraine fait au nom de la mission d'information sur la révision de la loi relative à la bioéthique, 2019, n° 1572 (www2.assemblee-nationale.fr/documents/notice/15/rap-info/i1572).


**Figure 2 : Embleema. (s.d.). Home/Embleema, *Blockchain for Real-World Evidence Marketplace*. Consulté le 13 août 2019 (www.embleema.com)**

En effet, cette entreprise revendique le fait de rendre au patient le contrôle sur ses données de santé, en garantissant l'authenticité de son consentement explicite et éclairé. Il met en avant le fait d'assurer une véritable traçabilité des données, contrairement aux services en ligne tels que Facebook ou Google, grâce à la technologie *blockchain*. En échange de la mise à disposition de ses données anonymisées, le patient est rémunéré lorsque ses données sont utilisées à des fins de recherche clinique, lorsque la réglementation locale le permet. Embleema garantit au patient la possibilité de partager en toute sécurité ses données avec les potentiels acheteurs de données et de recevoir une compensation proportionnelle à son apport, et ce à condition que le patient ait préalablement donné son consentement. Cette compensation se trouve sous forme de *tokens* EBL, convertissables par la suite en monnaie traditionnelle.

La plateforme de cette entreprise offre la possibilité au patient ayant épuisé toutes ses options de traitements existants de partager ses données afin d'identifier les essais cliniques auxquels il peut prétendre. Cela permet au patient de partager ses données en temps réel avec les autorités sanitaires et les entreprises pharmaceutiques afin de surveiller en permanence l'innocuité et l'efficacité des médicaments[(2)].

(2) Embleema, *Embleema Blockchain Network V.2 : White Paper* 2018 (www.embleema.com/wp-content/uploads/2018/10/White-paper-Embleema.pdf).

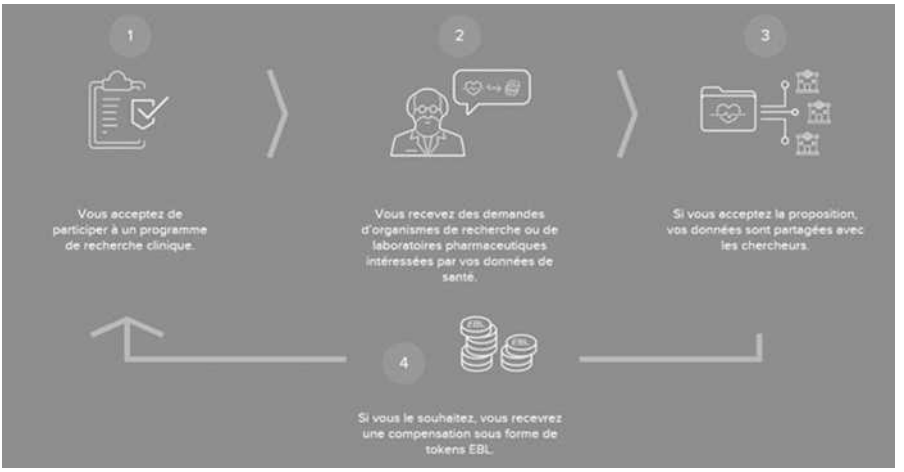



**Figure 3 : Embleema. (s.d.). Home / Embleema, *Blockchain for Real-World Evidence Marketplace*. Consulté le 13 août 2019 (www.embleema.com)**

Quitte à rétribuer la mise à disposition des données par les individus, on peut se poser la question de savoir s'il faut rétribuer la mise à disposition des données publiques par le biais de ces bases de données. Or, l'article L. 1461-2 du Code de la santé publique dispose clairement qu'elles « sont mises à disposition gratuitement ». En ce sens, le Comité interministériel pour la modernisation de l'action publique (CIMAP) avait réaffirmé « le principe de gratuité de la réutilisation des données publiques », en précisant « ne plus autoriser la création de nouvelle redevance »(3). Quant au rapport parlementaire relatif à « la protection des données personnelles dans l'*open data* », celui-ci avait présenté une position plus mesurée en préconisant que les « mesures d'anonymisation des données personnelles contenues dans des jeux de données publiques » soient subventionnées par l'État, sans pour autant « renoncer par principe au prélèvement d'une redevance en présence de coûts d'anonymisation élevés(4) »(5).

Depuis plusieurs années, « les GAFA se sont approprié les données. Ils investissent de l'argent dans diverses plateformes autour de la santé et estiment qu'en contrepartie, ils peuvent librement utiliser les données qui leur sont confiées. Et ce sont les GAFA qui vont devenir les assureurs de demain », observe Frédéric Bizard, économiste de la santé et professeur à Sciences Po. À cet égard, Amazon excelle dans les assurances, marché dans lequel l'entreprise a su s'implanter, en particulier dans le cadre des offres d'assurance-vie. À ce jour la réglementation interdit aux assureurs de tarifer le montant des contrats sur la base de données sensibles, y compris de santé. Néanmoins, de plus en plus de *Big Tech* mettent à disposition des individus des outils de santé à des fins de prévention.

(3) CIMAP, *Relevé de décisions du CIMAP* (4e Comité interministériel pour la modernisation de l'action publique 18 décembre 2013), 2013 (www.modernisation.gouv.fr/sites/default/files/fichiers-attaches/relevedecisions_cimap4.pdf).
(4) Sénat, *La protection des données personnelles dans l'open data : une exigence et une opportunité*, 2014, p. 12, Prop. n° 19 (www.senat.fr/rap/r13-469/r13-4696.html).
(5) J. Cattan, *La mise à disposition des données de santé : JCl. Droit administratif* 2016, n° 5, 15.

Dans cette nouvelle décennie d'innovation technologique, les GAFA joueront un rôle important pour proposer de nouveaux médicaments plus ciblés, plus précis, adaptés à la nouvelle médecine des « 4P ».

On pourrait envisager la possibilité selon laquelle les GAFA, suite à leurs partenariats avec les *Big Pharma*, soient à leur tour en mesure de développer et produire de nouveaux médicaments de façon autonome. Ainsi, ces entreprises technologiques pourraient continuer de proposer un accès « gratuit » à leurs services, en échange du partage par les utilisateurs de leurs données de santé, mais aussi proposer à leurs utilisateurs un accès gratuit à leurs médicaments. Cela reviendrait alors, non pas à remplacer les *Big Pharma*, mais à devenir de véritables concurrents. Ce scénario ne semble pas complètement illusoire quand on sait que les données sont considérées comme l'or noir du XXIe siècle, et que les GAFA détiennent déjà une quantité massive de données.

À cela s'ajoute le fait que ces *Big Tech*, pour la plupart basées dans la Silicon Valley, attirent de plus en plus de grands noms du domaine des essais cliniques. On peut citer, par exemple, Art Levison, ancien PDG de l'entreprise Genentech, qui a été nommé PDG de l'entreprise Calico (filiale de Google) en 2013. De même, Taha Kass-Hout, ancien responsable informatique de santé à la FDA, qui a été embauché par Amazon. Enfin, selon une étude du cabinet de conseil EY Alphabet, la société mère de Google a déposé 186 brevets dans le domaine de la santé, soit un accroissement de 38 % du nombre de brevets délivrés[6].

Au-delà du modèle de développement choisi (internalisation, externalisation ou modèle mixte), il est fondamental de s'assurer de sa complète compréhension, intégrité, transparence, conformité et sécurité, du flux des données aux plateformes et solutions IT utilisées, et cela inclut la compréhension des algorithmes.

(6) Sur ces sujets, voir : – C. Lemke, *Que va-t-il advenir de nos données de santé ? : L'Usine Santé* 15 mars 2018, consulté le 8 août 2019, www.usinenouvelle.com/article/donnees.N666629.
– M. Fontaine, S. Juillet et D. Froger, *La donnée numérique : l'or noir du XXIe siècle ?*, 8 sept. 2017, consulté le 5 juin 2019, www.lextenso.fr/petites-affiches/LPA129m1.
– *Tech Giants Tackle Health Care : An Opportunity or Threat for the Pharmaceutical Industry? : Clinical Trials Arena* 7 août 2018, consulté le 12 août 2019, www.clinicaltrialsarena.com/comment/tech-giants-tackle-health-care-opportunity-threat-pharmaceutical-industry.
– D. Ganev, *Big Pharma vs Big Tech : Healthcare Innovation Trends in the Media : Commetric* 27 juill. 2018, consulté le 12 août 2019, https://commetric.com/2018/07/27/big-pharma-vs-big-tech-healthcare-innovation-trends-in-the-media. – Federal Trade Commission, Data Brokers : A Call for Transparency and Accountability. États-Unis : *Createspace Independent Pub*, 2015. – Centre de recherches en droit privé et sciences criminelles d'Amiens et *al.*, 2015, p. 224.

# § 2. – Vers un encadrement de l'utilisation des produits et logiciels innovants dans le cadre des essais cliniques

## I. – L'appréhension juridique des algorithmes et la nécessaire transparence au service de la confiance dans le domaine du développement clinique

Un algorithme est défini comme l'« étude de la résolution de problèmes par la mise en œuvre de suites d'opérations élémentaires selon un processus défini aboutissant à une solution »(7). Le vocable « algorithme » renvoie donc à un principe mathématique. Cet algorithme, compte tenu de son mode de conception et de fonctionnement, relève soit de la catégorie des algorithmes d'automatisation, soit de la catégorie des algorithmes d'apprentissage. Si les premiers consistent en une simple technique d'intelligence artificielle, les seconds reposent sur des techniques complexes de système d'apprentissage machine(8).

Un algorithme d'automatisation est qualifié de déterministe car il s'agit d'un type d'algorithme qui se conforme « à un raisonnement déductif et probabiliste »(9) dont « la structure (…) est déterminée lors de sa conception : les paramètres de l'algorithme et la suite des étapes à suivre pour aboutir à un résultat sont fixés dès le début »(10). Le cheminement de ces algorithmes, qui accomplissent un enchaînement d'instructions conditionnelles, est donc prévisible, visible, et fidèle à la programmation déterminée par son concepteur. Il s'agit ici de « logiciels intelligents qui utilisent des connaissances et des inférences logiques pour résoudre des problèmes qui sont suffisamment difficiles pour nécessiter une expertise humaine importante pour trouver une solution »(11). En d'autres termes, les algorithmes ont pour but d'imiter et d'automatiser, par le biais de calculs rendus possibles grâce aux données massives disponibles, l'activité intellectuelle humaine.

Quant aux algorithmes d'apprentissage, ils reposent sur des règles de fonctionnement qui leur sont propres et permettent l'amélioration continue des instructions par le biais des techniques d'apprentissage machine complexes qui agissent par corrélations et par inductions (*machine learning* ou *deep learning* en anglais)(12). « On développe ces algorithmes, plus qu'on ne les conçoit »(13). Ces algorithmes sont qualifiés de « probabilistes » ou encore « non déterministes ». Ils ont la particularité de s'améliorer avec la quantité, et par conséquent connaissent depuis de

(7) A. 27 juin 1989, relatif à l'enrichissement du vocabulaire de l'informatique.
(8) L. Godefroy, *Les algorithmes : quel statut juridique pour quelles responsabilités ? : Comm. com. électr.* nov. 2017, n° 11 (https://lexis360.lexisnexis.fr/droit-document/article/communication-commerce-electronique/11-2017/018_PS_CCE_CCE1711ET00018.htm, consulté le 12 févr. 2019).
(9) *Ibid*.
(10) I. Pavel et J. Serris, *Modalités de régulation des algorithmes de traitement des contenus*, 2016 (www.economie.gouv.fr/files/files/directions_services/cge/Rapports/2016_05_Rapport_Algorithmes.pdf).
(11) E. Feigenbaum, *Knowledge engineering in the 1980s*, Department of Computer Science, Stanford University, 1982, p. 2-10.
(12) L. Godefroy, *Les algorithmes : quel statut juridique pour quelles responsabilités ? : Comm. com. électr.* nov. 2017, n° 11.
(13) Y. Caseau, *Strong Artificial Intelligence is Emerging as we Talk*, 30 juin 2015 (http://informationsystemsbiology.blogspot.com/2015/06/strong-artificial-intelligence-is.html, consulté le 24 mars 2019).

nombreuses années une progression importante due à l'amplification de leur capacité de calcul ainsi qu'à la mise à disposition d'une quantité massive de données[14]. C'est pourquoi certains estiment que cette catégorie d'algorithme s'inspire du fonctionnement des réseaux de neurones et de synapses du cerveau humain. En effet, les algorithmes d'apprentissage machine se fondent sur « les exemples, les cas où les expériences passées ou à partir des propres expériences ou explorations de la machine »[15]. Il s'agit donc d'algorithmes aptes à s'autoréguler en s'adaptant et en évoluant en continu[16]. Cela explique que les algorithmes de *machine* et *deep learning* constituent le socle de la plupart des avancées récentes en recherche.

On peut citer par exemple, l'analyse des images biomédicales qui représente une étape critique, dans le cadre des essais cliniques en R&D, qui permet d'établir l'absence ou la présence d'une réponse d'un patient au traitement faisant l'objet d'un essai clinique, en particulier en oncologie du fait de la localisation et de la taille de certaines tumeurs. Traditionnellement, ce sont des médecins hautement qualifiés qui sont responsables de l'examen de cette vaste quantité d'images. Afin de pallier le coût, le temps et l'incertitude que représente cet examen, certaines entreprises sont désormais capables de construire des modèles algorithmiques entraînés pour identifier des corrélations entre plusieurs types de données médicales (annotations, imageries, *etc.*) et plusieurs phénotypes cliniques.

Si le droit ne distingue pas ces différentes catégories d'algorithmes, ils sont, de façon générique, régulés depuis une quarantaine d'années, directement ou indirectement, par la loi. En ce sens, la loi Informatique et Libertés de 1978, fruit du rapport de la Commission Tricot, énumère trois principes couverts par le principe général présent à l'article 1, qui dispose que « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». De ce principe général, on observe une exigence de loyauté envers la personne concernée par le traitement de ses données par un algorithme, et sous une forme plus embryonnaire, les principes d'explicabilité et de transparence des algorithmes[17].

Ainsi, dans le prolongement du principe général inscrit dans l'article 1 de la loi Informatique et Libertés, le Conseil d'État, dans son étude annuelle de 2014 sur « Le numérique et les droits fondamentaux »[18] visant à « repenser les principes fondant la protection des droits fondamentaux », a rappelé l'importance de ce principe de loyauté, tout en affirmant l'existence d'un principe de vigilance. Le but étant de renforcer le rôle de l'individu dans la protection de ses données, selon un principe d'« autodétermination informationnelle »[19] permettant d'assurer un contrôle sur

(14) I. Pavel et J. Serris, *Modalités de régulation des algorithmes de traitement des contenus*, *op. cit.*
(15) *Ibid.*
(16) CNIL, *Compte-rendu, Événement de lancement du cycle de débats publics sur les enjeux éthiques des algorithmes*, 2017 (www.cnil.fr/sites/default/files/atoms/files/compte_rendu_table-ronde_-_ethique_et_numerique_-_les_algorithmes_en_debat.pdf).
(17) CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 2017.
(18) Conseil d'État, *Le numérique et les droits fondamentaux*, Doc. fr., 2014, p. 264 (www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf).
(19) Cour constitutionnelle fédérale, 16 févr. 1983 : *BVerfGE*, t. 62, p. 1 ; nalyse Fromont : *RDP* 1983, p. 954.

l'utilisation de ses propres données à caractère personnel. Principe introduit depuis le 7 octobre 2016 au sein de la loi pour une République numérique[20] qui s'inscrit dans une perspective d'affermissement de l'effectivité des principes antérieurs. En vertu de ce principe de loyauté, le Conseil d'État souligne notamment l'impossibilité d'utiliser des algorithmes dont la logique est somme toute contraire à l'intérêt des utilisateurs. Cette notion d'intérêt des utilisateurs est importante, car jusqu'à présent le législateur tendait à protéger les droits et libertés de l'individu, sans prendre en compte la dimension collective de cet intérêt. En effet, avec l'accroissement de la puissance des algorithmes et de la quantité de données à laquelle ces derniers ont accès, il ne s'agit plus de prendre en compte uniquement l'intérêt d'un seul individu mais de groupes entiers qui pourraient alors voir leurs droits et libertés, et par conséquent leurs intérêts collectifs, mis à rude épreuve.

Par intérêts collectifs, on entend les intérêts de catégories établis par la logique algorithmique, basée sur la jonction de certaines caractéristiques, et à même de faire l'objet de discriminations interdites par l'article 7 de la Déclaration universelle des droits de l'homme (DUDH), mais aussi la société dans son intégralité. Le développement en puissance des algorithmes d'apprentissage semble donc difficile à concilier avec le principe de loyauté. En effet, les algorithmes, et en particulier les algorithmes d'apprentissage, tendent à évoluer de façon autonome, au point de se poser la question de savoir si les développeurs sont en mesure de garantir la prise en compte de ce principe dès lors que l'algorithme est apte à se comporter de façon autonome, voire opaque pour ses propres concepteurs.

S'agissant de la conception des algorithmes il existe un principe, celui de vigilance, qui instaure une véritable méthodologie visant à orienter les concepteurs sur la façon dont ils devraient conceptualiser leurs algorithmes. Néanmoins, le caractère fluctuant et évolutif des algorithmes de *machine* et *deep learning* rend l'application de ce principe délicate. Pourtant ce principe pourrait permettre d'inverser cette tendance de confiance excessive ainsi que de déresponsabilisation, amplifiée par l'aspect « boîte noire » des algorithmes. En effet, ces derniers correspondent à des « suites d'opérations » complexes et longues, au cours desquelles de multiples acteurs sont susceptibles d'intervenir (concepteur, entreprise à l'initiative de la collecte des données utilisées, utilisateur final). Ce processus, semblable à celui d'une chaîne de sous-traitance, tend à diluer tout sentiment de responsabilité, et à annihiler de l'esprit les impacts susceptibles d'être engendrés par ces algorithmes. Or, l'objectif de l'utilisation des algorithmes est « de garantir que l'intelligence artificielle soit au service de l'homme, qu'elle l'augmente plutôt que de prétendre le supplanter »[21]. Il paraît indispensable de mettre en place un système de vigilance collective, que ce soit envers les phénomènes connus afin d'écarter leur survenue ou les phénomènes non envisagés originellement mais qui, du fait du caractère évolutif des algorithmes, sont envisageables.

(20) Source : Légifrance, L. n° 2016-1321 du 7 oct. 2016 pour une République numérique ; www.legifrance.gouv.fr/affichLoiPubliee.do?idDocument=JORFDOLE000031589829&type=general&legislature=14.

(21) CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 2017.

Dans cette perspective de vigilance collective apparaît alors un principe fondamental : l'explicabilité des algorithmes, principe défendu par Cédric Villani dans son rapport « Donner un sens à l'intelligence artificielle »[22]. Ainsi, il souligne la nécessité d'augmenter la transparence et l'auditabilité des systèmes algorithmiques. En effet, le fonctionnement des algorithmes d'intelligence artificielle est caractérisé par une opacité difficilement intelligible par le « commun des mortels », en raison de cette caractéristique, propre aux algorithmes, de « boîte noire ». Ces systèmes composés de suites mathématiques semblent très obscurs, d'autant plus pour les algorithmes d'apprentissage dont les instructions évoluent au fur et à mesure. Si les données d'entrée et de sortie, qui sont le résultat du traitement de ces données par l'algorithme, sont connues, on appréhende difficilement comment cela se produit. Par conséquent, si certains sont plus facilement explicables que d'autres (par ex., arbres décisionnels simples), les algorithmes d'apprentissage machine constitués de réseaux de neurones puissants ont moins vocation à être intelligibles.

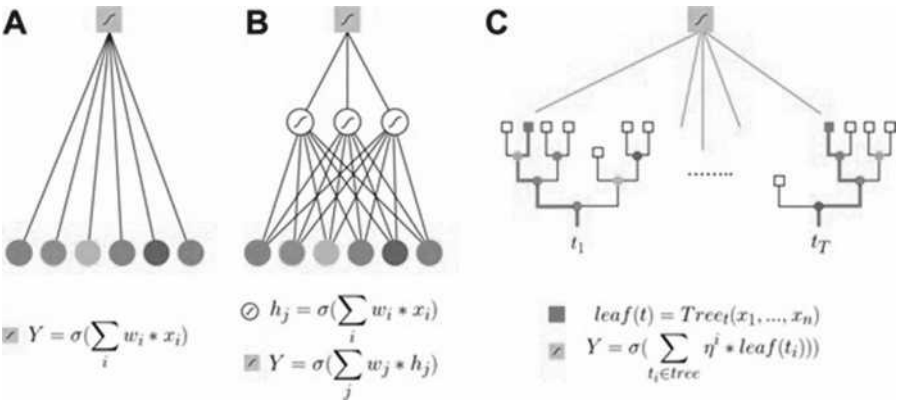



**Figure 4 : Représentation schématique de modèles d'apprentissage machine (www.nature.com/articles/s41598-019-46649-z)**

Néanmoins, à long terme, l'explicabilité des algorithmes apparaît nécessaire afin de permettre leur acceptabilité au sein de la société. En effet, dans une ère de transparence, il paraît peu admissible que des décisions importantes soient prises sans que les décisionnaires soient en mesure d'expliquer le fondement de cette décision, d'autant plus lorsqu'elles touchent un domaine tel que la santé.

L'adaptabilité de l'intelligence artificielle la différencie fondamentalement des *softwares* usuellement utilisés dans le cadre du développement des dispositifs médicaux. C'est pourquoi les autorités, et notamment la *Food and Drug Administration* (FDA), s'y intéressent de près. La FDA travaillait sur l'élaboration d'un cadre réglementaire spécifique en prenant une approche globale du développement de ce type de produit permettant alors de s'adapter au fur et à mesure de

(22) C. Villani, *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne*, 2018, p. 142 (www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf).

la collecte des données en temps réel[23]. Les technologies d'intelligence artificielle et d'apprentissage automatique ont le potentiel de transformer les soins de santé, en intégrant continuellement des informations issues de la vaste quantité de données générées chaque jour pendant la prestation des soins de santé et la réalisation des essais cliniques.

La FDA a délivré ses *guidelines* courant octobre 2020[24]. Elle propose ainsi un nouveau cadre réglementaire sur l'intelligence artificielle et les technologies d'apprentissage automatique.

La crise de la Covid-19 a accéléré la prise de conscience des autorités face à l'émergence et la nécessaire compréhension des solutions d'intelligence artificielle, notamment dans le cadre de solutions permettant l'identification de nouvelles indications de médicaments déjà existants pour lutter contre des maladies émergentes et difficiles d'appréhension.

Après avoir autorisé pour la première fois, courant avril 2018, une intelligence artificielle à formuler un diagnostic de rétinopathie diabétique, la FDA a récemment délivré des autorisations d'utilisation d'urgence pour aider les cliniciens à diagnostiquer et traiter la Covid-19, comme l'algorithme *COViage Hemodynamic Instability and respiratory Decompensation Prediction System* développé par une société californienne Dascena, et qui aide à prédire le nombre des patients Covid-19 devant être intubés. Toutefois, la FDA émet une réserve car cet outil ne doit pas être utilisé de manière indépendante pour formuler une décision médicale.

Il faut rester vigilant et s'assurer du suivi et de la transparence de ces nouvelles solutions du fait de l'existence de biais possibles par le manque de données représentatives basées sur des cohortes de patients suffisamment larges[25].

Après avoir brièvement évoqué les opportunités et les risques liés aux solutions digitales innovantes, il ne faut pas manquer de se questionner sur la nécessité, ou non, d'en sécuriser la propriété.

## II. – La propriété des outils innovants, et *in fine*, des résultats cliniques

Le développement de nouveaux algorithmes se fait généralement dans le cadre d'une collaboration entre une *startup* spécialisée dans le développement d'algorithmes d'intelligence artificielle et une société pharmaceutique, propriétaire de données confidentielles. En partant d'une technologie propriétaire, la *startup* développe un nouvel algorithme adapté au besoin exprimé par la société pharmaceutique, ledit algorithme étant ensuite « entraîné » à l'aide de données détenues par la société pharmaceutique. Plus les données seront nombreuses et labellisées, plus l'apprentissage de l'algorithme sera efficace et précis. L'algorithme entraîné sera

(23) U.S. FOOD & DRUG, Intelligence artificielle et apprentissage automatique dans le logiciel en tant que dispositif médical, janv. 2021 ; www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

(24) U.S. FOOD & DRUG, Résumé exécutif de la réunion du comité consultatif sur l'engagement des patients, 22 oct. 2020 ; www.fda.gov/media/142998/download.

(25) FDA, La FDA et Philips mettent en garde contre les biais de données dans l'IA et les appareils d'apprentissage automatique, 26 oct. 2020 ; www.medtechdive.com/news/fda-philips-warn-of-data-bias-in-ai-machine-learning-devices/587734.

ensuite capable de réaliser des prédictions qu'il faudra vérifier pour évaluer la fiabilité du modèle ainsi développé.

On voit que différents objets sont produits lors de cette collaboration : l'algorithme non entraîné développé par la *startup* et issu d'une technologie propriétaire, l'algorithme entraîné obtenu par la *startup* grâce aux données confidentielles de la société pharmaceutique, et la prédiction ou le résultat généré par l'algorithme entraîné.

La question de la propriété de ces objets et de leur utilisation devra être réglée dans le contrat de service ou de collaboration qui liera les deux parties. On peut penser que l'objectif principal de la *startup* sera de conserver la propriété de l'algorithme non entraîné et du savoir-faire acquis lors de ce développement, et de les réutiliser dans de futurs projets ; quant à la société pharmaceutique, elle souhaitera pouvoir utiliser l'algorithme entraîné (*i.e.* le modèle) et surtout détenir la propriété des prédictions ou des résultats obtenus en utilisant l'algorithme entraîné, afin de soutenir un futur développement clinique ou un enregistrement réglementaire, voire déposer un brevet.

Pour les deux parties, il est important de définir les enjeux du projet et de bien comprendre les attentes de l'autre partie pour traiter ces questions de propriété et de droit d'utilisation lors de la négociation du contrat. Il est notamment crucial d'anticiper les champs d'application techniques possibles d'un algorithme en vue de protéger son utilisation. Il est par exemple possible de laisser la propriété d'un algorithme à la *startup* qui l'a développé, mais d'obtenir une licence exclusive d'utilisation pour un cadre particulier et le droit de breveter cette utilisation.

Par ailleurs, au-delà de l'algorithme (entraîné ou non) et du résultat, on peut se poser la question de la protection du logiciel et de la technologie qui les abritent sans lesquels, dans le cas d'un projet numérique, l'algorithme peinerait à exister et le résultat peinerait à être obtenu. Une propriété ou un droit d'utilisation exclusive sur un logiciel (et son code) peut conférer un avantage compétitif indéniable à une entreprise innovante, et les sociétés pharmaceutiques sont en mesure de négocier ces dispositions parce que, sans leurs données, l'algorithme développé par la *startup* spécialisée ne pourrait ni fonctionner, ni s'améliorer. En effet, les algorithmes n'ont de vraie valeur commerciale que par la quantité de données qui y figurent, mais rappelons qu'au départ cette donnée est fournie par un expert (un scientifique, laboratoire pharmaceutique, *etc.*).

Il s'agit ici de regarder le logiciel non seulement comme le moyen d'obtenir un résultat, mais aussi comme une fin en soi, afin de pouvoir bénéficier de la protection conférée par les droits d'auteur. C'est là aussi essentiellement une question de négociation contractuelle : champ d'application des droits de licence, commercialisation, exclusivité, propriété, accès aux évolutions, redevances, et même obtention de parts dans la société numérique en question. Cela est d'autant plus vrai lorsque le produit de santé lui-même est un logiciel, pour lequel les entreprises de santé prennent financièrement en charge le développement.

Dans ce cadre, il est important de veiller à comprendre ce qui sera financé et ce qui appartiendra à l'entreprise de santé et, *a contrario*, de réfléchir aux conséquences du financement de ce qui ne lui appartiendra pas – une option très

largement proposée dans le modèle économique des sociétés du numérique. Il serait désavantageux, par exemple, de chercher à protéger uniquement les résultats générés par l'algorithme sans régler le régime du moyen technologique, donnant ainsi gratuitement la possibilité au logiciel et à l'algorithme incorporé de se perfectionner pour la concurrence.

Les situations peuvent être très différentes les unes des autres et il sera nécessaire de s'adapter. Un accès à un logiciel existant « sur étagère » (licence d'utilisation) est différent de l'adaptation d'un logiciel existant à certains besoins (développements spécifiques) ou du développement d'un nouveau logiciel qui intégrerait les données de la société pharmaceutique afin d'être commercialisé par ailleurs. Comprendre le modèle économique du partenaire numérique lors de la négociation du contrat devient alors essentiel pour s'assurer que les livrables et les enjeux du projet seront respectés.

## III. – Les brevets sur les résultats issus de l'utilisation d'une intelligence artificielle

Ces dernières années, l'augmentation des dépôts de demandes de brevet portant sur des inventions générées grâce à l'utilisation d'une IA a suscité de nombreuses questions devant les offices de brevet. La désignation de l'IA en tant qu'inventeur et le critère d'activité inventive ont notamment été au centre de l'attention.

Plusieurs juridictions nationales semblent à présent s'accorder sur le fait qu'une machine ou une IA ne peut être désignée en tant qu'inventeur.

Déposées par un particulier en 2018, les demandes de brevet EP 18275163 et EP 18275174 avaient été rejetées par l'Office européen des brevets (OEB) au motif qu'elles ne remplissaient pas l'exigence juridique, établie par la Convention sur le brevet européen (CBE), selon laquelle un inventeur désigné dans une demande doit être un être humain et non une machine. Dans les deux demandes, une IA appelée « DABUS », développée par le demandeur, était désignée comme inventeur. Or, les demandes portaient sur deux produits entièrement générés par l'IA, sans intervention humaine. Le demandeur avait déclaré avoir acquis le droit au brevet européen en sa qualité d'ayant cause de l'inventeur, faisant valoir qu'en tant que propriétaire de la machine, tout droit de propriété intellectuelle créé par celle-ci lui revenait. Dans sa décision, l'OEB a estimé que l'interprétation du cadre juridique du système du brevet européen permettait de conclure que l'inventeur désigné dans un brevet européen doit être une personne physique.

Dans une décision portant sur une demande de brevet américain correspondant (*U.S. Patent Application* No.16/524,350), l'USPTO a confirmé qu'une IA ne peut être considérée comme un inventeur, ce qui mène à la recommandation générique qu'en cas de doute, il est préférable d'identifier une personne physique comme inventeur, *e.g.*, le ou les créateurs de l'IA en question.

La question de l'impact de l'IA sur l'appréciation de l'activité inventive, l'un des critères essentiels de brevetabilité, pourrait à l'avenir se poser. En effet, une invention est considérée comme n'impliquant pas une activité inventive, et n'est donc pas brevetable, si elle découle d'une manière évidente de l'état de la technique.

Or, le recours à l'IA et aux algorithmes d'apprentissage permet de tester *in silico* infiniment plus de conditions qu'il serait possible d'envisager *in vitro* ou *in vivo*.

On peut citer par exemple la molécule DSP-1181, un nouvel agoniste de la sérotonine 5-HT1A, découverte conjointement par la *startup* Exscientia et le laboratoire pharmaceutique japonais Sumitomo Dainippon Pharma, dont la structure a été imaginée par une IA entraînée à générer de nouveaux agonistes de la sérotonine 5-HT1A. Les prédictions de l'IA se sont révélées correctes, et la molécule DSP-1181 est la première molécule imaginée par une IA à entrer en phase clinique. On peut également mentionner le cas de l'halicine, une molécule initialement développée pour le traitement du diabète, mais dont le développement a dû être arrêté. De manière indépendante, l'halicine a ensuite été identifiée par une IA développée par une équipe à la recherche de nouveaux antibiotiques parmi une bibliothèque de molécules. Cette prédiction a été vérifiée *in vitro* et chez la souris.

Ainsi, ce qui était hors de portée d'une approche conventionnelle semble à présent accessible grâce aux nouvelles technologies. Ce bond technologique permis par l'IA va-t-il entraîner un durcissement du critère *d'activité* inventive ? Est-il recommandé de divulguer dans une demande de brevet que l'invention a été permise grâce à l'utilisation d'une IA, au risque de la rendre plus « évidente » ? On peut en douter, d'autant plus qu'il n'est pas requis de décrire comment les inventeurs sont parvenus à l'invention, mais uniquement de démontrer que celle-ci résout un problème technique, de préférence de manière supérieure aux solutions de l'état de la technique.

SECTION 2

# L'ÉMERGENCE DE NOUVELLES STRATÉGIES DE CONFORMITÉ DANS LE DÉVELOPPEMENT DES PRODUITS DE SANTÉ : DE LA « DÉFIANCE » À LA « CONFIANCE »

## § 1. – L'introduction du concept d'*accountability* dans la stratégie opérationnelle des acteurs de la santé numérique : une stratégie de « défiance » *ab initio*

La première pierre de l'analyse concerne la protection des données personnelles, et en particulier des données de santé. Devenue une véritable matière, la protection des données de santé a connu un développement considérable, notamment en France, pour intégrer, avec le RGPD, le « cœur du réacteur » de tout développement clinique et médical alliant le digital. Le RGPD a changé la donne non seulement en rendant les acteurs de la santé numérique responsables, mais aussi en intégrant les risques imputables au propre développement de ces outils. C'est le principe de responsabilisation, ou « d'*accountability* ».

Si cette révolution vers une gestion responsable, délivrée de la plupart des contrôles *a priori* (les déclarations à la CNIL ont pour la majeure partie été abolies), peut être saluée comme un progrès, l'application de la réglementation applicable reste fortement imprégnée d'une défiance à l'égard des technologies, plutôt que de tenter d'intégrer celles-ci dans une « confiance numérique » assumée. Un long chemin reste à parcourir.

## I. – Le récent concept d'*accountability* introduit par la réglementation en matière de protection des données

L'*accountability*, dont la traduction française se situe à mi-chemin entre la « responsabilisation » et la « démontrabilité », désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à une réglementation. Ce concept, issu d'une logique anglo-saxonne et jusqu'alors étranger à la tradition juridique française, a fait son entrée dans plusieurs domaines réglementaires au cours des dernières années : il a par exemple émergé dans le cadre de la lutte anticorruption ou encore dans la nouvelle réglementation relative à l'encadrement des liens d'intérêt entre industriels et professionnels de santé. À ce titre, la loi n° 2016-1691, dite loi « Sapin II », la loi Bertrand en matière de transparence dans le secteur pharmaceutique, ou encore – en matière de protection des données – le RGPD, imposent tous la mise en place d'outils et de processus internes similaires, dont les acteurs doivent apporter la preuve en cas de contrôle de la part de l'autorité de régulation.

Quel que soit le secteur réglementaire concerné, l'*accountability* se fonde sur une logique commune, celle du « connais-toi toi-même ». En d'autres termes, c'est à l'entreprise d'établir son plan de conformité, sans l'aide des autorités de contrôle : en cas d'interrogations de la part des acteurs, celles-ci ne donnent pas de réponses personnalisées, mais les renvoient à leur propre interprétation des lignes directrices publiées sur leurs sites Internet. Les acteurs ne peuvent donc plus compter sur la validation *a priori* des autorités, et doivent eux-mêmes interpréter les textes et lignes directrices afin d'élaborer un plan de conformité. Il s'agit d'une véritable émancipation, mais sans contrôle *a posterori* des autorités de régulation. Par exemple, en matière de failles de sécurité, la CNIL semble privilégier une approche d'accompagnement des acteurs : ainsi, si l'entreprise notifie l'incident de sécurité dans les soixante-douze heures conformément à la réglementation applicable, la CNIL se dirigera peut-être moins facilement vers une sanction.

Dans le domaine de la santé numérique, l'*accountability* a eu un impact significatif sur l'organisation fonctionnelle et la stratégie opérationnelle de l'entreprise « responsable de traitement ».

D'une part, les acteurs de la santé numérique doivent désormais établir leurs propres plans de conformité et mécanismes permettant *in fine* de démontrer leur conformité à la réglementation de protection des données personnelles. Cette obligation de rendre compte permet de s'assurer de l'efficacité des mesures à la fois techniques et organisationnelles mises en œuvre par le responsable de traitement. La mise en conformité doit s'effectuer en collaboration avec les juristes mais

également les services techniques (« IT »). En pratique, il s'agit par exemple d'apporter la preuve de la réalisation d'une « cartographie des risques », ou d'analyses d'impact menées en interne, en amont du lancement d'un projet numérique. Il s'agit aussi de pouvoir démontrer des mesures techniques et organisationnelles adoptées pour sécuriser les données de santé, par exemple dans le cadre de transferts de données de santé vers des sous-traitants basés hors de l'Union européenne. Afin de garantir un traitement conforme des données, il est important que les mesures d'*accountability* soient révisées et mises à jour régulièrement.

D'autre part, les acteurs de la santé numérique ont désormais une compréhension un peu plus précise, même si non exhaustive, des risques associés à une mauvaise gestion des données et aux manquements des obligations d'un contrôleur de données. Cette compréhension est essentielle pour ces acteurs, maintenant qu'ils sont tenus d'être responsables de leurs actes, en acceptant le principe d'*accountability* et en assumant les responsabilités associées.

Le principe d'*accountability* permet en effet aux instances de contrôle propres à chaque pays membre de l'Union européenne de vérifier le bon respect des règles de sécurité par les entreprises et organismes publics, puisque la traçabilité et la transparence des mesures mises en œuvre grâce au principe d'*accountability* sont des points essentiels pour garantir la protection des utilisateurs. Ainsi, l'incapacité de démontrer l'existence de tels processus internes devient ainsi déjà en soi une responsabilité pour les acteurs et les expose à des sanctions pécuniaires, qui ont augmenté de façon exponentielle : qui se souvient encore qu'il y a cinq ans à peine, une condamnation à une pénalité de 100 000 € par la CNIL relevait de l'acte de bravoure, là où désormais les condamnations proposées par la CNIL aujourd'hui peuvent atteindre plusieurs dizaines de millions d'euros.

Dans tous les cas, la stratégie de conformité des acteurs de la santé numérique – induite par le principe d'*accountability* – doit nécessairement composer avec la protection des données de santé, prévue par le RGPD et les lignes directrices de la CNIL.

## II. – *L'accountability* des acteurs de la santé numérique, une notion à géométrie variable

La donnée de santé est devenue la pierre angulaire du système de santé et plus particulièrement des activités de recherche et de développement clinique. La pertinence des essais cliniques dépend en effet de la rigueur scientifique et médicale, ainsi que de l'intégrité et la sécurité des données.

En matière de protection des données, cette réalité se heurte à un hiatus dès le départ : le traitement des données concernant la santé est, en principe, interdit, en vertu de l'article 9 du RGPD, en raison du caractère sensible de ces données et des risques que leur traitement pourrait entraîner. Cette interdiction a un champ d'application particulièrement étendu, dans la mesure où le RGPD, la loi Informatique et Libertés, tout comme les lignes directrices de la CNIL proposent une définition très large de la donnée de santé. Il s'agit des données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y

compris la prestation de services de soins de santé) qui sont de nature à révéler des informations sur l'état de santé de cette personne. En d'autres termes, il peut s'agir de toute donnée pouvant concerner de près ou de loin l'état de santé de l'individu.

À défaut d'une parfaite maîtrise de la part des acteurs collectant et gérant des données de santé, le risque juridique est grand, d'autant que la mise en œuvre de solutions digitales connectées devient laborieuse et potentiellement dangereuse. En effet, les risques de violation des données sont nombreux, quelles que soient les réglementations applicables. Outre-Atlantique, l'*American Medical Collection Agency* (AMCA) a subi une violation de données de huit mois. LabCorp et Quest Diagnostics ont utilisé l'AMCA comme une agence de recouvrement. L'AMCA était alors le responsable de traitement de millions de données sensibles. En mars 2019, l'AMCA a découvert avoir subi une cyberattaque exceptionnellement longue et minutieuse. Les cybercriminels ont réussi à infiltrer les systèmes d'information d'AMCA pendant de longs mois pour y exploiter les précieuses données privées. 24,4 millions de données personnelles et vingt et une entreprises ont été touchées par la violation.

Au sein de l'Union européenne, la relation avec les communautés de patients peut également s'avérer compliquée. En 2018, il a été établi que Facebook avait révélé par inadvertance des informations médicales sensibles contenues au sein du groupe fermé « BRCA (BReast Cancer) Sisterhood » créé en tant que réseau de soutien pour les femmes atteintes du gène BRCA, une mutation qui augmente considérablement le risque de cancer du sein, entraînant souvent une mastectomie préventive.

En France également, la CNIL est en train d'explorer son pouvoir de sanction, en condamnant des sociétés pour lesquelles ont été observés non pas un manquement ponctuel et délimité dans le temps, mais des violations continues. Si, avant l'adoption du RGPD, la CNIL était limitée dans le montant de sa sanction à 800 000 €, puis à 3 millions d'euros, les montants sont désormais significatifs puisque la CNIL peut aller jusqu'à 4 % du chiffre d'affaires. Force est de constater une augmentation progressive des amendes depuis mai 2018. La CNIL a par exemple condamné la société Optical Center à une amende de 150 000 € à la suite de « fuites » de données de santé, sur le fondement de la loi Informatique et Libertés, ou encore la société Uber à 400 000 € pour manquement aux obligations de sécurisation des données personnelles. La CNIL témoigne également désormais de sa volonté ne pas laisser impunis les « géants du web » : elle vient par exemple de condamner le 7 décembre 2020 les sociétés Google LLC et Google Ireland Limited à la somme de 100 millions d'euros d'amende notamment pour avoir déposé des cookies publicitaires sans avoir correctement recueilli le consentement préalable des utilisateurs, ni les avoir informés de manière satisfaisante. Cette condamnation suit les condamnations des sociétés Carrefour et Amazon sur des fondements similaires. Les risques découlant de l'application de mesures de sécurité insuffisantes s'appliquent donc désormais à tous les acteurs traitant des données personnelles, ce qui rend la démarche d'*accountability* d'autant plus nécessaire.

En matière d'essais cliniques, l'*accountability* du promoteur s'étend à ses sous-traitants, et est essentielle pour se prémunir des risques de contentieux. Toutefois,

cette *accountability* doit ici dépasser le domaine des données personnelles, pour se penser plus largement en termes de responsabilité scientifique, clinique et médicale. Les acteurs de la santé numérique doivent à cet égard faire preuve d'une très grande rigueur scientifique et transparence, et le sponsor doit être garant de l'intégrité scientifique de ses études.

À ce titre, la Déclaration d'Helsinki, élaborée par l'Association Médicale Mondiale, insiste sur la responsabilisation des acteurs dans le cadre des essais cliniques. Elle énonce notamment, parmi les principes éthiques applicables à la recherche médicale impliquant des êtres humains, les obligations et la responsabilité du promoteur quant à la publication et à la dissémination des résultats : « Les chercheurs ont le devoir de mettre à la disposition du public les résultats de leurs recherches impliquant des êtres humains. Toutes les parties ont la responsabilité de fournir des rapports complets et précis. (…). Les résultats aussi bien négatifs et non concluants que positifs doivent être publiés ou rendus publics par un autre moyen ». En pratique, il suffit de se remémorer les affaires *Rosiglitazone* et *Rofecoxib* pour comprendre les enjeux de l'intégrité scientifique et de la transparence. Sans la nécessaire obligation de transparence et d'accès aux données, ces deux affaires auraient pu ne jamais être révélées.

C'est dans ce contexte également que la notion de l'intégrité des données (*data integrity*) prend tout son sens, popularisée sous le sigle ALCOA dans l'industrie pharmaceutique. Les données doivent en effet être attribuables (*Attribuable*), lisibles (*Legible*), contemporaines (*Contemporaneous*), originales (*Original*) et fiables (*Accurate*). Cette exigence est désormais pleinement appliquée par les autorités réglementaires aux acteurs de l'industrie pharmaceutique, comme l'illustrent la ligne directrice émise par la FDA en réponse aux lacunes constatées lors des inspections (*Data Integrity and Compliance with drug CGMP. Questions and Answers Guidance for Industry*, December 2018) ou encore les questions-réponses de l'EMA sur les bonnes pratiques de fabrication et de distribution (*cf. Data Integrity*, August 2016).

## III. – L'*accountability* des acteurs de la santé numérique face aux défis de l'innovation

L'une des principales difficultés que doivent prendre en compte les acteurs de la santé numérique concerne l'éventuel décalage temporel entre la réglementation et l'innovation numérique. En effet, la réglementation a, par définition presque, un temps de retard par rapport au mouvement constant de digitalisation des acteurs de la santé numérique et des moyens numériques que ceux-ci souhaitent utiliser, notamment dans le cadre de la recherche clinique et du suivi de santé des patients. Ce décalage temporel se traduit en pratique par une certaine « défiance » de la réglementation en matière de protection des données, qui, au nom de la sécurisation des flux de données, entre en conflit avec d'autres intérêts légitimes, jusqu'à la protection de la santé elle-même. En effet, certaines mesures de sécurité techniques et organisationnelles voulues par le RGPD et appliquées aux données de santé peuvent, si elles sont appliquées trop strictement, entraîner une « sur-protection » des données.

En effet, la sécurisation des données, bien entendu nécessaire, peut conduire à des situations totalement ubuesques en pratique et constituer des obstacles tels que seule la « débrouille » peut ici permettre le fonctionnement des équipements concernés. À titre d'exemple, la réglementation relative à l'hébergement de données de santé, qui est propre à la France, requiert, là où les acteurs de la santé numérique travaillent avec des GAFA (parfois non certifiés) sur les autres marchés, que les mêmes acteurs fassent appel à des hébergeurs agréés/certifiés HDS. Pour que les hôpitaux puissent accéder à ces données hébergées, il faut prévoir une authentification forte et des sessions limitées dans le temps. Que faire en cas de vol ou de perte du badge, en cas d'absence du médecin ? Le patient devra-t-il rester bloqué hors de la salle d'opération ? Si l'authentification est faite *via* la combinaison d'un code secret et d'un *One time password* reçu par téléphone, que faire si le téléphone ne capte pas quand la salle d'opération est au sous-sol ? Et le chirurgien n'a pas à être sur son ordinateur, mais auprès de son patient : une session limitée dans le temps conduit à lancer des fils sur les disques pour prolonger la session. La sécurisation est-elle vraiment bien pensée ici ?

De même, de nombreuses questions se posent concernant la stratégie de sécurisation et de verrouillage des dispositifs médicaux connectés et autres applications de santé connectées utilisés par les hôpitaux et les médecins afin de permettre le suivi de l'état de santé des patients. Jusqu'où doit-on sécuriser l'accès du médecin à l'application ou au dispositif ? L'accès aux bases de données de santé peut-il être donné aux équipes informatiques devant assurer la maintenance du dispositif en situation d'urgence ?

Par ailleurs, une application trop zélée des dispositions relatives à la protection des données de santé ne doit pas entraver les projets de recherche, par exemple en mettant à mal tout transfert de données. C'est la position qui semble avoir été adoptée par le Conseil d'État concernant l'hébergement des données de la plateforme publique dite *Health Data Hub*, dans une récente décision du 13 octobre 2020, à la suite de l'interdiction de tout transfert de données basé sur le *Privacy Shield* par la Cour de justice de l'Union européenne (décision *Shrems II*). Le *Health Data Hub* est une plateforme digitale mise en place afin de favoriser le partage des données dans le cadre de la recherche. Récemment, certaines de ces données ont été utilisées à des fins de gestion des urgences sanitaires et d'amélioration des connaissances sur le virus Covid-19. Le 15 avril 2020, la plateforme a signé un contrat d'hébergement avec une filiale irlandaise de la société américaine Microsoft. Le Conseil d'État a considéré que l'activité d'hébergement des données pouvait se poursuivre, dans la mesure où les données n'étaient pas transférées vers les États-Unis (en vertu du contrat signé avec Microsoft, mais également en vertu d'un arrêté ministériel du 9 octobre 2020). Dans ce contexte, le juge français a donc considéré que les services ne devaient pas être interrompus, étant donné leur importance dans le cadre de la crise sanitaire et des mesures de sécurité, et notamment de pseudonymisation, mises en œuvre pour sécuriser les données. Mais le risque qu'il en soit autrement demeure sur le fond, comme le montrent les recommandations de la CNIL, qui visent à choisir des hébergeurs en Europe et à ne contracter qu'avec des prestataires européens.

Les contrôles diligentés par les autorités réglementaires et le risque accru de sanctions ont conduit les acteurs de la santé numérique à adopter dans un premier temps une logique préventive « de défiance » dans le cadre du traitement de leurs données de santé, face à la digitalisation constante du monde de la santé. Selon la Commission européenne, le manque de confiance dans le « partage des données » serait un obstacle majeur. Au sein de l'Union européenne, les acteurs de la santé numérique se doivent d'élaborer une stratégie de « confiance » dans leur manière d'appréhender la protection des données personnelles, afin que leurs projets de santé digitaux ne soient pas entravés par une application trop stricte de la réglementation.

## § 2. – Vers une élaboration au cas par cas de la stratégie de conformité des acteurs de la santé numérique : vers une stratégie de « confiance »

### I. – Une réflexion à mener autour des différentes finalités et bases légales ouvertes aux acteurs de la santé numérique dans le cadre du traitement des données de santé

Les acteurs de la santé numérique sont régulièrement confrontés, par une réglementation défiante face aux technologies, à devoir peser les intérêts en présence, faire peser « la santé face aux données de santé ». Autrement dit, la conformité induite par le RGPD ne peut pas prendre les allures d'un travail simplement « bureaucratique » consistant à « cocher des cases », tellement bureaucratique qu'il viendrait en collision avec un protocole de soins efficace. Afin d'éviter cet écueil – qui ne permettrait pas de faire face aux enjeux du *big data* –, la conformité doit se baser structurellement sur une relation de confiance. C'est l'idée fondamentale du « connais-toi toi-même » induite par le RGPD.

Il y a ici d'abord une réflexion à mener autour des différentes ***bases légales*** ouvertes à l'entreprise dans le cadre du traitement des données de santé à des fins de recherche clinique. En effet, pour traiter des données de santé, il faut « lever » l'interdiction de traitement des données de santé prévue par l'article 9 du RGPD. Différentes options et stratégies s'offrent aux acteurs pour adapter la contrainte réglementaire attachée aux données de santé. Il peut s'agir d'identifier plus précisément les finalités pour lesquelles les données peuvent être collectées et traitées, mais également de réfléchir en amont aux mesures de sécurité techniques et organisationnelles pouvant être envisagées.

Dans un premier temps, il revient à l'entreprise responsable de traitement d'**identifier les types de données personnelles qu'elle est en droit de traiter, et de déterminer pour quelles finalités** elle a le droit de le faire, dans le respect du principe de « minimisation » instauré par le RGPD. À ce titre, il est possible de percevoir une « hiérarchisation » dans la sensibilité des données de santé. Certaines données de santé peuvent en effet faire l'objet de règles strictes, et d'une vigilance

particulière selon l'État membre de l'Union européenne concerné. En France, c'est par exemple le numéro d'inscription au répertoire (NIR) national d'identification, communément appelé « numéro de sécurité sociale », qui ne peut être traité que par certaines catégories déterminées de responsables de traitement, et pour des finalités bien définies. De plus, la réglementation en matière de données personnelles a prévu de nombreuses exceptions à l'interdiction du traitement des données de santé, que les acteurs se doivent d'identifier et de tenter d'exploiter, notamment dans le cadre de la recherche scientifique. Ceci implique de se demander – au cas par cas – si le traitement des données de santé peut être fondé sur l'une des bases légales prévues par le RGPD, tels que le consentement explicite du patient au traitement de ses données personnelles pour une finalité donnée, ou des motifs d'intérêt public, dans le cadre d'une recherche scientifique.

Dans le cadre de la recherche clinique, le promoteur doit donc s'interroger sur les bases légales qu'il peut utiliser, et sur leur bonne utilisation. Ainsi, lors de la collecte du consentement du patient, le promoteur doit s'assurer de travailler ses formulaires de consentement afin d'offrir une information lisible et compréhensible, faute de quoi il existe un risque d'acceptation d'office de la part des patients, qui ne seraient pas suffisamment informés. Mais le consentement du patient à l'essai clinique est-il réellement libre et éclairé, face à la potentielle opacité des algorithmes utilisés dans le cadre de l'essai clinique ? Cette question se pose d'autant plus que toute atteinte aux données personnelles de santé du patient peut avoir des conséquences majeures pour celui-ci, telles que des risques potentiels de discrimination dans le cadre de l'accès aux soins.

La question des bases légales se pose également si les promoteurs sont amenés à se demander dans quelle mesure ils pourraient réutiliser les données issues de précédents essais cliniques. Schématiquement, trois questions principales sont à prendre en considération pour préciser les frontières de l'action juridique. Tout d'abord, comment rendre compte de décisions et en préciser les responsabilités, lorsqu'elles sont issues d'algorithmes souvent caractérisés par leur opacité ? Par ailleurs, quels sont les risques de discrimination envers des personnes protégées ou groupes sensibles ? Enfin, comment évaluer l'équilibre bénéfice/risque entre l'intérêt public, d'une part, et le risque pour la vie privée des personnes touchées par l'utilisation de leurs données personnelles, d'autre part ?

Les possibles éléments de réponses conduisent à des recommandations déontologiques ou réglementaires indispensables à la transparence des outils utilisés, face au patient. Il s'agit de mettre en œuvre une protection drastique des données de santé, notamment génétiques, et de leurs utilisations. Ceci implique nécessairement de s'assurer de la rigueur scientifique des pratiques de recherche pour produire des résultats reproductibles, et donc scientifiques, mais également d'expliciter le protocole d'information des patients.

Par ailleurs, les acteurs de la santé numérique doivent également s'interroger sur les ***finalités*** du traitement des données personnelles, et des finalités de l'essai clinique en général. Cette question des finalités du traitement peut notamment se poser très concrètement dans le cadre de l'utilisation de produits du corps humain à une fin médicale ou scientifique autre que celle pour laquelle ils ont été prélevés.

À ce titre, des règles spécifiques existent. Selon l'article L. 1211-2 du Code de la santé publique, un changement de finalité est possible, sous réserve que la personne soit dûment informée au préalable de cette autre fin et ait la possibilité de s'y opposer, et avec l'accord du Comité de protection des personnes : « Le prélèvement d'éléments du corps humain et la collecte de ses produits ne peuvent être pratiqués sans le consentement préalable du donneur (…) L'utilisation d'éléments et de produits du corps humain à une fin médicale ou scientifique autre que celle pour laquelle ils ont été prélevés ou collectés est possible, **sauf opposition exprimée par la personne sur laquelle a été opéré ce prélèvement ou cette collecte, dûment informée au préalable de cette autre fin** ».

La question des finalités implique, plus abstraitement, de prendre le recul nécessaire afin de peser les intérêts en présence : par exemple, l'intérêt public ou le bien commun attendu de la recherche en comparaison des risques encourus par l'ouverture de l'accès aux données personnelles. Cette réflexion concerne également le but ultime des solutions e-santé : la protection de la donnée de santé peut-elle dans certaines situations s'avérer être un obstacle à la protection de la santé ? Au-delà des exigences relatives à la protection des données personnelles, l'entreprise responsable de traitement ne doit pas perdre de vue la finalité même de la solution innovante qu'elle a pu déployer : la santé des personnes concernées. L'invalidation du « Bouclier de protection des données UE-États-Unis », dit *Privacy Shield*, implique ainsi que les solutions de santé innovantes proposées par des sociétés américaines et prévoyant des transferts de données vers les États-Unis et basées jusqu'alors sur le *Privacy Shield*, soient modifiées : les process internes doivent être modifiés et prendre appui sur un autre mécanisme de transfert. Cette mise en conformité avec la nouvelle réglementation peut dans certains cas prendre plusieurs mois. Mais le cadre réglementaire ne facilite pas pour le moment la tâche aux acteurs de la santé numérique : les mesures de sécurité recherchées ne sont pas nécessairement clairement définies.

## II. – Une réflexion à mener autour des mesures de sécurisation des flux de données de santé

En amont de tout projet digital impliquant des données de santé, il est indispensable de **déterminer quelles mesures de sécurité techniques et organisationnelles pourraient être envisagées** pour assurer un niveau de sécurité suffisant. Ces mesures impliquent, par exemple, d'avoir recours à un hébergeur de données de santé certifié, dans le cas d'un hébergement de données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social et entrant dans le champ de l'application de l'article L. 1111-8 du Code de la santé publique.

Il en va de même dans le cadre de transferts de données, notamment lorsque des données de patients européens sont transférées vers des pays situés hors de l'Union européenne, comme les États-Unis. À cet égard, de récents bouleversements réglementaires à la suite de l'invalidation du *Privacy Shield* par la Cour de justice de l'Union européenne ont mis en avant la nécessité de revoir les mécanismes mis

en place ou de prévoir des garanties supplémentaires pour encadrer les transferts de données vers les États-Unis. Ces bouleversements ont des répercussions systémiques considérables, puisqu'ils vont affecter tout transfert de données hors UE par la révision des clauses contractuelles types.

Dans ce contexte, il est plus que jamais indispensable de **prendre en compte les risques liés à l'externalisation**, ce qui implique, notamment dans le cadre de la réalisation des essais cliniques, une transparence accrue des transferts de données avec toute partie prenante. La recherche et le développement ont toujours été dépendants du partage des données pour confirmer ou infirmer de nouvelles hypothèses de recherches ou ouvrir de nouvelles opportunités. Ce mouvement est encouragé par les autorités *via* des obligations de transparence de plus en plus présentes (*cf.* Lignes directrices de l'EMA relatives à la publication des données cliniques). Le partage de données doit alors être anticipé et se faire de manière maîtrisée, responsable, encadrée et précise. La question n'est pas tant l'identification du propriétaire de la donnée, mais celle des droits et responsabilités du responsable de traitement de la donnée.

Ceci implique la nécessité d'établir un plan de partage des données, qui doit être élaboré au lancement de l'essai clinique. Ce plan de partage des données prévoit notamment quelles données spécifiques seront partagées et à quel moment particulier de l'essai clinique. Au regard des obligations de transparence de plus en plus prononcées, ce plan devra prévoir des justifications solides à toute tentative de limitation de partage des données. Les différents acteurs intéressés par le partage des données générées lors des essais cliniques peuvent être les participants à l'essai clinique comme les patients, les comités de recherche éthique, les comités de revue des données, les promoteurs, les agences réglementaires (EMA, FDA…), les investigateurs comme les spécialistes des essais cliniques et analystes, les institutions de recherche et académiques, les journaux scientifiques et les sociétés savantes.

À l'autre bout de la chaîne, la relation avec les patients, au gré de l'évolution de la réglementation sur les données personnelles, revêt une importance critique : rien n'est plus possible sans un consentement éclairé que le RGPD a considérablement renforcé. Ce consentement est stratégique car il doit éviter l'écueil de « figer » l'essai dès le départ : si le consentement est trop restreint, il bloquera l'avancée de la recherche clinique. Afin de pallier ce risque, les consentements des patients doivent alors être rédigés de telle sorte qu'ils permettent une réutilisation des données pour des finalités ultérieures de recherches non incompatibles avec la finalité première.

Les systèmes d'informations technologiques et les procédures d'écosystème des données doivent permettre quant à eux la fluidification du partage des données dans le strict respect des règles de conformité et de sécurité informatique. Une telle politique de partage des données a nécessairement un coût, mais le bénéfice au regard du potentiel offert par les solutions digitales innovantes est conséquent. La maîtrise du partage des données est elle aussi critique, eu égard au risque croissant, tant financier que réputationnel, lié à une politique de partage de données non maîtrisée.

Maîtriser le partage des données, c'est s'assurer, par une sélection rigoureuse des partenaires, comme les sous-traitants, dit « CRO » (*Clinical Research Organisation*),

que leurs systèmes d'infrastructure de l'information et de la communication soient suffisamment sécurisés et flexibles pour permettre la fluidification des données tout en offrant une sécurité optimale pour le contrôleur des données.

Parmi tant d'autres, la compétence juridique de la CRO en matière de données personnelles devra être un critère de sélection important lors des appels d'offres. Un cahier des charges clair et précis sur la prérogative de la CRO en termes de négociation des clauses relatives aux données personnelles et à la responsabilité dans les contrats avec les centres investigateurs devra nécessairement être inséré dans le contrat entre le promoteur et la CRO. En effet, il en va de la responsabilité du promoteur d'être le garant de l'intégrité des données personnelles de santé des patients ; dans un contrat le promoteur et le CRO vont à présent négocier leurs rôles respectifs et leurs responsabilités, puisque le RGPD a ouvert un nouveau chantier de responsabilisation des acteurs par le biais des contrats de traitement de données (*data processing agreement*).

Les enjeux ne sont pas neutres : en effet, le promoteur, en qualité de contrôleur des données, doit être capable de démontrer que ses activités de traitement sont conformes aux principes de protection des données prévus par le RGPD ou toute autre réglementation applicable, telle que l'HIPPA aux États-Unis. Il est alors important que les contrats soient parfaitement négociés, notamment en termes de conformité aux réglementations de données personnelles avec des clauses de responsabilité adaptées aux enjeux. La CRO, en fonction de son autonomie dans la conduite de l'essai clinique, résistera à la qualification de coresponsable de données pour privilégier la position moins risquée, mais désormais également exposée à la suite du RGPD, de sous-traitant. Cet enjeu est d'autant plus complexe dans un contexte international où le promoteur peut être situé en Europe et les centres investigateurs sur un autre continent. Se poseront alors inévitablement des questions relatives à l'applicabilité territoriale de telle ou telle réglementation. La voie ouverte par certaines réglementations américaines considérées comme particulièrement intrusives en Europe, telles que la réglementation américaine anticorruption FCPA, a été empruntée par de nombreux autres pays.

Par ailleurs, un autre rempart de protection pouvant être envisagé par les acteurs de la santé numérique pourrait consister à vouloir tout simplement « sortir » la donnée du champ d'application de la réglementation relative aux données personnelles, par le biais de mesures d'anonymisation. L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit, et ce de manière irréversible. Lorsque l'anonymisation est effective, le RGPD ne s'applique plus aux données ainsi anonymisées, celles-ci n'étant dès lors plus à caractère personnel. En d'autres termes, les données personnelles doivent subir un traitement suffisamment fort permettant de les rendre irréversiblement non identifiantes.

Ce procédé ne doit pas être confondu avec la technique dite de la « pseudonymisation », permettant de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe, mais qui permet bien souvent de ré-identifier les personnes concernées, grâce à des données tierces. En pratique, la pseudonymisation consiste simplement à remplacer les données directement identifiantes (nom, prénom, *etc.*)

d'un jeu de données par des données indirectement identifiantes (alias, numéro dans un classement, *etc.*). Ainsi, les données pseudonymisées demeurent des données personnelles. Contrairement à la pseudonymisation – opération réversible –, l'anonymisation pourrait constituer un moyen pour transmettre des données pour une utilisation secondaire, puisque ces données ne sont pas visées par la réglementation relative aux données personnelles. Ainsi, des pratiques exemplaires en matière d'anonymisation permettront de faire en sorte que les données, qui sont un élément essentiel de l'activité économique de l'entreprise de santé, soient rendues disponibles de manière responsable. Cependant, en pratique, cette affirmation doit être nuancée eu égard à la fiabilité des mécanismes d'anonymisation mis en œuvre. Ainsi, à partir de quand peut-on considérer que l'on est face à une solution anonyme suffisante ? La notion d'irréversibilité de l'anonymisation pose un vrai problème de sécurité où l'on voit se confronter la sécurité de donnée de santé avec la santé.

## III. – Question ouverte sur la propriété et la responsabilité dans le cadre de solutions innovantes utilisant de l'intelligence artificielle

En droit français, les algorithmes ne disposent pas d'un régime juridique particulier. Par conséquent, il convient de faire appel aux principes juridiques de droit commun lors de la rédaction de contrats avec des entreprises d'intelligence artificielle, d'autant plus que l'algorithme ne peut se restreindre à sa définition mathématique au vu de sa valeur commerciale considérable.

L'algorithme en tant que principe mathématique est considéré comme étant « une idée de libre parcours »[(26)], par conséquent non protégeable par le droit d'auteur. Si le droit d'auteur permet de protéger le logiciel support de l'algorithme, il ne permet pas de protéger l'algorithme en lui-même. En effet, « seule l'expression d'un programme d'ordinateur est protégée par le droit d'auteur, les idées et les principes qui sont à la base (…) des algorithmes (…) ne sont pas protégés »[(27)]. Quant aux « théories scientifiques, les méthodes mathématiques ainsi que les programmes d'ordinateur »[(28)], ces derniers sont expressément exclus de la brevetabilité par le Code de la propriété intellectuelle. Conception confirmée par la jurisprudence[(29)] et actée par la directive 2009/24/CE relative à la protection juridique des programmes d'ordinateur[(30)].

Néanmoins, l'algorithme est, par nature, destiné à être intégré au code source des logiciels ou d'une invention brevetable, ce qui permet de le protéger, indirectement, par la propriété intellectuelle. En effet, la protection des logiciels est

(26) H. Desbois, *Le droit d'auteur en France : RID comp.* 1967, 19(1), 305-306.
(27) CJUE, 2 mai 2012, aff. C-406/10, *SAS Institute Inc./World Programming Ltd.*
(28) CPI, art. L. 611, 1°.
(29) Cass. 1re, 14 novembre 2013, MM. X et Y c/ *Microsoft*, n° 12-20687 – CA Paris, 24 nov. 2015, n° 13/24577. – CA Caen, ch. app. corr., 18 mars 2015, XXX c/ *Skype*.
(30) INPI, *La propriété intellectuelle et la transformation numérique de l'économie*, 2015 (www.inpi.fr/fr/la-propriete-intellectuelle-et-la-transformation-numerique-de-l-economie).

admise[31], et a été confirmée par l'arrêt *Pachot* de 1986 qui a permis à la Cour de cassation de confirmer qu'un logiciel peut être protégeable dès lors que son code source comporte « la marque de l'apport intellectuel »[32] du concepteur. Ainsi l'algorithme intégré au code source d'un logiciel pourrait, par accessoire, bénéficier de la protection accordée aux logiciels. Cependant, cette protection reste partielle, car l'algorithme contenu dans le logiciel doit avoir une fonction plus importante à la simple exécution de ce dernier. En ce sens, la Cour de cassation a écarté le droit d'auteur comme mesure de protection des algorithmes, en considérant que « les intéressés n'avaient fourni aucun élément de nature à justifier de l'originalité des composantes du logiciel, telles que les lignes de programmation, les codes ou l'organigramme, ou du matériel de conception préparatoire »[33]. En revanche, la brevetabilité de l'algorithme de façon indirecte est possible. En effet, l'Office européen des brevets (OEB) a considéré que les inventions mises en œuvre par un ordinateur, dès lors qu'elles comportent un caractère technique, ne sont pas exclues de la brevetabilité et peuvent faire l'objet d'un brevet si les conditions de brevetabilité sont réunies, à savoir que l'invention elle-même apporte une solution technique nouvelle, non évidente, et susceptible d'application industrielle[34]. De tels brevets peuvent ainsi protéger l'utilisation à des fins techniques d'un algorithme ou d'un logiciel.

L'Office européen des brevets ne fait pas de distinction entre un algorithme « classique » et un algorithme d'intelligence artificielle ou d'apprentissage automatique (*machine learning*). Ainsi, un algorithme de reconnaissance d'image, qu'il soit entraîné ou non, ne pourra être breveté en tant que tel ; en revanche, son utilisation pour détecter un cancer de la peau ou une rétinopathie peut l'être (*cf. Orientations de l'*Office Européen des Brevets dans ses Directives, section G-II 3.3). De la même manière, un réseau neuronal, aussi innovant soit-il, n'est pas brevetable en tant que tel, mais son utilisation dans un appareil de surveillance cardiaque pour détecter des battements irréguliers apporte une contribution technique et est donc potentiellement brevetable.

Enfin, la protection des algorithmes la plus courante demeure celle accordée aux secrets d'affaires ou informations hautement confidentielles, qui peuvent être protégées contractuellement. En effet, les dispositions de la directive (UE) 2016/943 sur le secret d'affaires[35] créent un régime propre au secret d'affaires, distinct de celui de la propriété intellectuelle. Ainsi, le secret d'affaires permet d'accorder aux algorithmes une protection juridique plus adaptée et efficace visant à pérenniser leur usage, et par conséquent leur valeur commerciale. Néanmoins, cette notion de secret d'affaires est à mettre en perspective avec les principes de loyauté et d'explicabilité évoqués précédemment.

(31) CPI, art. L. 112-2, 13°.
(32) Cass. ass. plén., 7 mars 1986, n° 84-93.509 : *D.* 1986, 406, note B. Edelman ; *RTD com.* 1986, 399, obs. A. Françon ; *JCP* G 1986, II, 20631, note J.-M. Mousseron, B. Teyssié et M. Vivant.
(33) Cass. 1re civ., 14 nov. 2013, n° 12-20.687.
(34) OEB, 21 avr. 2004, T-0258/03, *Auction method/HITACHI*.
(35) PE et Cons. UE, dir. (UE) 2016/943, 8 juin 2016, sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Texte présentant de l'intérêt pour l'EEE).

De plus, comme pour tout contrat, le paiement d'une somme sous-entend l'exécution par l'autre partie d'un travail déterminé, et donc la fourniture d'un livrable. *Quid* de la propriété de cette œuvre issue du travail d'un algorithme ? En effet, l'algorithme est un programme informatique conçu par une personne physique ou morale, alimenté par une vaste sélection de données préexistantes, afin que l'algorithme fasse sa propre synthèse et produise un résultat. Par raisonnement juridique, on pourrait logiquement assimiler l'œuvre de l'algorithme à ce que l'on appelle des « œuvres dérivées » ou encore « composites »[36]. Or, ces notions nécessitent l'existence d'un auteur. L'algorithme étant un principe mathématique, et non une personne, il ne peut être considéré comme auteur de l'œuvre dérivée[37]. En effet, « l'œuvre étant une création intellectuelle, seule une personne physique peut être auteur, car une personne morale, création juridique, n'a pas d'esprit et donc *a fortiori* pas d'esprit créatif »[38].

En droit, le fait qu'une « chose » soit à l'origine d'autres « choses » n'est pas une exception. De tout temps, il existe des « choses » non détentrices d'une personnalité juridique, et pourtant productrices de richesses. En ce sens, l'article 547 du Code civil énonce dans le chapitre « Du droit d'accession sur ce qui est produit par la chose » plusieurs catégories de fruits susceptibles d'être produits : naturels ou industriels, civils ou encore le croit des animaux. Le Code civil définit le droit d'accession comme « la propriété d'une chose soit mobilière, soit immobilière, donne droit sur tout ce qu'elle produit, et sur ce qui s'y unit accessoirement soit naturellement, soit artificiellement »[39]. Ainsi le propriétaire d'une chose le devient par accession de l'ensemble de ce qui est dérivé de la chose, « en réalité, le droit qu'a le propriétaire de percevoir les fruits de la chose est la conséquence même de son droit de propriété »[40]. Dans le cadre des algorithmes, on retrouve, d'une part, les concepteurs de l'algorithme et, d'autre part, l'entreprise pharmaceutique qui a fourni à l'algorithme les données, les deux demeurant propriétaires de leurs œuvres originaires[41]. À partir de celles-ci l'algorithme produit un résultat, un modèle entraîné à détecter la « réactivité » d'un patient à un traitement par exemple. Ils pourront donc être considérés copropriétaires par accession des « fruits industriels » produits par le système algorithmique.

Enfin, pour des questions d'assurance, il est important d'identifier quels fondements juridiques sont susceptibles d'être invoqués pour obtenir l'indemnisation d'un dommage causé par cet algorithme. En principe, en cas de dommages causés à un tiers, deux acteurs sont impliqués, à savoir le développeur et l'utilisateur. Le développeur est la personne à l'initiative de la conception de l'algorithme ; quant à l'utilisateur, il s'agit de la personne qui utilise l'objet technique basé sur un algorithme[42].

(36) CPI, art. L. 113-2, al. 2 et art. L. 113-4.
(37) CPI, art. L. 113-1.
(38) C. Baranes, Avocat Contrefaçon et Droit des affaires, chargé d'enseignement à l'Université Paris 1 Panthéon Sorbonne. – P.-Y. Gautier, *De la propriété des créations issues de l'intelligence artificielle : JCP* G 2018, 37.
(39) C. civ., art. 546.
(40) W. Dross, *Les choses*, LGDJ, 2012, n° 16, « Les fruits sont une utilité de la chose ». – F. Zenati-Castaing et Th. Revet, *Les biens*, PUF, 3e éd. 2008, n° 126. – C. Grimaldi, *Droit des biens*, LGDJ, 2016, n° 38.
(41) CPI, art. L. 112-3.
(42) L. Godefroy, *Les algorithmes : quel statut juridique pour quelles responsabilités ? : Comm. com. électr*. nov. 2017, n° 11.

Les algorithmes d'automatisation, enfermés dans un fonctionnement prédéfini sont susceptibles d'être régis par les régimes actuels de responsabilités en cas d'éventuels dommages. Dans un premier temps, on peut écarter la responsabilité du fait des produits défectueux[43] puisqu'un algorithme n'est pas un produit au sens de la directive ; de même pour l'entité immatérielle dont il permet l'action. En revanche, si l'algorithme anime une entité matérielle, on peut imaginer la personne victime d'un dommage mettre en cause le fabricant en invoquant un défaut de sécurité préexistant à sa mise en circulation, fabricant qui pourra à son tour se retourner contre le concepteur de l'algorithme dans l'hypothèse où le dommage serait attribuable à un défaut dans la programmation de ladite entité. Néanmoins, si la responsabilité du fait des produits défectueux n'est pas applicable, on peut envisager de mettre en œuvre la responsabilité du fait des choses[44]. Ici, la mise en œuvre de cette responsabilité suppose de rapporter la preuve du rôle actif de cet algorithme au moment de l'apparition du dommage. Nonobstant l'apport de cette preuve, l'identification du gardien de la chose est d'autant plus compliquée. *Quid* de savoir si, dans le cadre des algorithmes, le concepteur et l'utilisateur ont réellement un pouvoir de direction sur l'algorithme lors de la survenance du dommage. En effet, ils ne contrôlent pas l'entité qui, elle, répond à un comportement automatique en exécutant une succession d'instructions préétablies. Enfin, la responsabilité du fait personnel[45] peut être envisagée si on estime que le concepteur a compromis le fonctionnement de l'algorithme en question en présentant des données inappropriées, ne correspondant pas aux données choisies par le laboratoire pharmaceutique, par exemple le mauvais essai clinique. À charge pour le développeur ou l'utilisateur de démontrer l'absence de faute. Cependant, il faut se rappeler que l'algorithme renferme ce que l'on appelle une « boîte noire », ainsi le processus qui mène au dommage en question peut être difficile à prouver.

Par opposition, les algorithmes d'apprentissage recèlent « une certaine marge d'indétermination »[46], ce qui complique l'application des régimes de responsabilité traditionnels. Néanmoins, dans l'hypothèse où une entité matérielle causerait un dommage ou présenterait un défaut de sécurité préexistant à sa mise en circulation, on pourrait appliquer les règles de la responsabilité du fait des produits défectueux. À défaut, la victime pourra invoquer le régime de responsabilité du fait des choses dès lors qu'au moment de l'apparition du dommage, l'utilisateur détenait un pouvoir de direction sur la « chose ». De plus, l'algorithme étant considéré comme une « chose », dans l'hypothèse où ce dommage serait lié à l'autonomie de ce dernier, on pourrait envisager de mettre en œuvre le régime de responsabilité du fait des animaux. Ce régime prévoit une présomption de garde entre le propriétaire de la « chose » et la personne qui est pourvue d'un réel pouvoir de contrôle sur l'animal ou la « chose ». Nonobstant la qualification de « chose », une entité

(43) Cons. UE, dir. 85/374/CEE, 25 juill. 1985, relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux.
(44) C. civ., art. 1242, al. 1er.
(45) C. civ., art. 1240 et 1241.
(46) L. Godefroy, *Les algorithmes : quel statut juridique pour quelles responsabilités ? : Comm. com. électr.* nov. 2017, n° 11.

matérielle ne peut être assimilable à un animal, être vivant doué de sensibilité[47]. D'autre part, comme pour les algorithmes d'automatisation, dans l'hypothèse où le comportement dommageable serait consécutif à une faute due soit à la programmation initiale, soit à une utilisation inadéquate, alors on pourrait envisager la mise en cause de la responsabilité du fait personnel aussi bien du concepteur que de l'utilisateur[48]. Cependant, les algorithmes d'apprentissage sont caractérisés par une certaine autonomie décisionnelle. De ce fait, en cas d'incidences négatives dues à l'apprentissage, le dommage ne pourrait pas être réparable en invoquant ce régime de responsabilité[49].

De plus, leur architecture en réseaux de neurones ne permet pas d'appréhender la façon dont le résultat a été obtenu. Par conséquent, il paraît difficile d'incriminer un tel dommage comme résultant d'un fait personnel, dès lors que le gardien de l'objet technique n'a aucun pouvoir de direction lors de la survenance du dommage, et que ce dommage résulte d'une décision autonome. En revanche, on pourrait ici imaginer l'élaboration d'« une responsabilité objective du fait de l'autonomie décisionnelle de l'objet technique »[50]. Dans le cadre de ce régime de responsabilité, le fait générateur consisterait alors en une présomption de défaut de programmation engendrant des conséquences néfastes non maîtrisées[51] dont l'indemnisation reviendrait au concepteur. À charge pour ce dernier de prouver que le préjudice subi par la victime est consécutif à un aléa technologique, au même titre que l'aléa thérapeutique. Ainsi, il paraît indispensable de prévoir dans les contrats des dispositions relatives au suivi et à la maintenance des algorithmes.

Le 20 octobre 2020, le Parlement européen a adopté une résolution contenant des recommandations à la Commission pour l'adoption d'un règlement européen sur le régime de responsabilité civile applicable aux opérateurs des systèmes d'intelligence artificielle. Les grandes lignes suggèrent la responsabilité des opérateurs de systèmes d'intelligence artificielle sur la base d'une responsabilité stricte fondée sur la notion de faute, sauf si réglementation locale plus stricte. Les contrats, limitant ou contournant la responsabilité telle qu'arrêtée dans la future réglementation, seraient considérés comme nuls, et toute tentative d'exempter sa responsabilité en opposant que le dommage a été causé par un process ou un instrument dirigé par une intelligence artificielle serait inopérante.

## CONCLUSION

Les acteurs de la santé numérique doivent faire face à des défis permanents, et il est clair que, face aux incertitudes résultant du décalage entre la réglementation et le développement continu des nouvelles technologies, toutes les questions de

(47) C. civ., art. 515-14.
(48) CNIL, *Compte-rendu – Événement de lancement du cycle de débats publics sur les enjeux éthiques des algorithmes*, 2017.
(49) Groupes de travail réunis à l'initiative du Gouvernement, *Rapport de synthèse France intelligence artificielle*, 2017, p. 22 (www.economie.gouv.fr/files/files/PDF/2017/Rapport_synthese_France_IA_pdf).
(50) L. Godefroy, *Les algorithmes : quel statut juridique pour quelles responsabilités ? : Comm. com. électr*. nov. 2017, n° 11.
(51) *Ibid*.

conformité ne peuvent pas être résolues par les acteurs à ce jour. Il faut ici faire le deuil d'une conformité que l'on essaierait de figer. Il s'agit bien au contraire de rechercher une adaptation continue, de par un mode de fonctionnement collaboratif, impliquant nécessairement plusieurs équipes et chefs de projet au sein d'une même structure.

Afin de faire face aux défis identifiés dans cet article, nos réflexions nous ont conduits à proposer une méthodologie en cinq étapes. Il s'agit, en pratique, d'évaluer les risques légaux en amont, puis au fur et à mesure, de la vie d'un projet selon l'approche *Privacy by design* induite par la réglementation relative aux données personnelles. Il s'agit donc d'une approche *Project by design*, pour laquelle nous proposons une méthodologie en cinq étapes, constituant une trajectoire de conformité qui peut, selon nous, être appliquée à différents projets du monde de la santé, et notamment dans le cadre de la conduite d'essais cliniques.

Les données étant un vecteur clé de la digitalisation du monde de la santé, la première étape de notre analyse consiste à évaluer les risques en matière de **données** : il s'agit, entre autres, de se demander quelles sont les données traitées et de les catégoriser (données scientifiques, données financières, données de santé, *etc.*), de se demander qui est propriétaire de ces données, si elles sont libres de droit, où elles sont stockées, et quelles mesures de sécurité peuvent leur être appliquées afin d'assurer une sécurisation suffisante. Les données sont-elles, par exemple, anonymisées, ce qui serait de nature à réduire tout risque lié à la protection des données personnelles ? L'entreprise a-t-elle suffisamment anticipé un partage élargi des données dans un plan, élaboré et intégré, dès le lancement des études cliniques ?

Comme nous avons tenté de le démontrer tout au long de cet article, les **technologies de l'information** doivent désormais être associées à tous les projets numériques, et sont donc intimement liées à toutes les interrogations en matière de données qui peuvent émerger. Les départements IT sont aujourd'hui essentiels pour assurer la sécurité, la conformité, et l'intégrité des données. Cette deuxième étape de notre méthodologie consiste donc à se focaliser sur les technologies au cœur du projet numérique, et à s'assurer que toutes les spécificités technologiques soient revues et validées par le département IT de l'entreprise. C'est l'approche *IT by design* que nous avons détaillée plus haut dans ce chapitre, et qui est un véritable « changement de paradigme » : l'IT ne peut plus être considérée comme un simple département au service de l'entreprise, qui en serait la cliente. Les données et la technologie sont désormais « au cœur du réacteur » des industries et sont la source de l'activité économique.

Ensuite, face à l'augmentation exponentielle du nombre d'algorithmes dans les projets engagés, et les incertitudes juridiques qu'ils peuvent susciter, les acteurs doivent nécessairement s'interroger sur les différents types d'**algorithmes** qui peuvent être utilisés dans le cadre de leurs projets numériques. Ceci implique de s'interroger sur le statut de ces algorithmes (par ex., qui les a développés ?), sur l'émergence de la *blockchain* et sur les garanties de transparence qui peuvent être mises en œuvre.

Après s'être interrogés successivement sur les données, les technologies de l'information et les algorithmes, les acteurs de la santé numérique peuvent se tourner

vers les **résultats**. Il s'agit ici notamment de s'interroger sur des problématiques de secret des affaires et de propriété intellectuelle qui pourraient être attachées aux résultats de l'essai clinique. Il s'agit par exemple de mener des réflexions autour des logiciels innovants, qui doivent être protégés par la propriété intellectuelle.

Tout ce travail amène finalement les acteurs de la santé numérique à s'interroger sur les **finalités** de leurs projets, eu égard aux problématiques de protection des données, d'intégrité, de confidentialité et de transparence. Il s'agit d'anticiper de futures réutilisations des données, et surtout de se mettre en position de pouvoir adapter les contrats conclus et mener une réflexion autour des différentes bases légales offertes par la réglementation en matière de données personnelles, notamment en s'interrogeant sur la nécessité de se rapprocher des personnes concernées afin de collecter de nouveau leur consentement pour des finalités différentes de celles proposées initialement. Cette solution est très peu praticable dans la réalité, d'où l'importance de réfléchir en amont au plan de partage des données afin de maximiser leur potentiel, tout en assurant une juste conformité.

| MÉTHODOLOGIE EN 5 ÉTAPES : L'APPROCHE *PROJECT BY DESIGN* | | | | |
|---|---|---|---|---|
| **Données** | **IT** | **Algorithmes** | **Résultats** | **Finalités** |

Cette approche permet, selon nous, de prendre le recul nécessaire face aux défis que nous identifions aujourd'hui et avec lesquels nous allons devoir travailler à moyen terme. Elle implique nécessairement une coordination, un travail d'équipe, à travers les différents départements de l'entreprise. À l'image de cet article, qui est le résultat d'une méthodologie collaborative associant des angles de vue variés au sein du monde de la santé numérique.

CHAPITRE 4

# L'IMPACT DU NUMÉRIQUE DANS L'ÉVALUATION DE LA MISE SUR LE MARCHÉ

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Ruby ARCHEN
Caroline KAK
Lindsay PECQUERIAUX

La célérité de la mise sur le marché des médicaments et produits de santé est devenue un enjeu primordial, dans un contexte de mondialisation, d'informatisation, notamment par le remplacement de l'humain par des robots et algorithmes. Afin de réduire les coûts et pouvoir obtenir des bénéfices rapidement, il faudrait permettre l'accélération du processus de recherche et développement (R&D) qui dure en moyenne dix à quinze ans avant qu'un produit de santé ne puisse être autorisé sur le marché. Dès lors, l'objectif des industriels est de réduire ce temps considérable, et de ne plus en perdre lors des démarches de demande d'autorisation de mise sur le marché. Il est devenu important de contrôler les flux de dépenses, car les produits de santé sont fragilisés par une réglementation lourde, qui se complexifie et oblige régulièrement les laboratoires à rappeler leurs produits. Par conséquent, une nouvelle « course contre la montre » se dessine, celle d'être le premier sur le marché à obtenir un rapport bénéfice/risque satisfaisant permettant de répondre à un nouveau champ thérapeutique nécessaire pour le traitement des patients. Il faut certes améliorer la qualité de vie, ce qui est avec la pandémie de Covid-19 devenu une préoccupation centrale au cours de l'année 2020. Cependant, il faut également pouvoir présenter un médicament[1], un dispositif médical[2], un produit innovant

(1) PE et Cons. UE, dir. 2004/27/CE, 31 mars 2004, modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain.
(2) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, les règlements (CE) n° 178/2002 et n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

qui permettrait de remplir toutes les conditions indispensables pour une mise sur le marché. Cette proportionnalité entre rapidité, numérique et sécurité est encore difficile à trouver et cela apparaît de façon évidente dans les réglementations actuelles des autorités compétentes pour la mise sur le marché.

Cette analyse s'inscrit dans le contexte de la pandémie du coronavirus, qui pousse à obtenir des solutions curatives dans l'urgence. Cette crise sanitaire démontre une faculté d'adaptation de la part des autorités, notamment sur le plan de l'autorisation de la mise sur le marché qui fut délivrée dans un temps record, avec moins de documentations. Ces éléments permettent de poser la question du *Market Access* qui se doit d'être efficace et rapide. Le numérique s'impose alors afin de simplifier les procédures d'obtention d'autorisation de mise sur le marché. Un nombre croissant d'autorités de santé s'y intéressent, notamment les hautes instances de l'Union européenne qui enjoignent les États membres d'utiliser la technologie au service des procédures et des demandes d'autorisation de mise sur le marché.

Le digital étant devenu la clé de croissance au sein de la société, les industriels s'attachent à l'inclure dans tout le cycle de vie des produits de santé. Cependant, il faut s'adapter à ces nouveaux produits qui intègrent la technologie aux médicaments et aux dispositifs médicaux afin d'améliorer leur efficacité, notamment grâce au suivi des patients. Ce système se vérifie en outre par l'explosion des outils de e-santé qui se sont encore renforcés à l'occasion de la distanciation sociale imposée lors de cette pandémie de Covid-19. Désormais, il est d'usage de réaliser des consultations *via* des applications et de voir son médecin par visioconférence, ce qui restait très minoritaire il y a deux ans. Désormais le numérique est entré dans la pratique médicale et constituera le mode privilégié dans les dix ans à venir.

À l'échelle mondiale, ce contexte fait apparaître des disparités d'adaptation entre les États. Certains comme les États-Unis accordent une importance particulière à l'encadrement des nouveaux produits de santé connectés. Cela peut être dû à leur historique où certains médicaments ont été utilisés à d'autres fins que celles octroyées dans le cadre de leur autorisation de mise sur le marché, ce qui a conduit à certaines réglementations de la FDA, comme le *Federal Food Drug and Cosmetics Act* de 1938 qui s'accompagne du *Code of federal regulation*, mais également le *Food and drug administration Act* en 2007[3]. D'autres pays se montrent plus réticents à moderniser leur législation, peut-être craignent-ils de manquer à leur devoir de sécurité en ne prévoyant pas toutes les éventualités.

De par sa diversité, le numérique inclut tout type de technologie tel que les robots, les intelligences artificielles, les algorithmes élevés, autonomes autoapprenants, les *blockchains*, la e-santé, les plateformes en ligne, les applications, les logiciels, les produits de santé connectés…

Le numérique est certes présent dans les produits, mais il est aussi devenu un outil qui s'intègre parfaitement à l'évaluation d'autorisation de mise sur le marché. L'Union européenne a compris cet enjeu et pousse à son usage afin que les délais

(3) Sénat, Rapport d'information sur « la réglementation américaine du médicament » (www.senat.fr/rap/r96-196/r96-19682.html, consulté le 8 avr. 2021).

de traitement des dossiers de demande soient raccourcis, néanmoins l'usage d'algorithmes demeure restreint notamment au niveau national.

Afin de mieux comprendre les problématiques qui résultent du numérique, il est nécessaire de revenir sur l'implémentation du numérique dans la réglementation qui entoure la mise sur le marché des produits de santé, que ce soit sur le versant des procédures ou leurs définitions (Section 1). Ensuite, il faut se pencher sur l'aspect du *Market Access* qui permet de négocier le prix et le remboursement de ces produits de santé tout en intégrant les nouveaux outils numériques (Section 2). Enfin, il serait pertinent d'évoquer ce que l'apport du numérique dans le cadre de l'autorisation de mise sur le marché a permis de révolutionner, mais ce qu'il a également soulevé comme risques (Section 3).

SECTION 1

# LE NUMÉRIQUE ET LA MISE SUR LE MARCHÉ DES PRODUITS DE SANTÉ PILOTÉE PAR DES ACTEURS COMPÉTENTS

La réglementation des procédures de mise sur le marché des produits de santé s'est adaptée au format numérique et permet ainsi l'accessibilité aux produits de santé au sein du marché européen (§ 1). Par ailleurs, les laboratoires innovent en matière de produits de santé, ce qui impacte directement la qualification et la classification des produits de santé et donc leurs conditions de mise sur le marché (§ 2).

## § 1. – L'évolution des procédures d'évaluation de mise sur le marché permettant l'accessibilité des produits de santé au patient

La réglementation de la procédure de mise sur le marché est à la fois européenne et nationale (I) ; afin d'accélérer les délais à ces deux échelles, les États ont dû s'emparer des outils numériques, permettant ainsi de réduire le temps de communication (II).

### I. – L'état actuel de la réglementation des autorités dans l'évaluation de la mise sur le marché (des produits de santé)

Tout produit de santé doit faire l'objet d'une autorisation avant d'atteindre le marché. C'est le cas pour une variété de produits de santé telle que les biocides[4],

(4) PE et Cons. UE, règl. (UE) n° 528/2012, 22 mai 2012, concernant la mise à disposition sur le marché et l'utilisation des produits biocides (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ :L :2012 :167 :0001 :0123 :fr :PDF).

les dispositifs médicaux[5], les produits cosmétiques[6] ainsi que les médicaments[7]. En dépit de l'intérêt qu'il pourrait y avoir à étudier les conditions d'accès au marché de cette multiplicité de produits soumis à des réglementations spécifiques, cette étude ciblera davantage les médicaments et les dispositifs médicaux. Pour cette dernière catégorie, l'autorisation à obtenir est le marquage CE, qui définit la conformité de ce produit de santé aux exigences de sécurité prévues dans le nouveau règlement, tandis que dans le cadre du médicament, le terme approprié est l'autorisation de mise sur le marché (AMM). En pratique, cette dernière peut être délivrée selon trois procédures à portée européenne, dites centralisée, décentralisée et de reconnaissance mutuelle et une dernière propre à chaque État.

Une prise de conscience quant à l'enjeu d'une harmonisation des procédures d'évaluation des produits de santé sur le territoire européen a engendré la création de certaines entités. C'est notamment le cas de l'Agence européenne du médicament (EMA) créée en 1995, qui permet de mutualiser les procédures à l'échelle européenne. Son siège, anciennement à Londres, a été déplacé à Amsterdam le 1er mars 2019 suite au Brexit[8]. En effet, sa localisation en dehors de l'Union européenne entraînait des problèmes quant au suivi des dossiers engendrant ainsi des retards de mise sur le marché des médicaments. L'EMA possède en son sein le Comité des médicaments à usage humain (CHMP) composé d'experts de chaque État membre. Ce comité a pour mission de tenir un rôle d'intermédiaire entre les systèmes européens et nationaux et contribue au développement de la réglementation en aidant les industriels à préparer des demandes d'autorisations de mise sur le marché pour la catégorie des médicaments à usage humain.

Cette harmonisation est prégnante au niveau des procédures d'évaluation de mise sur le marché, et c'est ce que l'on observe à travers les procédures **centralisée, décentralisée et de reconnaissance mutuelle**. La première, prévue par l'article 3, § 2 du règlement n° 726/2004, permet d'octroyer une autorisation de mise sur le marché à un titulaire, qui pourra ensuite commercialiser le médicament sur l'ensemble du territoire de l'Union européenne. Cela offre un gain de temps et d'argent considérable, car la procédure demeure unique, mais aussi et surtout de sécurité avec une procédure unique au sein des États membres. Certaines catégories de produits, visées par la réglementation, tels que les médicaments de biotechnologies[9], ou orphelins[10], ont l'obligation de se soumettre à cette procédure. La **procédure décentralisée** réglementée par la directive 2001/83/CE modifiée par la directive 2004/27/CE permet d'obtenir une autorisation simultanée et commune délivrée par plusieurs États membres. Ces deux procédures doivent s'étendre sur

(5) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, les règlements (CE) n° 178/2002 et n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

(6) PE et Cons. UE, règl. (CE) n° 1223/2009, 30 nov. 2009, relatif aux produits cosmétiques (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32009R1223&qid=1614121975600).

(7) PE et Cons. UE, dir. 2004/27/CE, 31 mars 2004, modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain.

(8) PE et Cons. UE, règl. (UE) n° 2018/1718, 14 nov. 2018 portant modification du règl. (CE) n° 726/2004 en ce qui concerne la fixation du siège de l'EMA (https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX :32018R1718&from=EN).

(9) Un médicament biologique est une substance produite à partir d'une cellule ou d'un organisme vivant ou dérivé de ceux-ci. C'est notamment le cas des vaccins ou des médicaments dérivés du sang.

(10) Un médicament est dit « orphelin » lorsqu'il est destiné au traitement de maladies rares.

une durée maximale de 210 jours ; cependant, la procédure la plus rapide est la pénultième, qui a un délai minimal de 80 jours tandis que la décentralisée doit au moins s'étendre sur 90 jours. Enfin, la procédure de **reconnaissance mutuelle** peut être rapprochée de la procédure décentralisée du fait qu'elle est réglementée par la même directive. Elle consiste à faire reconnaître un produit à un État membre de référence, puis à l'étendre aux autres États où le produit pourrait être commercialisé. Cette procédure se déroule par le dépôt d'un dossier dans un pays, puis il est demandé aux autres de reconnaître le médicament en se basant sur le rapport rendu par le premier État. Cependant, cette procédure dure 90 jours, mais elle est suivie de 30 jours de clôture pour la délivrance de l'AMM nationale (qui est le temps durant lequel il est possible pour un laboratoire de demander la reconnaissance de cette autorisation dans un ou plusieurs États membres de l'Union européenne)[11].

Il est essentiel de comprendre l'importance d'obtenir cette autorisation administrative. En effet, après le long processus de recherche et développement qui précède cette demande, ce produit ne sera commercialisé qu'après avoir obtenu l'autorisation de mise sur le marché auprès de l'autorité compétente, ce qui engendre plusieurs problématiques. Tout d'abord, le demandeur de l'AMM devra conditionner son profit à l'obtention de l'autorisation. Or, cette procédure peut s'avérer longue, car l'étude du dossier est un processus relativement complexe. Le demandeur se devra donc de patienter pour pouvoir valoriser son produit. D'autre part, les patients doivent également attendre cette autorisation pour accéder à un traitement qui pourrait les soigner, voire les sauver. On comprend ainsi l'enjeu crucial lié à l'optimisation de cette procédure de mise sur le marché.

L'existence de mesures européennes n'est en rien incompatible avec la présence de procédures nationales. En effet, la France s'est également dotée de procédures pour évaluer les critères sans lesquels les médicaments n'accéderaient pas au marché. Dès lors, c'est sous la responsabilité de la Commission de la transparence de la Haute Autorité de santé que trois critères[12] seront appréciés dans un délai maximal de 90 jours. Tout d'abord, il s'agit d'analyser la qualité du produit, en appréciant la documentation pharmaceutique fournie par le demandeur de l'AMM, puis d'étudier le profil sécuritaire du produit en contrôlant les résultats des essais précliniques. Enfin, il suffira de se concentrer sur l'efficacité du produit en se basant sur les résultats des essais cliniques. Une fois cette vérification réalisée, la Commission transmet un avis à l'ANSM qui est l'autorité seule responsable de délivrer ou non une AMM. Cette dernière sera valable pour une durée de cinq ans à l'exception des demandes d'AMM conditionnelles qui ont une durée inférieure.

Il est important de garder à l'esprit le bouleversement récent du régime des autorisations temporaires d'utilisation (ATU) à travers le projet de loi de finances de la sécurité sociale (PLFSS) de 2021[13]. En effet, alors que ce système apparaissait de manière innovante en 1994 en France, cette loi réalise une refonte totale de ce

(11) EMA, *Le système européen de réglementation des médicaments Une approche cohérente de la réglementation des médicaments dans l'Union européenne*, EMA/716925/2016, 2016.

(12) LEEM, *Comment se décide une autorisation de mise sur le marché (AMM) ?*, 24 nov. 2017 (www.leem.org/comment-se-decide-une-autorisation-de-mise-sur-le-marche-amm).

(13) LFSS pour 2021 n° 2020-1576, 14 déc. 2020 (www.legifrance.gouv.fr/jorf/id/JORFTEXT000042665307).

système. Tout d'abord, l'article 78 de la loi de finances de la sécurité sociale annonce la fin des ATU au profit d'un double système dérogatoire combinant, d'une part, le nouveau système d'autorisation d'accès précoce (AAP) et, d'autre part, les autorisations d'accès compassionnel (AAC). Les AAP englobent désormais les ATU de cohorte et d'extension d'indication, la prise en charge post-ATU ainsi que l'accès direct post-AMM, tandis que les AAC se substituent aux ATU nominatives et aux recommandations temporaires d'utilisations (RTU). Ces modifications auront de nombreuses conséquences sur les procédures de mise sur le marché, dont l'une que l'on peut dès lors appréhender. Il s'agit du transfert de l'ANSM vers la HAS pour accorder les AAP ainsi que l'ajout d'un nouveau critère, celui du « médicament présumé innovant ». Ce mécanisme, bien qu'incitatif et facilitateur pour les industriels se retrouvant face à un système unifié, il va tout de même falloir attendre les décrets d'application pour réellement identifier le potentiel de cette réforme vis-à-vis de l'inclusion d'outils numériques. Ce mécanisme, bien que français, traduit effectivement la volonté d'élargir le champ des *off-label use*[14] qui se développe au niveau européen du fait de la multiplication des systèmes dérogatoires. Malgré le fait que la législation européenne régule les autorisations de commercialisation des produits de santé, elle ne régule pas directement les procédures d'accès précoces et se base sur les différentes législations des États membres dans l'UE. La présence de la directive 2010/84/UE témoigne bel et bien de la reconnaissance de leur existence, sans pour autant fixer de règles pour les contrôler.

Par ailleurs, les différentes procédures de mise sur le marché permettent de faciliter l'évaluation des produits, car elles accélèrent le processus tout en harmonisant les différentes réglementations présentes sur le territoire européen. En revanche, la crise liée à la Covid-19 a mis en exergue les lacunes de ce système qui atteint ses limites. En effet, les délais originellement prévus pour garantir la sécurité des patients ont été réduits pour faire face à l'urgence de la situation. Ce fut notamment le cas de l'Agence européenne du médicament qui a innové en incorporant le mécanisme du *rolling view*[15] dans l'évaluation des vaccins anti-Covid. Ce mécanisme vise à évaluer les vaccins sur une plus courte période pour qu'ils accèdent au marché, puis de poursuivre l'examen en continu en recueillant les données « au fil de l'eau ». Un *rolling view*, examen continu, est l'un des outils réglementaires que l'EMA utilise pour accélérer l'évaluation d'un médicament ou d'un vaccin prometteur lors d'une urgence de santé publique. Normalement, toutes les données sur l'efficacité, la sécurité et la qualité d'un médicament et tous les documents requis doivent être soumis au début de l'évaluation dans une demande officielle d'autorisation de mise sur le marché. Dans le cas d'un examen continu, le Comité des médicaments à usage humain (CHMP) de l'EMA examine les données au fur et à mesure qu'elles deviennent disponibles à partir des études en cours, avant qu'une demande formelle ne soit soumise. Une fois que le CHMP décide que des données suffisantes sont disponibles, la demande formelle doit être soumise par la société.

(14) EMA, *Utilisation d'un médicament hors AMM* (www.ema.europa.eu/en/glossary/label-use).
(15) ANSM, *Évaluation des demandes de mise sur le marché* (www.ansm.sante.fr/Dossiers/COVID-19-Vaccins/Evaluation-des-demandes-de-mise-sur-le-marche/(offset)/2).

En examinant les données au fur et à mesure qu'elles sont disponibles, le CHMP peut se prononcer plus tôt sur l'autorisation ou non du médicament ou du vaccin. Cette procédure a été utilisée pour le vaccin AstraZeneca dans la phase Covid-19.

En outre, certains traitements comme le Bamlanivimab du laboratoire Eli Lilly ont été autorisés par l'analogue américain de l'ANSM[16] de manière rapide en acceptant que les risques soient plus élevés et que les bénéfices continuent d'être évalués. Cet anticorps monoclonal a fait l'objet de recherches et d'essais cliniques réalisés sur une période d'un an pour faire face à l'urgence et répondre rapidement aux besoins liés à la crise sanitaire.

Ces mécanismes, visant à réduire la durée de l'évaluation des produits de santé en période d'urgence pourraient être retranscrits pour les périodes plus ordinaires, et ainsi permettre une commercialisation plus rapide. Une solution serait d'inclure le numérique en santé. En effet, les opportunités du numérique dans ce secteur sont multiples et permettraient une amélioration de la qualité et de l'efficience des soins conférés aux patients.

Les procédures d'autorisation de mise sur le marché se sont numérisées en termes de communication et de réception des demandes par l'évolution des outils numériques. Cette numérisation apporte une accélération dans le traitement des demandes par les autorités, ce qui simplifie le système d'autorisation de mise sur le marché. Mais le développement de l'IA autonome permettra d'aller plus loin et plus vite dans l'évaluation des rapports bénéfices/risques des produits.

## II. – L'effet des outils numériques sur l'évolution des réglementations des autorités régissant l'accès sur le marché

La progression constante de l'usage numérique et de l'intelligence artificielle a impacté le fonctionnement des autorités de santé comme l'EMA, la HAS et l'ANSM. Mais il reste à intégrer au sein des différentes réglementations l'encadrement de l'accès au marché par l'intelligence artificielle.

Les pays se sont réunis pour créer des outils numériques communs au niveau mondial, ce qui a pu permettre une accélération des procédures d'autorisation de mise sur le marché entre les différents pays.

L'*International Conference Harmonisation* (ICH) a été créée lors d'une réunion à Bruxelles en avril 1990 pour réunir les industriels et autorités de santé d'Europe, du Japon et des États-Unis. L'objectif était de faire converger les procédures d'enregistrement des médicaments pour ces trois territoires, tout en harmonisant les critères d'évaluation des médicaments (efficacité, sécurité, qualité) et ainsi réduire les coûts de développement. Depuis que les autorités sont passées au numérique, les dossiers d'AMM sont dématérialisés, et doivent ainsi être déposés au format *common technical document* (CTD)[17]. Ce format est international, ce qui permet une rapidité

(16) FDA, *Mise à jour sur le coronavirus (Covid-19) : la FDA autorise l'anticorps monoclonal pour le traitement du COVID-19*, 9 nov. 2020 (www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-authorizes-monoclonal-antibody-treatment-covid-19).

(17) A. Feroyard, *Constitution d'un dossier d'autorisation de mise sur le marché d'un médicament à usage humain et ses différentes procédures d'enregistrement en Europe*, thèse pour le diplôme d'état de docteur en pharmacie, 16 juin 2014 (https://dumas.ccsd.cnrs.fr/dumas-01064013/document).

d'échange des dossiers entre les différentes autorités, notamment lorsqu'elles s'appuient sur une autre autorisation pour déterminer si elles vont autoriser le produit de santé sur leur territoire. C'est cet organisme, nommé Conférence internationale d'harmonisation (ICH), qui va initier le format électronique de dossiers d'AMM, CTD qui vient remplacer le format *Notice To Applicant* (NTA) lors d'une conférence à San Diego en juillet 2000. Son utilisation était basée, à partir de juillet 2001, sur le volontariat pour ensuite devenir obligatoire au sein de l'Union européenne dès 2003. L'EMA a notamment diffusé des *guidelines* afin de référencer les dossiers devant être communiqués sous ce format, comme la *Guideline pour les produits d'herbes médicinales* en 2016[18].

Au niveau de l'Union européenne, l'accent a été mis sur la nécessité pour les autorités d'user des outils du numérique afin d'accélérer les procédures. Cela s'illustre dans la pratique par des échanges par mail et *via* des plateformes permettant de communiquer et réunir les pièces nécessaires à la constitution d'un dossier d'AMM. La communication entre le fabricant et l'EMA étant facilitée, les délais de réception des pièces ont pu être réduits. Les échanges réalisés anciennement par voie postale se font maintenant directement par ordinateur. Ce qui permet d'induire une réduction des délais au sein des échanges d'informations entre les autorités et les fabricants. En effet, le fabricant va soumettre son dossier à la *Common European Submission Platform* (CESP) au format e-CTD (*Electronic Common Technical Document*), un courriel automatique va lui confirmer le téléchargement de celui-ci. Ensuite, dans un délai de quatorze jours, le fabricant va recevoir un accusé de réception, suivi d'une confirmation de recevabilité, ou d'une notification de non-recevabilité de la demande[19].

Cependant, même si le numérique permet une rapidité d'action, il comporte également ses limites. La cybercriminalité pourrait avoir un impact significatif si des données venaient à être divulguées.

Au niveau national, la loi pour une République numérique du 8 octobre 2016[20] a imposé aux autorités nationales d'utiliser le digital afin d'améliorer l'échange des données entre les différentes institutions. Ceci permet d'avoir accès aux données nécessaires pour l'étude d'un dossier d'AMM de façon instantanée. L'ANSM s'aligne sur les recommandations de l'EMA et applique le format e-CTD pour les dossiers d'AMM déposés auprès de la CESP depuis 2018 pour les procédures de reconnaissances mutuelles et décentralisées, et depuis 2019 au niveau national. Le format électronique Nees (*Non-eCTD electronic Submission*), anciennement utilisé, était certes numérique mais non harmonisé, c'est pour cela qu'il n'a été accepté que jusqu'au 31 décembre 2018. L'ANSM enjoint depuis 2018 les industriels à éviter l'usage du format papier[21]. Tout cela converge vers l'objectif

(18) EMA, *Ligne directrice sur l'utilisation du format CTD dans la préparation d'une demande d'enregistrement pour les médicaments traditionnels à base de plantes*, 27 juin 2016 (www.ema.europa.eu/en/guideline-use-ctd-format-preparation-registration-application-traditional-herbal-medicinal-products).

(19) ANSM, *Optimisation des délais d'instruction d'une demande d'AMM soumise en procédure nationale. Optimisation des délais d'instruction d'une demande d'AMM…* (www.ansm.sante.fr.).

(20) L. n° 2016-1321, 7 oct. 2016 pour une République numérique.

(21) ANSM, *Soumission électronique CESP (Common European Submission Platform)* (www.ansm.sante.fr/Activites/Autorisations-de-Mise-sur-le-Marche-AMM/Soumission-des-demandes/(offset)/9.).

de centralisation de l'information de l'historique des demandes, mais également de rapidité des procédures. Dès lors, il sera plus simple et rapide de modifier un dossier d'AMM numérique que de rechercher un dossier papier dans des archives. Cela sous-tend une sécurisation absolue des procédures numériques et des outils techniques et technologiques permettant le fonctionnement de l'usage numérique.

Cette évolution du numérique dans les procédures administratives d'évaluation du médicament est en phase avec celle constatée au sein des industries de santé qui évoluent dans cet univers de l'évaluation numérique du médicament précédent sa mise sur le marché, répondant à la nécessité d'aller de plus en plus vite, avec le plus de sécurité possible dans la mise sur le marché de produits complexes.

## § 2. – L'influence du numérique sur l'évolution des critères de qualification

Le recours au numérique peut être conçu tout à la fois comme un outil permettant d'évaluer les produits de santé, mais aussi comme un outil s'incorporant aux produits de santé, et modifiant leur qualification, la rendant plus complexe. Ces nouveaux produits de santé mixtes, ou complexes, font apparaître un enjeu d'harmonisation et d'adaptation des définitions au niveau européen (I). Ces éléments numériques doivent ainsi pouvoir être enregistrés dans une classe afin de pouvoir être évalués par les autorités en tant que tels (II).

### I. – Les règles de classification et de qualification inhérentes aux produits de santé

Afin de répondre à ce nouvel enjeu des produits de santé incluant du numérique, l'Union européenne a dû harmoniser les terminologies et procédés d'évaluation au sein des pays membres. Cependant, malgré un travail hors du commun de la part des instances de l'UE, il reste difficile d'imposer des prises de décision aux instances nationales, car les pays demeurent souverains dans leur politique de santé. En dépit de l'enchaînement de directives et de règlements, les différences d'évaluations sont encore bien présentes.

Ainsi, afin de faciliter l'évaluation des produits de santé, leurs définitions ont été harmonisées au niveau européen par le biais de directives et règlements (V. *supra*, § 1, I). Le contenu des critères de qualification et classification pourrait également être totalement harmonisé, toutefois certains pays se montrent plus exigeants que d'autres et, dans le cadre de leur pouvoir souverain en matière de santé (TFUE, art. 168), élèvent le niveau de protection, dans le respect des principes du TFUE, à savoir la proportionnalité et l'objectif des mesures spécifiques nationales. C'est notamment le cas de la France. La réglementation française est fondée sur un niveau de sécurité des produits très élevé ce qui peut avoir pour conséquence de considérer un produit comme un médicament alors qu'en Allemagne ce même produit peut être classé comme un complément alimentaire. L'arrêt *Juvamine* rendu

par la chambre criminelle de la Cour de cassation le 21 janvier 2014[22] illustre ce cas. En l'espèce, la cour a considéré que la vitamine C1000 commercialisée par les laboratoires Juva Santé était un médicament. Ce produit, considéré comme un médicament en France, est vendu comme un complément alimentaire dans d'autres pays membres de l'Union européenne. Si un État membre souhaite élever ses critères de qualification, il pourrait démontrer qu'il s'agit d'une question d'ordre public, et donc agir en s'appuyant sur le principe de souveraineté. Cela impacte directement l'évaluation ainsi que l'obtention de l'autorisation de mise sur le marché d'un produit qui circule sur un autre territoire. Certes, les procédures de reconnaissances mutuelles et décentralisées limitent ces possibilités, mais encore faut-il qu'elles soient utilisées et que le pays concerné n'ait pas de réelle opposition à présenter pour complexifier la mise sur le marché. En effet, chaque État membre est tenu *a minima* d'appliquer les réglementations en vigueur ; ceci dit, il est libre de les durcir et par conséquent, de différer largement son traitement des AMM d'un pays voisin tenu par la même réglementation. Le pays pourra décider de retirer un produit ou le faire retirer par le laboratoire en mettant par exemple en avant les effets indésirables constatés.

La phase Covid-19 illustre parfaitement ces divergences au sein de l'Union européenne. En effet, les États membres se sont engagés en ordre dispersé au sujet de la mise sur le marché des vaccins. Les États ont adopté des positions très différentes concernant les décisions de retrait ou au contraire de maintien des vaccins.

La Commission de l'Union européenne a adopté en ce sens le règlement n° 2019/9 sur les médicaments vétérinaires[23], la directive 2004/24/CE relative aux médicaments à usage humain[24], et le règlement n° 2017/745 concernant les dispositifs médicaux. Ces règlements viennent harmoniser la réglementation des produits de santé et s'appliquent directement sans transposition. La directive, au contraire, doit s'intégrer dans les législations nationales avant de pouvoir être appliquée.

Dans le secteur des dispositifs médicaux (DM), le règlement n° 2017/745[25] est un outil de l'Union européenne qui vise à harmoniser la réglementation des États membres et permet une obtention plus rapide du marquage CE et notamment pour les DM présentant un caractère numérique et contenant un logiciel, ou des logiciels eux-mêmes qualifiés comme DM. Le règlement n° 2017/745 crée une nouvelle classification qui permet d'élargir le champ d'application des dispositifs médicaux. Par exemple, avec l'intégration des accessoires des dispositifs médicaux comme étant des DM à part entière. Il s'adapte également au numérique avec les logiciels proposés en solution médicale dans les DM de classe I à IIa et les dispositifs médicaux d'intelligence artificielle dans les classes IIb à III. L'objectif est

(22) Cass. crim., 21 janv. 2014, n° 13-80.112, inédit.
(23) PE et Cons. UE, règl. (UE) n° 2019/6, 11 déc. 2018, relatif aux médicaments vétérinaires et abrogeant la directive 2001/82/CE (Texte présentant de l'intérêt pour l'EEE).
(24) PE et Cons. UE, dir. 2004/27/CE, 31 mars 2004, modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain.
(25) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, les règlements (CE) n° 178/2002 et n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (Texte présentant de l'intérêt pour l'EEE).

de s'adapter et d'inclure davantage d'appareils dans cette classification, ce qui permet un contrôle de la sécurité par l'organisation de la matériovigilance.

Toutefois, il n'existe pas à ce jour une adaptation permettant de couvrir toutes les nouvelles formes de produits de santé incluant du numérique et notamment des IA autonomes présentant des risques spécifiques pour les utilisateurs et patients. De ce fait, les critères de qualification ne sont pas parfaitement adaptés et engendrent des difficultés. Notamment la question pourra se poser de savoir comment qualifier les médicaments connectés, c'est-à-dire disposant d'un DM, en nanotechnologie. S'agit-il d'un médicament complexe, ou d'un produit composé, dont chaque partie est soumise à un encadrement spécifique et notamment au règlement européen n° 2017/745 pour les dispositifs médicaux appliqué à partir du 26 mai 2021 ? Cela vaut également pour le règlement européen n° 2017/746[(26)] qui n'entrera en vigueur que le 26 mai 2022. La Commission a en effet laissé des délais supplémentaires aux fabricants de dispositifs médicaux afin de s'aligner au règlement en fonction de la classe de risque du DM fabriqué. D'autres autorités étrangères de santé ont intégré de nouveaux critères, comme la *Food and Drug Administration* (FDA)[(27)]. Cette dernière a réalisé un guide pour en faire un standard permettant de prendre en compte l'inclusion de l'intelligence artificielle dans les produits de santé.

En France, les autorités ont pris conscience de la nécessité d'adapter les critères d'évaluation. C'est pourquoi la Haute Autorité de santé (HAS) envisage d'établir des critères comprenant les intelligences artificielles et le numérique. Ainsi, elle rassemble tous les dispositifs médicaux dotés d'intelligence artificielle sous le terme « d'innovation ». Elle organise également les demandes d'évaluation des dispositifs médicaux connectés en précisant les spécificités de son évaluation aux industriels. Cela engendre un gain de temps en qualifiant au mieux le logiciel intégré à leur dispositif médical[(28)]. Dès lors, il y a un réel engagement des autorités au niveau international pour encadrer ces nouvelles technologies.

Pour la détermination de logiciels en tant que DM ou DMDIV, l'ANSM[(29)] se positionne de manière identique à l'Union européenne en anticipant l'entrée en vigueur effective des règlements n$^{os}$ 2017/745 et 2017/746. L'ANSM met en évidence les critères nationaux qui apportent un éclairage quant à des critères auparavant absents. Par exemple, pour être caractérisé comme un DM ou un DMDIV, le logiciel doit répondre à trois critères cumulatifs. Le premier concerne la destination du produit, c'est-à-dire s'il est destiné à des fins médicales, en d'autres termes si l'appareil permet « un diagnostic, une aide au diagnostic, un traitement ou une aide au traitement, donner un résultat au bénéfice d'un seul patient et effectuer

(26) PE et Cons. UE, règl. (UE) n° 2017/746, 5 avr. 2017, relatif aux dispositifs médicaux de diagnostic *in vitro* et abrogeant la dir. 98/79/CE et la décision 2010/227/UE de la Comm. (Texte présentant de l'intérêt pour l'EEE).

(27) FDA, *Guide permettant d'ébaucher un standard pour la prise en compte d'intelligences artificielles dites « évolutives »* (www.fda.gov/media/122535/download ?utm_campaign=2019-04-02%20Discussion%20Paper%20on%20Regulating%20Artificial%20Intelligence&utm_medium=email&utm_source=Eloqua).

(28) HAS, *Un nouvel outil pour l'évaluation des dispositifs médicaux embarquant de l'intelligence artificielle*, 14 oct. 2020 (www.has-sante.fr/jcms/p_3212876/fr/un-nouvel-outil-pour-l-evaluation-des-dispositifs-medicaux-embarquant-de-l-intelligence-artificielle).

(29) ANSM, *Mise sur le marché des dispositifs médicaux et dispositifs médicaux de diagnostic in vitro (DM/DMIA/DMDIV)*, 2020 (www.ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Logiciels-et-applications-mobiles-en-sante/(offset)/3.

une action sur les données entrantes »[30]. Le deuxième se doit de donner un résultat spécifique au bien-être d'un seul patient. Et dans un troisième temps, le logiciel se doit d'effectuer une action sur les données entrantes en fournissant une information médicale nouvelle.

Ces prises de position des autorités démontrent que les autorités nationales des États au niveau européen, et l'ensemble des agences au niveau international, s'engagent activement dans la qualification des logiciels et objets connectés à visée médicale, et notamment des médicaments embarquant un logiciel. Elle adapte aussi en interne leurs méthodes d'évaluation afin de répondre aux exigences de mise sur le marché anticipée de produits indispensables au traitement du patient.

## II. – La connexité entre l'évolution des critères de qualification et l'émergence des produits innovants

Le numérique pose des difficultés qui se sont révélées plus importantes avec la pandémie de Covid-19, car il contraint les autorités à revoir les conditions de mise sur le marché et à adapter les réglementations en vigueur, dans cette phase d'urgence sanitaire. En d'autres termes, il s'agit de repousser les frontières des critères de classification actuels, afin de garantir une sécurité suffisante aux usagers, tout en encadrant la mise sur le marché plus rapide de produits complexes. C'est notamment le cas pour les objets de e-santé comme la téléconsultation, les logiciels comprenant de nombreux outils, des *packages* permettant notamment la prise en charge de la carte Vitale du patient ou l'accès aux rédactions d'ordonnance. Si le *package* contient ces éléments, seul le logiciel du *pack* concerné par ces accès sera plus sécurisé, dès lors il sera considéré et évalué comme un DM d'une classe importante.

Malgré l'inclusion des logiciels comme DM et DMDIV, il existe encore des exclusions qui sont affirmées, par des autorités d'États membres comme l'ANSM, qui rappelle que certains logiciels ne peuvent pas être pris en considération dans la qualification du numérique (V. *supra*, Section 1, § 2, I). C'est dans une jurisprudence européenne rendue le 7 décembre 2017[31], que la Cour de justice de l'Union européenne exclut les logiciels qui sont « destinés à l'observance, ceux ayant pour seule destination la communication de données sans alerter le médecin, ceux destinés à être utilisés dans le cas d'entraînements sportifs, également ceux où le résultat aboutirait à un diagnostic pour un groupe de patients, et enfin les logiciels n'ayant que des fonctions administratives ».

La question suscitée par cette jurisprudence est de savoir si les logiciels antérieurement exclus rentreront dans le champ d'application du règlement européen n° 2017/745[32] concernant les DM. Cela correspondrait notamment aux logiciels médicaux qui pourraient entrer dans les classes de risque I à III avec une tendance

(30) ANSM, *Mise sur le marché des dispositifs médicaux et dispositifs médicaux de diagnostic in vitro (DM/DMIA/DMDIV)*, 2020, (www.ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Logiciels-et-applications-mobiles-en-sante/(offset)/3).

(31) *Ibid.*

(32) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, les règlements (CE) n° 178/2002 et n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (Texte présentant de l'intérêt pour l'EEE).

au durcissement des règles. À titre d'exemple, les logiciels d'aide à la décision auparavant classés I basculent vers des classes plus sévères de IIa à III[33]. Il est fort probable que la Cour de justice de l'Union européenne sera forcée de se prononcer à nouveau sur le sujet.

Par ailleurs, une enquête de l'Union européenne réalisée en novembre 2018[34], sur la défaillance des processus d'évaluation de plusieurs dispositifs médicaux, met en exergue les failles d'évaluation des dispositifs médicaux par les organismes certificateurs. En effet, les prothèses, pompes, implants auraient dû être plus contrôlés notamment au niveau de leurs matériaux avant d'être mis sur le marché en tant que dispositifs médicaux par les autorités de santé des États membres. Seulement, les algorithmes prédictifs n'ont pas été étudiés dans le cadre de cette enquête alors qu'ils sont utilisés plus fréquemment afin d'analyser, diagnostiquer et prédire. L'enquête *Implant Files* menée par un consortium international de journalistes en 2018 dénonce des défaillances graves dans la surveillance des dispositifs médicaux au niveau international et démontre qu'il est impossible de constater l'évaluation de l'ensemble des produits numériques, tout simplement, car les pays ne les prennent pas tous en considération. Même si les algorithmes n'ont pas été étudiés dans le cadre de cette enquête, il ne faut pas pour autant oublier l'importance de leur rôle qui implique nécessairement que ceux-ci doivent être certifiés au même titre que n'importe quel dispositif. Par ailleurs, l'implication de l'intelligence artificielle dans ces nouveaux produits de santé questionne, notamment sur les responsabilités afférentes à son utilisation.

Au niveau communautaire, la Commission européenne a adopté un plan d'action détaillant les moyens que devrait déployer l'Europe pour encourager la « transformation des soins et de la santé dans le marché unique numérique »[35]. En matière d'intelligence artificielle, elle a adopté un livre blanc le 19 février 2020, suivie par le Parlement européen qui a adopté trois résolutions le 20 octobre 2020 contenant des recommandations à la Commission, dont la résolution sur un régime de responsabilité civile pour l'intelligence artificielle[36]. De son côté, la HAS a consacré son analyse prospective de 2019 à la (r)évolution numérique et a formulé vingt-neuf propositions pour que le numérique soit un outil au service de tous les acteurs[37].

Au niveau national, l'ANSM essaye de poser les bases d'une nouvelle adaptation tout en prenant en compte les logiciels. Conjointement, la HAS a organisé une consultation publique en janvier 2020[38], afin de mettre en place une nouvelle grille

(33) G. Promé, *Logiciels médicaux et nouveau règlement sur les DM*, 24 avr. 2017 (www.qualitiso.com/applis-logiciel-reglement-dispositifs-medicaux).

(34) Santé personnalisée et société, *Comprendre les algorithmes : alors que les algorithmes prédictifs prennent de plus en plus de place dans nos vies et la gestion de notre santé, comment être sûr qu'ils sont à la fois efficaces et sûrs ?*, 21 déc. 2018 (https://santeperso.ch/Pour-comprendre/Algorithmes-l-epineuse-question-de-la-validation).

(35) Comm. UE, Livre blanc, *Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance :* Doc. COM [2020], 0065 final, 2020 (https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf).

(36) PE, *Un régime de responsabilité civile pour l'intelligence artificielle*, 2020/2014(INL), 2020 (www.europarl.europa.eu/doceo/document/TA-9-2020-0276_FR.htm).

(37) HAS, Rapport d'analyse prospective 2019, *Numérique : quelle (R)évolution ? 2019* (www.has-sante.fr/upload/docs/appli-cation/pdf/2019-07/rapport_analyse_prospective_20191.pd).

(38) HAS, *Consultation publique sur le projet de grille d'analyse destinée à être utilisée par la CNEDiMTS pour contribuer à son évaluation de DM embarquant des systèmes décisionnels s'appuyant sur des procédés d'apprentissage automatique (« Intelligence artificielle »)*, 20 nov. 2019, (www.has-sante.fr/upload/docs/application/pdf/2019-11/notice_consultation_algorithmes.pdf).

de critères pour évaluer les dispositifs médicaux. L'objectif étant de recueillir des éléments d'évaluations pour déterminer de façon précise de nouveaux critères de classification. En ce sens, le guichet national de l'innovation et des usages en e-santé (gnius.esante.gouv.fr) est destiné à faire gagner du temps aux entrepreneurs et à accélérer la mise sur le marché de leurs innovations. Le guichet national de l'innovation et des usages en e-santé (G_NIUS) a une approche par type de réglementation, d'acteurs et de sources de financements.

Suite à cette consultation publique, Guillaume Hochard, expert en intelligence artificielle à la HAS, a publié une grille d'évaluation permettant d'inclure le numérique dans la qualification des dispositifs médicaux[39], tout en incorporant les algorithmes auto-apprenants[40].

La HAS essaye d'élargir les critères d'évaluation, mais devrait prendre en considération l'ensemble des éléments du règlement « DM ». Elle s'engage par différents avis, recommandations, qui constituent une *soft law* utile en la matière[41]. Ainsi elle a publié une classification fonctionnelle, selon leur finalité d'usage, des solutions numériques utilisées dans le cadre de soins médicaux ou paramédicaux validée par le Collège le 4 février 2021[42].

Par ailleurs, une autre difficulté liée au numérique a été mise en évidence par la Commission nationale d'évaluation des dispositifs et des technologies de santé (CNEDiMTS)[43], qui évalue les objets connectés, car ceux-ci, même s'ils sont surveillés, ne sont pas systématiquement classés en tant que dispositifs médicaux, et peuvent ne pas entrer dans la catégorie des produits de santé. Ces objets connectés peuvent prendre la forme de logiciels, applications au service du patient, mais également du médecin. Ceux-ci disposent de données médicales sensibles et nécessitent une évaluation qui n'est pas forcément décrite sur le site des autorités, alors qu'ils sont l'essence même du suivi du patient dans son traitement. Les objets connectés sont conseillés par les médecins à leurs patients sans restriction, ils s'inscrivent dès lors dans le processus thérapeutique. Pourtant, la réglementation qui les entoure manque de précision. De même, cette question de fiabilité et de sécurité de ces outils met en évidence l'utilité de nouvelles modalités d'évaluation. La sécurité est un enjeu important que les industriels ont bien compris en renforçant leurs départements *compliance*, afin de respecter le règlement général sur la protection des données (RGPD)[44]. Cette notion de données personnelles apparaît de plus en plus importante dans le cadre des produits

(39) G. Morisse et G. Hochard, *Vers un standard d'évaluation des dispositifs médicaux embarquant de l'IA*, Quantmetry, 8 janv. 2020 (www.quantmetry.com/blog/standard-devaluation-dispositifs-medicaux-embarquant-lia/).

(40) HAS, *Évaluer les dispositifs médicaux avec intelligence artificielle*, 20 nov. 2019 (www.has-sante.fr/jcms/p_3119829/fr/evaluer-les-dispositifs-medicaux-avec-intelligence-artificielle).

(41) HAS, *Référentiel de bonnes pratiques sur les applications et les objets connectés en santé* (*mobile Health ou mHealth*), 2016.

(42) HAS, *Classification fonctionnelle, selon leur finalité d'usage, des solutions numériques utilisées dans le cadre de soins médicaux ou paramédicaux*, févr. 2021.

(43) HAS, *Projet de grille d'analyse pour l'évaluation de dispositifs médicaux avec intelligence artificielle*, 15 janv. 2020 (www.has-sante.fr/jcms/p_3118247/fr/projet-de-grille-d-analyse-pour-l-evaluation-de-dispositifs-medicaux-avec-intelligence-artificielle).

(44) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 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 (règl. général sur la protection des données).

de santé ; elles sont utilisées à chaque étape et la technologie ne peut s'en passer. Dès lors, la CNIL s'est saisie du problème et veille à ce que le RGPD soit respecté, elle n'hésite pas à sanctionner les erreurs des entreprises. Chaque patient doit pouvoir exercer ses droits sur ses données, même si celles-ci sont utiles, elles doivent rester intègres et être supprimées dès qu'elles ne sont plus utilisées. Ainsi dans la phase Covid-19 les risques sont accentués. En prévision de la levée des restrictions de déplacements en France en mai 2021, le ministère des Solidarités et de la Santé déploie l'outil « TousAntiCovid-Carnet » qui permet de stocker les résultats de tests et de vaccination. Si la CNIL valide à ce stade le dispositif, elle met en garde contre une utilisation qui viserait à réguler l'accès à certains lieux, ce qui serait une atteinte aux libertés fondamentales.

Mais ces mesures concernant la protection des données ne sont pas absolument efficaces dans le cadre de l'utilisation d'une intelligence artificielle autonome, et posent clairement la question des conditions d'encadrement de son usage dans les produits de santé et les pratiques de soins. Avec la proposition de nouvelle réglementation sur l'IA (nouvelle fenêtre) présentée le 21 avril 2021, la Commission européenne réaffirme l'importance stratégique de l'IA pour l'Europe et la nécessité d'encadrer son usage dans les différents secteurs d'application.

Cela est d'autant plus vrai qu'il faut garantir l'évaluation d'outils qui se sont généralisés dans les pratiques, notamment avec l'apparition de la pandémie. Les consultations à distance se sont multipliées, forçant les professionnels et les patients à utiliser des applications, logiciels qui ne sont pas forcément pris en compte. Pourtant, toutes ces technologies collectent des données sensibles notamment sur le plan médical, ce qui impose de garantir une certaine fiabilité et sécurité. Tout cela converge vers l'idée d'une révision de l'évaluation des outils, peut-être en ne s'arrêtant plus aux qualifications existantes au niveau national.

La DGCCRF fait le même constat sur les critères de qualification, qui sont parfois restrictifs, c'est-à-dire que de nombreux médecins dirigent leurs patients vers des objets connectés, alors que ceux-ci ne sont pas évalués. Au lieu d'être qualifiés de dispositifs médicaux et d'être soumis aux mêmes conditions de marquages CE qu'un produit de santé, ces outils numériques évoluent dans la sphère des produits frontières, relevant des produits soumis à la réglementation sur la consommation et les communications numériques. Pourtant, les patients utilisent ces objets en complément de leur traitement sans pour autant être garantis de la fiabilité du produit qu'ils ont acheté. C'est une problématique qui pourrait potentiellement prendre fin avec le règlement, car ces appareils sont souvent utilisés en accessoire et pourraient dès lors être requalifiés en dispositifs médicaux.

Enfin, l'Assemblée nationale a tenu à répondre aux nouvelles questions sur les dispositifs médicaux technologiques et plus particulièrement au sujet des nanotechnologies[45], que ce soit pour les médicaments ou les dispositifs médicaux. Elle précise que les évaluations du bénéfice/risque doivent prendre en compte la dimension nanométrique afin de limiter au maximum les risques liés à l'utilisation de ces

(45) Lexis, AN, Ministère du travail, de l'Emploi et de la Santé, *Question écrite à l'Assemblée nationale sur les dispositifs médicaux technologiques*, *JO* 13 juill. 2010.

produits. Par conséquent, la technologie n'est pas seulement un outil à part entière, elle peut se comprendre comme un élément permettant d'aboutir à une innovation et des conditions spécifiques concernant le *Market Access*.

SECTION 2

# PILOTAGE DE LA MISE EN ŒUVRE DU *MARKET ACCESS* ET DES STRATÉGIES NUMÉRIQUES

La fixation du prix peut être décidée en fonction du remboursement, seulement c'est un élément qui ne peut être négligé, car les laboratoires et fabricants de DM connectés ont une phase de R&D particulièrement onéreuse et risquée, ce qui nécessite d'optimiser les conditions d'accès au marché (§ 1). Mais les outils numériques présentent une complexité qui impose la réalisation de nouveaux modes de contrôles (§ 2).

## § 1. – L'approche des acteurs nationaux au service de la fixation des prix et du taux de remboursement sur les produits de santé

Au-delà des phases d'essais cliniques et de qualification des produits de santé, des modalités de négociation des prix par les organismes en vue de leur remboursement rentrent en compte (I). Ces modalités sont adaptables en fonction de l'innovation promise par le médicament ou le dispositif médical connecté (II).

### I. – Les modalités d'études de fixation des prix par les organismes nationaux

La dépense de médicaments et de dispositifs médicaux en France a atteint 48,8 milliards d'euros en 2019[46]. Avec un système de santé particulier, tous les patients bénéficient d'un accès équitable aux produits de santé dont ils ont besoin, du fait qu'ils financent peu ou pas leur consommation. Cela est possible grâce à l'assurance maladie qui finance la grande majorité du prix d'un médicament et à l'assurance complémentaire individuelle qui vient compléter ce régime. Mais cette politique, bien que profitable au patient, invite les laboratoires à adopter des stratégies bien définies au niveau du *Market Access*. En effet, il ne suffit pas d'avoir une AMM en France pour que l'entreprise puisse commercialiser le produit, tout en ayant une rentabilité acceptable et conforme aux objectifs qui ont été fixés. De même, l'AMM ne signifie pas que le médicament sera pris en charge pour le patient.

(46) DREES, *Les dépenses de santé en 2019 – Résultats des comptes de la santé*, 15 sept. 2020, mis à jour le 4 févr. 2021 (https://drees.solidarites-sante.gouv.fr/publications-documents-de-reference/panoramas-de-la-drees/les-depenses-de-sante-en-2019-resultats).

En l'espèce, il s'agit de se pencher sur les médicaments remboursables, qui bénéficient des prix administrés, contrairement aux médicaments en vente libre qui ont par conséquent un prix libre. Légalement, c'est l'article L. 162-16-4 du Code de la sécurité sociale qui prévoit que le prix de vente au public d'un médicament est fixé par convention entre l'entreprise exploitant le médicament et le Comité économique des produits de santé (CEPS).

Le CEPS est un organisme placé sous l'autorité des ministres chargés de la santé, de la sécurité sociale et de l'économie. Afin de fixer les prix des médicaments et des dispositifs médicaux, le CEPS met en œuvre des orientations pour les prix, le suivi des dépenses et la régulation financière du marché. Le comité négocie ainsi avec l'entreprise le prix du produit de santé selon des critères fixés par la loi. L'un des principaux critères est l'amélioration du service médical rendu (ASMR), il s'agit de l'évaluation de la valeur thérapeutique d'un produit. À titre indicatif, les autres valeurs correspondent à la population touchée par la pathologie, mais également au prix des médicaments déjà disponibles sur le marché. Le premier critère est communiqué au CEPS par la HAS.

En effet, le laboratoire qui souhaite avoir une prise en charge du produit de santé qu'il va mettre sur le marché doit, premièrement, en faire la demande auprès de la Commission de la transparence (CT), elle-même membre de la HAS. C'est à elle que revient la charge d'évaluer la place du médicament dans la stratégie thérapeutique à travers deux indicateurs : le service médical rendu (SMR) et l'amélioration du service médical rendu (ASMR)[47].

En premier lieu, le SMR mesure la valeur thérapeutique en prenant en compte plusieurs critères tels que l'efficacité et les effets indésirables, de même que la place de la stratégie thérapeutique et l'intérêt pour la santé publique du produit. Le SMR varie de majeur, modéré à insuffisant. Si le SMR est insuffisant, alors la Commission estime qu'une prise en charge n'est pas prioritaire[48].

Le second indicateur qu'est l'ASMR mesure quant à lui le progrès thérapeutique apporté par le produit de santé sur chaque indication thérapeutique définie. Cette valeur varie de majeure à inexistante. Ces évaluations changent avec le temps en fonction des données disponibles à un moment donné, elles sont donc par définition temporaires et sont susceptibles d'évoluer. La Commission de la transparence de la HAS émet un avis public à l'attention du ministère de la Santé. C'est ce même avis qui est transmis au CEPS et à l'Union des caisses nationales d'assurance maladie (UNCAM)[49]. C'est donc une étude médico-économique qui permet la fixation du prix du médicament en France. Dans d'autres pays comme l'Allemagne, les prix sont libres pour une durée d'un an[50].

(47) HAS, *Commission de la Transparence*, 18 déc. 2020 (www.has-sante.fr/jcms/c_412210/fr/commission-de-la-transparence).
(48) HAS, *Le service médical rendu (SMR) et l'amélioration du service médical rendu (ASMR)*, 16 avr. 2013 (www.has-sante.fr/jcms/r_1506267/fr/le-service-medical-rendu-smr-et-l-amelioration-du-service-medical-rendu-asmr).
(49) Ministère des Solidarités et de la Santé, *La fixation des prix et du taux de remboursement*, mis à jour le 10 nov. 2016 (https://solidarites-sante.gouv.fr/soins-et-maladies/medicaments/le-circuit-du-medicament/article/la-fixation-des-prix-et-du-taux-de-remboursement).
(50) Institut Montaigne, *Le prix des médicaments : des spécificités nationales dans un marché global* (www.institutmontaigne.org/blog/le-prix-des-medicaments-des-specificites-nationales-dans-un-marche-global).

Cette procédure est possible entre autres, grâce à l'utilisation des bases de données gouvernementales mises à la disposition des entités telles que la HAS, l'UNCAM ou l'ANSM. Le système national des données de santé (SNDS) regroupe les principales bases de données médico-administratives (BDMA) et pourrait même servir pour la surveillance de certaines anomalies. Des bases de données qui référencent les médicaments existent déjà, et récemment, la base EUDAMED pour les dispositifs médicaux a été mise en place grâce au règlement de la Commission européenne n° 2017/745 et sera *a priori* complètement fonctionnelle en mai 2022[51].

Avec une étude du marché, ainsi qu'un investissement pour des médicaments innovants, la rentabilité du produit pourrait être perfectionnée grâce à l'utilisation du numérique dans l'accélération du processus de mise sur le marché.

Concernant les dispositifs médicaux, le système français prévoit deux modalités de prise en charge du DM dans le cadre du remboursement : celle passant par l'inscription sur la liste des produits et prestations remboursables (LPPR) et celle passant par les prestations d'hospitalisation « Intra-GHS ». La gestion du remboursement est effectuée par la Haute Autorité de santé (HAS) et à l'ANSM pour une partie. Au sein de la HAS, l'évaluation est réalisée par la CNEDiMTS et le CEPS. Deux types d'inscription sont actuellement en vigueur pour la LPPR : en nom de marque ou en description générique. L'inscription en ligne générique consiste à identifier un groupe de DM avec des indications de prise en charge identiques, un même service rendu et répondant à des spécifications techniques communes minimales à respecter. Dans cette modalité d'inscription, il s'agit d'une auto-inscription sur une description générique identifiée sur la LPPR avec déclaration obligatoire auprès de l'ANSM. La CNEDiMTS réévalue les descriptions génériques au minimum tous les cinq ans. La procédure par nom de marque ou nom commercial porte sur les DM présentant un caractère innovant ou lorsqu'il est nécessaire de mettre en œuvre un suivi particulier du DM. Le fabricant doit transmettre un dossier médico technique (DMT) à la CNEDiMTS et un dossier médico économique (DME) au CEPS. Dans le cadre d'une première demande d'inscription, le DMT doit faire la démonstration du service attendu (SA), l'amélioration du SA (ASA) et la population cible. Le SA est évalué sur la base d'informations cliniques fournies par le demandeur. L'ASA est évaluée sur la base de données comparatives issues d'essais cliniques (utilisation d'un comparateur). Il existe deux niveaux de SA (suffisant et insuffisant) et quatre niveaux d'ASA (majeure, importante, modérée, mineure et absence d'amélioration).

Dans la fixation du prix de remboursement, le CEPS se base sur les informations fournies dans le DME mais également sur le niveau de SA et d'ASA. La détermination des tarifs de remboursement tient compte principalement du SA, de l'ASA, des tarifs et prix des produits ou prestations comparables inscrits sur la LPPR, des volumes de ventes et des conditions prévisibles d'utilisation.

Le *Guide pour le dossier de demande d'inscription, de modification des conditions d'inscription et de renouvellement d'inscription d'un produit ou d'une prestation sous nom de marque sur la liste prévue à l'article L. 165-1 du Code de la sécurité sociale*

(51) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, les règlements (CE) n° 178/2002 et n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

est présenté par la HAS[52], ainsi qu'un ensemble de guides permettant au fabricant de déposer un dossier innovant et d'obtenir un remboursement du produit[53].

Concernant les dispositifs connectés, présentant les particularités de mise en lien du patient et du professionnel de santé, la HAS a construit des avis spécifiques visant à aider les fabricants dans leurs démarches de demande de remboursement[54]. Elle s'investit fortement dans la présentation des conditions de qualification de ces produits complexes et des enjeux de remboursement et communique notamment au travers d'outils de formation des fabricants[55].

## II. – La stratégie de l'étude de marché laissant une marge de manœuvre aux acteurs de l'industrie de santé pour une meilleure rentabilité du produit

Afin d'optimiser le délai de la mise à disposition des produits de santé innovants pour les patients, le législateur a apporté des ajustements à la procédure classique en collaboration avec les autorités de santé, tant pour les médicaments que pour les DM, et ce d'autant plus dans la phase d'urgence liée à la pandémie, qui crée une situation d'exception.

La procédure de fixation des prix est une procédure longue notamment à cause du délai d'évaluation par la CT et prend en moyenne 131 jours. Cela complexifie la mise sur le marché des médicaments, y compris celle relative aux médicaments innovants. Cependant, le législateur est venu réduire le délai de traitement de cette procédure concernant la catégorie des médicaments « innovants ».

Les médicaments innovants, autrement dit qui « sauvent ou changent la vie des patients atteints d'une maladie grave ou évolutive dans un contexte de besoin médical mal couvert (pas d'alternatives ou alternatives peu efficaces) »[56] peuvent également donner lieu à un dépôt de demande d'avis d'efficience. Le dépôt de dossier de l'avis d'efficience, depuis le 2 avril 2019, se fait uniquement en ligne de façon numérique et les envois papiers ne sont plus acceptés. Une plateforme dédiée (Sésame) sur le site de la HAS a été développée pour cela, avec la possibilité de créer un compte d'accès en amont. Cette manière de déposer le dossier de façon numérique simplifie son traitement. Cette demande se fait auprès de la Commission d'évaluation économique et de santé publique (CEESP) de la HAS qui vient articuler son expertise autour de l'expertise de la Commission de la transparence et de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé[57]. Des études cliniques avec des données réelles d'utilisations

(52) HAS, *Parcours du dispositif médical en France*, nov. 2017, version 2020.
(53) HAS, *Choix méthodologiques pour l'évaluation économique à la HAS*, juill. 2020. – HAS, *Forfait innovation. Guide pour le dépôt de dossier de demande de prise en charge dérogatoire pour un produit innovant (CSS, art. L. 165-1)*, 8 avr. 2015, mise à jour oct. 2020.
(54) *Guide sur les spécificités d'évaluation clinique d'un DMC en vue de son accès au remboursement. Rapport méthodologique d'évaluation clinique d'un dispositif médical connecté.*
(55) HAS, *DM & Intelligence artificielle : quelles spécificités pour l'évaluation ?*, webinaire, 15 oct. 2020.
(56) HAS, *Médicaments : une évaluation rigoureuse et scientifique par la HAS*, 12 juin 2019 (www.has-sante.fr/jcms/pprd_2974176/en/medicaments-une-evaluation-rigoureuse-et-scientifique-par-la-has).
(57) HAS, *Dépôt d'un dossier en vue d'un avis économique de la commission d'évaluation économique et de santé publique (CEESP)*, 27 janv. 2020 (www.has-sante.fr/jcms/c_1627022/fr/depot-d-un-dossier-en-vue-d-un-avis-economique).

sont demandées dans le cadre de cette procédure et permettent une prise en charge plus rapide qu'avec la demande standard. À cet effet, certaines sociétés de recherche contractuelle, comme l'association française des CRO (*Contract Research Organization*), peuvent intervenir. Ce sont des sociétés de services qui gèrent pour leurs clients industriels des études cliniques réalisées auprès des professionnels de la santé. Leur rôle est de les accompagner au moment de la négociation des prix et notamment dans les demandes auprès des commissions de la HAS et du CEPS. Elles aident les industriels de la santé à fournir des études et des datas assez rapidement. De plus, ces sociétés anticipent les demandes de la HAS et collectent des données pour le compte de leurs clients notamment en matière d'épidémiologie, et ceci très tôt dans la phase de recherche clinique. Ces sociétés, tournées vers le numérique et vers la rapidité d'évolution en matière de santé, appuient les industriels et leurs demandes en leur permettant d'anticiper les demandes des autorités et d'optimiser les temps de traitement en fournissant rapidement des *datas*.

Le législateur a par ailleurs, dans l'article L. 165-1-1 du Code de sécurité sociale, mis en place le forfait innovation. Il s'agit d'un dispositif de prise en charge dérogatoire et temporaire qui permet de faciliter l'accès précoce aux produits de santé autres que les médicaments présentant une technologie innovante en phase précoce de développement clinique. Des données tirées d'études cliniques doivent établir que l'utilisation du produit de santé apporte un bénéfice important pour la santé ou en réduit les dépenses. Ce forfait est accordé par les ministres chargés de la santé et de la sécurité sociale après l'avis de la HAS qui évalue l'éligibilité de la demande. Cette dernière doit également être faite depuis le 30 juin 2020 de manière électronique sur la plateforme Sésame[58].

Auparavant, pour un accès plus rapide à des produits de santé innovants, les autorisations temporaires d'utilisation (ATU) nominatives, de cohorte, pour des extensions d'indication, ou de prise en charge anticipée post-AMM, pouvaient être délivrées par l'ANSM quand le médicament ne disposait pas d'AMM et pour le traitement de maladie sans alternatives thérapeutiques. Il s'agit là d'un dispositif créé en 1994[59] et qui est pionnier en Europe. Il a permis à des patients atteints de maladies graves d'avoir un accès à des médicaments qui n'avaient pas d'AMM. Afin de faciliter et d'accélérer le traitement des demandes mais aussi de garantir un accès « transparent, rapide et équitable à l'innovation thérapeutique », l'ANSM n'accepte plus que les demandes d'ATU nominative faites grâce à la plateforme e-Saturne.

Les recommandations temporaires d'utilisation (RTU) sont quant à elles octroyées pour l'utilisation des médicaments hors du cadre de leur AMM. Les RTU sont établis à l'initiative de l'ANSM, tandis que les ATU sont demandées par le laboratoire.

Cependant, depuis la loi de financement de la sécurité sociale pour l'année 2021[60], les mécanismes relatifs aux ATU/RTU seront remplacés par ceux de l'accès précoce et l'accès compassionnel aux médicaments afin de gagner en clarté

(58) HAS, *Forfait innovation*, 5 févr. 2020 (www.has-sante.fr/jcms/c_2035788/fr/forfait-innovation).
(59) Sénat, Y. Daudigny, C.Deroche et V.Guillotin, *Médicaments innovants : consolider le modèle français d'accès précoce*, 13 juin 2018 (www.senat.fr/rap/r17-569/r17-5693.html).
(60) L. n° 2020-1576, 14 déc. 2020, de financement de la sécurité sociale pour 2021.

et en lisibilité. L'accès précoce visera les médicaments soupçonnés d'être innovants pour lesquels le laboratoire a le projet de déposer une demande d'AMM rapidement. Ce mécanisme sera donc une anticipation de l'AMM. De plus, l'autorisation ne sera plus donnée par l'ANSM comme pour les ATU, mais par la HAS après avis conforme de l'ANSM. L'accès compassionnel, quant à lui, concernera les médicaments ayant une AMM, mais dont l'utilisation est justifiée pour une indication thérapeutique qui sort du cadre de l'AMM, donc pour un besoin thérapeutique différent[61].

De surcroît, le décret n° 2019-855 du 20 août 2019 relatif à la prise en charge précoce de certains produits de santé[62] a introduit un nouveau dispositif de prise en charge précoce et temporaire d'indications pour les médicaments n'ayant pas fait l'objet d'ATU. Ce dispositif permet un accès rapide au patient dès l'obtention de l'AMM avant même la prise en charge collective. Les octrois se font suite à une demande de prise en charge précoce (PECP) faite par le laboratoire sur la plateforme Sésame.

Dans un autre sens, dans le but d'optimiser la rentabilité d'un produit, les industriels de la santé peuvent s'appuyer sur une bonne stratégie marketing. En effet, bien que les médicaments et les DM soient des produits de santé, ils restent des produits destinés à la consommation. Pour cela, il faut prendre en compte tous les aspects qui en découlent. Le médicament est un produit qui s'adresse au patient, mais qui est pris en charge par la collectivité. Par conséquent, la stratégie marketing doit être ciblée en fonction du parcours de soin. Il appartient aux industriels d'adapter leur stratégie en l'espèce et donc de l'orienter plus localement, c'est-à-dire à l'attention des professionnels de la santé, des établissements de santé, mais aussi en fonction des demandes des différentes agences régionales de santé (ARS).

Concernant les dispositifs médicaux connectés[63], qui auront été au préalable évalués dans le cadre de la réglementation sur les essais cliniques, ils devront être évalués par la CNEDiMTS. Leur évaluation doit s'adapter au rythme des évolutions technologiques. La confiance et la sécurité dans l'utilisation sont au cœur de l'évaluation de ces dispositifs médicaux connectés. Un des enjeux pour la CNEDiMTS est de concilier les exigences en matière d'évaluation avec le rythme d'évolution des DMC, pour favoriser l'introduction rapide dans le système de soins de ceux susceptibles d'apporter un bénéfice. Le rapport du groupe de travail commandité par le CCNE avec le concours de la CERNA3, publié le 19 novembre 2018, relève que « pourtant, les travaux de certification et de normalisation sur l'intelligence artificielle et la robotisation en santé, en dépit de leur intérêt, en restent, en l'état, à un stade très parcellaire »[64]. Les DM qui sont évalués sont en nombre

(61) A.-C. Maillols-Perroy, *LFSS pour 2021 : les points clés dans le domaine des médicaments*, 22 déc. 2020 (www.editions-legislatives.fr/actualite/lfss-pour-2021-les-points-cles-dans-le-domaine-des-medicaments).

(62) D. n° 2019-855, 20 août 2019, relatif à la prise en charge précoce de certains produits de santé : *JO* 22 août 2020.

(63) HAS, *Guide sur les spécificités d'évaluation clinique d'un dispositif médical connecté (DMC)*, janv. 2019. Ce guide a pour objectif d'aider les entreprises qui fabriquent ou assurent l'exploitation du DMC à intégrer dans leur stratégie de développement les études cliniques qui permettront de déterminer son intérêt, en vue de son remboursement par la solidarité nationale.

(64) CCNE, Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene, *Numérique et santé. Quels enjeux éthiques pour quelles régulations ?*, Paris, 2018 (www.ccne-ethique.fr/sites/default/files/publications/rapport_numerique_et_sante_).

infime par rapport à la multitude des objets utilisés dans la pratique courante de soins et de traitement ou prévention par le patient. La mission d'évaluation scientifique de la CNEDiMTS n'intervient que lorsque le marquage CE a été obtenu (CSS, art. R. 165-4). Son évaluation est complémentaire à celle du marquage CE : au-delà de la démonstration des performances et de la sécurité, elle s'attache à évaluer l'intérêt du DM pour le patient et pour la santé publique ainsi que sa place dans l'arsenal disponible en France. Outre le marquage CE, d'autres prérequis s'imposent. Tout fabricant qui dépose un dossier de demande de prise en charge d'un DMC doit s'être acquitté du respect des exigences législatives et réglementaires nationales et européennes, notamment en termes d'hébergement et de traitement des données[65]. La HAS insiste dans ses recommandations sur le caractère évolutif du produit et la nécessité au plan réglementaire de s'adapter en permanence, sur le caractère interopérable des produits entre eux et donc sur les risques concernant la sécurisation des données, enfin sur les risques concernant la construction et l'évolution des algorithmes avec les conséquences juridiques qui en découlent.

Il en résulte une nécessité claire d'entrer dans une phase d'accompagnement dynamique et agile des autorités dans ce contexte d'innovation, dans un encadrement juridique précis des risques, qui se met en place au niveau de l'Union européenne au travers du règlement sur l'IA.

Pour conclure, il est clair que cette utilisation du numérique, telle que la collecte de données, le traitement électronique des dossiers, et l'usage des bases de données médico-administratives permettent l'utilisation du numérique au service de l'évaluation de la mise sur le marché des produits de santé. Ces pratiques sont par ailleurs encouragées par l'Organisation de coopération et de développement économiques (OCDE)[66] qui aide les pays à construire des systèmes de santé solides en mesurant les résultats et l'utilisation des ressources du système de santé. Mais ces nouveaux modes de prise en charge du patient, au travers d'outils numériques connectés ou de produits de santé connectés, ouvrent aussi un nouveau marché concurrentiel complexe.

## § 2. – L'utilisation des outils numériques dans la réduction des coûts engendrés par l'évaluation des produits de santé

Les nouvelles technologies sont appréhendées par les acteurs de la santé afin d'accélérer les étapes menant à la mise sur le marché (I), seulement celles-ci nécessitent d'être contrôlées afin d'éviter tout risque de sécurité (II).

(65) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016, *Hébergement de données de santé à caractère personnel* (RGPD), C. santé publ., art. L. 1111-8.

(66) Ticpharma, Rapport, *L'OCDE encourage le recours au numérique pour renforcer le suivi du médicament*, 6 mars 2019, (www.ticpharma.com/story/881/locde-encourage-le-recours-au-numerique-pour-renforcer-le-suivi-du-medicament-(rapport).html).

## I. – Les outils numériques permettant l'accélération du processus de mise sur le marché

Le recours aux usages numériques en santé est une voie d'amélioration non seulement de l'état de santé du patient, des modalités de prise en charge rapide et efficace, mais aussi de réduction des coûts de la santé publique. Plusieurs exemples permettent d'illustrer l'intérêt de cet usage.

La technologie est devenue un outil important avec la mondialisation, et les industriels ont vite compris que pour trouver les informations rapidement, les bases de données constituaient un allié. Seulement, ce qui s'est fait promptement au niveau des entreprises a pris plus de temps au niveau des autorités. Notamment, car beaucoup de questions se sont posées en remettant le pouvoir de décision aux machines. C'est le cas du logiciel d'aide à la décision[(67)], qui permet d'accélérer la procédure d'évaluation des produits de santé. Il représente un avantage non négligeable, car son utilisation se rapproche étonnamment du fonctionnement de la pensée humaine. Il est conçu de façon à avoir un système de pensée, et en partant de ce postulat, il peut agir comme un être doté de raison. Cependant, ce logiciel ne peut pas apprendre au fur et à mesure, mais *a contrario*, il peut rassurer les autorités par sa fiabilité, car ses décisions pourront toujours être expliquées. D'ailleurs, l'Union européenne pousse ses États membres à utiliser les logiciels et algorithmes afin d'accélérer la mise sur le marché. Cela est encore trop peu fait, et il n'y a aucune trace de l'utilisation certaine de ces logiciels d'aide à la décision.

À côté de ces logiciels, il existe les algorithmes prédictifs. Ceux-ci permettent d'analyser des informations et de prédire un événement. Ce type d'algorithme pourrait éventuellement être utilisé dans le domaine de la pharmacovigilance et ainsi éviter des situations fâcheuses comme celle du Mediator[(68)]. Pour l'évaluation des produits de santé, cela permettrait un gain de temps considérable, car l'étude des documents ainsi que des résultats d'essais cliniques est un travail long qui ralentit l'obtention de la mise sur le marché. L'algorithme prédictif est utilisé pour la prévision de la défaillance d'implants dentaires en exploitant les analyses discriminantes qui ont permis d'identifier 72 % des implants échecs et 62 % d'implants intacts. Dès lors, il est considéré que cet algorithme peut être utilisé comme module d'aide à la décision clinique pour participer à l'approche personnalisée des patients ayant un implant dentaire[(69)].

Les autorités de contrôle demeurent réticentes à l'inclusion de l'IA, car ses mécanismes d'utilisation n'ont pas encore été suffisamment appréhendés.

(67) J. Le Gat, *Logiciels d'aide à la décision : quels enjeux pour l'accès au marché*, 2019 (https://dumas.ccsd.cnrs.fr/dumas-02455018/document).

(68) Le Mediator ou benfluorex est un médicament bénéficiant d'une autorisation de mise sur le marché pour les personnes en surcharge pondérale et atteint de diabète de type 2. Toutefois, ayant des propriétés anorexigènes, ce produit a été prescrit comme coupe-faim entraînant ainsi une augmentation de valvulopathie cardiaques, et dans certains cas la mort.

(69) IEEE Xplore, 41e conférence internationale annuelle de la société d'ingénierie en médecine et de biologie de l'IEEE (EMBC), Prévision de la défaillance des implants à l'aide de l'analyse discriminante, 2019 (https://ieeexplore.ieee.org/document/8856783).

Aux côtés de l'IA, et en complément de ces outils numériques intelligents, les *blockchains* sont des outils qui se sont répandus et leur utilisation est devenue massive dans de nombreux domaines. En les combinant à d'autres outils, ils permettent d'avoir un traitement des informations de manière sécurisée, notamment en donnant des accès limités aux données et en assurant leur traçabilité. La *blockchain* est un moyen permettant de donner la confiance aux autorités qui statue sur l'autorisation de mise sur le marché, notamment par la transparence qu'elle offre(70). Elle pourrait à long terme les encourager à utiliser davantage d'outils numériques qui évalueront les produits de santé.

Malgré ce manque de confiance assez général, on remarque que certaines autorités comme l'ANSM ont effectué des travaux, comme celui de 2019 afin d'étudier l'utilisation d'outils qui pourront faciliter le travail et améliorer la procédure d'autorisation de mise sur le marché, en la rendant notamment plus rapide, ce qui représente un gain de temps énorme. À titre d'illustration, e-Saturne, la plateforme précédemment citée, ouverte 24 heures sur 24 et 7 jours sur 7 permet de recevoir les demandes d'ATU numériquement, alors qu'auparavant, elles étaient réceptionnées par fax. Cela permet également une meilleure conservation des demandes et un meilleur traitement, car tout se situe au même endroit. Le logiciel QlikView permet de son côté d'améliorer la prise de décision en créant un réel échange entre les membres concernés. Il permet également le croisement des données, ce qui facilite la vue d'ensemble sur un dossier(71).

La solution pour répondre aux pratiques scientifiques et réglementaires nécessaires en santé serait l'intelligence augmentée qui laisse sa place à l'humain, car elle nécessite une collaboration humain-machine. C'est un concept proche de l'intelligence artificielle, mais qui pourrait être utilisé plus facilement en santé, car il intègre l'Homme. Cela s'illustre notamment par le projet européen « Désirée » qui aide à la prise en charge du traitement et du suivi des patientes atteintes de cancers du sein. Son raisonnement se fonde sur une ontologie, mais également sur une approche symbolique, sur un raisonnement d'expérience. Le système apprend des cas déjà résolus, ce qui lui permet de faire évoluer ses propositions sur la prise en charge thérapeutique des patientes(72).

Avec l'émergence de tous ces outils, des labels ont dû être mis en place, notamment ceux en e-santé que l'agence numérique de santé doit générer. Ce contrôle par le label permet de rassurer, car il atteste de la conformité à un *corpus* d'exigences et de solutions que les éditeurs ont présentées. Il faut dès lors que le logiciel soit en adéquation fonctionnelle avec les besoins des professionnels, mais également qu'il soit en conformité avec la réglementation en vigueur. Les programmes concernés par cette évaluation sont aussi bien ceux qui sont présents dans les maisons et centres de santé que ceux disponibles pour les industriels et professionnels

(70) C. Strub, *Contribution de la Blockchain au management des données de santé*, *Researchgate* (thèse d'exercice), juin 2020 (www.researchgate.net/publication/342871864_Contribution_de_la_Blockchain_au_management_des_donnees_de_sante_-_These_d%27_Exercice_Cedric_Strub_-_final).

(71) ANSM, Programme de travail 2019 (https://ansm.sante.fr/var/ansm_site/storage/original/application/485b914bc398277585b267955cd8ad92.pdf).

(72) INSERM, *Intelligence artificielle et santé, des algorithmes au service de la médecine*, 6 juill. 2018 (www.inserm.fr/information-en-sante/dossiers-information/intelligence-artificielle-et-sante).

de santé[73]. Il coexiste deux niveaux de labellisation, l'un dit « standard » et l'autre dit « avancé »[74]. Ce label fait transparaître le souci du contrôle nécessaire pour qu'un logiciel puisse être utilisé en toute confiance.

## II. – Le contrôle des outils numériques susceptibles de faciliter l'évaluation des produits de santé

Bien que révolutionnaire, l'idée d'inclure des outils numériques dans l'évaluation de mise sur le marché demeure controversée. En effet, pour l'incorporer dans nos processus, il faut préalablement réfléchir aux questions éthiques. Dans le passé, lors de l'activation des IA dans nos smartphones, il avait été question de la marche à suivre : en d'autres termes d'y inclure une certaine éthique ou alors de répondre purement aux questions des utilisateurs. C'est là tout l'enjeu des technologies qui ne peuvent remplacer totalement les humains, mais qui peuvent tout de même faciliter les procédures. En l'occurrence, concernant leur intégration dans l'évaluation des produits de santé, la solution actuelle allie les deux idées : on inclut du numérique, de ce fait les outils technologiques accélèrent le processus, tout en installant également un « garde-fou » : les humains, qui sont responsables de surveiller et de contrôler ces différents outils.

C'est la raison pour laquelle réguler les outils numériques demeure une préoccupation indissociable à leur intégration dans les processus de mise sur le marché. Aux États-Unis, un programme visant à tester des certifications pour des logiciels à vocation médicale avait déjà vu le jour, « le programme Pré-cert »[75]. Impulsé par la FDA, ce programme vise à contribuer à un futur modèle réglementaire permettant une surveillance plus rationnelle des dispositifs médicaux, eux-mêmes basés sur des logiciels développés par des fabricants (par ex. : Apple – les montres connectées). En effet, la FDA tente de calquer les mécanismes de surveillance des logiciels, pour les transposer vers une surveillance des événements indésirables ou aux problèmes de sécurité qui pourraient survenir lors de l'utilisation des DM connectés. L'importance de ce programme est liée au fait que la FDA se base sur les résultats de ces études pour les autoriser. La complexité des dispositifs médicaux connectés fait qu'il est préférable d'instaurer un mécanisme de pré-certification, qui se traduit par un examen simplifié avant même d'atteindre le marché et qui permettra un accès plus rapide aux patients. De plus, ce contrôle pousse les industriels qui les développent à faire preuve de plus d'efficacité et de qualité lors du développement des logiciels. De ce fait, ce programme permet d'accélérer l'accès au marché en contrôlant les logiciels inclus dans les DM en amont et non seulement le produit en lui-même.

La FDA a également été le précurseur dans la mise sur le marché de médicaments connectés à travers la commercialisation en 2017 de la première pilule connectée nommée « Abilify MyCite ». Cet antipsychotique visait à assurer au prescripteur

(73) ANS, *Esanté, Label e-santé logiciel maisons et centres de santé, agence du numérique en santé* (https://esante.gouv.fr/labels-certifications/label-e-sante-logiciel-maisons-centres-de-sante, consulté le 8 avr. 2021).

(74) ANS, *Les solutions labellisées e-santé*, 18 janv. 2021 (https://esante.gouv.fr/labels-certifications/label-e-sante/solutions-labellisees).

(75) FDA, *Digital health Software Precertification (Pre-Cert) Program*, 2020 (www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-software-precertification-pre-cert-program).

une traçabilité quant à la prise de médicament du patient. En effet, dans les cas de maladies liées à la santé mentale, une étude menée par l'Organisation mondiale de la santé a démontré qu'un nombre élevé de rechutes étaient directement liées aux ruptures lors de la prise de médicaments. Partant de ce postulat, cette pilule comprenant un capteur de la taille d'un grain de sel permettrait aux prescripteurs de tracer l'absorption de ce produit. Le mécanisme se base sur le signal émis lors du contact de la puce avec les sucs gastriques, confirmant alors la bonne prise du médicament. Malgré l'obtention d'une AMM aux États-Unis(76), ce produit n'a pas obtenu d'AMM en France du fait du manque de données probantes démontrant la qualité de cette innovation, menant à un retrait par la demande d'autorisation réalisée par le laboratoire(77). Une fois de plus, cela soulève des questions quant au contrôle de ces nouvelles technologies qui sont, pour l'instant, contrôlées par des êtres humains.

Concernant les logiciels d'aide à la prescription (LAP), c'est suite à une question préjudicielle du 7 décembre 2017(78) que la Cour de justice de l'Union européenne précise leur qualification juridique. De même, elle ajoute l'exigence d'une obligation nécessaire et suffisante de l'apposition d'un marquage CE, pour contrôler leur conformité lors de leur évaluation précédant leur accès au marché. Cette décision est importante, car elle va à l'encontre de la volonté nationale qui souhaitait instaurer une double certification aux LAP, c'est-à-dire un marquage CE et une certification provenant de la HAS. Il va sans dire qu'en retraçant le contexte national qui subit les retombées de l'affaire *Mediator*, l'objectif était de tendre vers une sécurité et une efficacité irréprochables dans le but d'éviter un autre scandale. La France aborde prudemment la question de l'instauration du numérique dans l'évaluation des produits de santé. En effet, la sensibilité du secteur médical pousse à une plus stricte élaboration de processus de contrôle de ces logiciels.

Concernant les maisons et centres de santé, un label « e-santé »(79) a déjà été élaboré par le ministère de la Santé en collaboration avec l'Agence du numérique en santé. Ce label permet d'attester la conformité du logiciel utilisé avec les exigences présentes dans le Référentiel fonctionnel de labellisation (RF) en vigueur depuis 2016. Il existe plusieurs catégories allant du niveau 1 : le « niveau standard », au niveau 2 : le « niveau avancé ». L'utilisation de la certification dans ce domaine démontre la possibilité de contrôler les outils numériques également dans l'évaluation des produits, ce qui est indispensable à leur arrivée sur le marché. Ce label permet notamment de vérifier la compatibilité au dossier médical partagé, ou encore d'identifier s'il est bel et bien conforme à la réglementation en vigueur(80).

(76) FDA, *FDA approves pill with sensor that digitally tracks if patients have ingested their medication*, 13 nov. 2020 (www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication).

(77) AEM, *Retrait de la demande d'autorisation de mise sur le marché*, 17 juill. 2020 (www.ema.europa.eu/en/medicines/human/withdrawn-applications/abilify-mycite).

(78) CJUE, 7 déc. 2017, aff. C-329/16, *Réglementation nationale soumettant les logiciels d'aide à la prescription médicamenteuse à une procédure de certification établie par une autorité nationale* (http://curia.europa.eu/juris/document/document.jsf?text=&docid=197527).

(79) ANS, *Les solutions labellisées e-santé*, 18 janv. 2021 (https://esante.gouv.fr/labels-certifications/label-e-sante/solutions-labellisees).

(80) ASIP-Santé, *Règlement du label « e-santé ». Logiciel Centres de santé*, 31 mars 2016 (https://esante.gouv.fr/sites/default/files/media_entity/documents/label_e-sante_centres_de_sante_v2_reglement_version_v4.0_du_31_mars_2016.pdf).

Cette solution permet un contrôle des logiciels utilisés dans le secteur de la santé et démontre la complémentarité de l'instauration du numérique avec des « garde-fous ». Ce mécanisme pourrait, et devrait être retranscrit dans les différents processus visant à évaluer les produits de santé.

L'optimisation des outils de contrôle quant aux instruments numériques utilisés dans le monde de la santé doit respecter la sécurité à laquelle l'utilisateur doit légitimement s'attendre(81). Par ailleurs, ce critère lié à la sécurité est indispensable pour dégager des bénéfices significatifs comparés aux risques inhérents pouvant en résulter.

SECTION 3

## LE « BÉNÉFICE/RISQUE » DE L'UTILISATION DU NUMÉRIQUE DANS LE MONDE DE LA SANTÉ

Il est parfois compliqué de concilier l'utilisation du numérique avec le système de santé. En effet, en dépit des progrès que ces outils apportent (§ 1), des difficultés demeurent quant à la protection des données sensibles des personnes (§ 2).

### § 1. – Vers une optimisation du monde de la santé à travers le déploiement du numérique

Le numérique est à l'origine de nombreuses évolutions en matière de santé. C'est un outil qui est devenu indispensable afin d'accélérer l'obtention d'une autorisation de mise sur le marché. Les industriels et autorités de santé s'en sont saisis comme un moyen de simplification des échanges, de réduction des coûts et des délais. Ce mécanisme s'appuie sur des données qui constituent la base de l'intelligence artificielle. Cette mise en commun d'informations a pour objet de donner aux pouvoirs publics, mais également aux acteurs privés, un meilleur accès en accélérant la circulation de ces données.

Il est désormais possible de réduire les coûts en utilisant un outil de prédiction du succès d'un médicament. Ce cas s'est retranscrit dans le domaine thérapeutique du cancer, où une équipe de médecins, chercheurs et ingénieurs a utilisé une intelligence artificielle nommée Resolved2, qui permet de déterminer si la molécule pourra être autorisée dans les six ans à venir, en se fondant sur des données pharmacologiques et des essais cliniques de phase I en cancérologie. Ce nouvel outil permet aux industriels de réduire considérablement les coûts de recherche et, par conséquent, du médicament une fois que celui-ci sera autorisé sur le marché, car les délais et les essais cliniques voués à l'échec seront considérablement limités(82).

(81) C. civ., art. 1386-4, concernant les produits défectueux.

(82) Mutualité Française, *Innovation mutuelle. Cancer, une intelligence artificielle prévoit le succès d'un médicament*, 20 déc. 2019 (www.innovation-mutuelle.fr/actualite/cancer-une-intelligence-artificielle-prevoit-le-succes-dun-medicament).

Lorsque cette technologie prédit qu'une molécule ne pourra pas être autorisée sur le marché, l'information s'avère fiable dans 92 % des cas.

Dans le même cadre, le Sniiram, devenu Système national des données de santé (SNDS), contient des données de l'assurance maladie. Il est utilisé afin de réaliser des études visant à évaluer les médicaments[83]. Cet outil permet de réduire les coûts pour les industriels, car ses données sont utilisées pour évaluer la sécurité du médicament et ainsi évaluer le coût du traitement. L'assurance maladie use de cette base de données en s'appuyant sur des algorithmes de définition de pathologies afin d'établir son chapitre sur « la cartographie des dépenses de soins et des pathologies ».

Le numérique a un effet sur les autorités de santé, car les produits de santé intégrant de l'intelligence artificielle doivent être évalués selon des standards qu'il faut mettre en place. Aux États-Unis, la FDA a instauré, en janvier 2021, un plan d'action pour la certification des logiciels d'intelligence artificielle et *machine learning* afin de les évaluer en tant que dispositifs médicaux. Le 7 février 2020, elle avait autorisé la mise sur le marché du premier logiciel d'échographie cardiaque qui utilise l'intelligence artificielle[84]. La FDA a fait mention de ce logiciel afin de décrire son plan d'action d'évaluation de ces logiciels en tant que dispositifs médicaux[85]. Ce nouveau plan permet de donner des exemples de lignes de conduite qui pourront être suivies par les autres autorités de santé pour l'évaluation de ce type de produits de santé.

De surcroît, la pandémie sans précédent de Covid-19, à laquelle les États doivent faire face depuis décembre 2019, a contribué à la modification de la perception du numérique par les autorités de santé. En effet, pour s'adapter à la vitesse de la progression du virus, les autorités devaient utiliser des outils numériques performants. Afin d'en évaluer l'efficacité, l'OMS a entrepris une évaluation des systèmes d'information sanitaires nationaux et a publié l'ensemble de ses constatations le 1er février 2021. Ce rapport met en exergue la nécessité de renforcer les systèmes d'information, car ceux-ci ont des difficultés à fournir les données en temps réel. Par ailleurs, il en résulte que l'absence d'un système mondial d'information limite indéniablement la planification d'actions concrètes. Par conséquent, l'Organisation mondiale de la santé a mis en place un outil nommé SCORE (*Survey*, *Optimize*, *Review*, *Enable* – Étudier, Comptabiliser, Optimiser, Analyser) afin de répondre aux besoins de la gestion de la crise sanitaire actuelle. Ce dernier va contenir « un ensemble de techniques d'interventions essentielles, d'actions recommandées, d'outils, de ressources » qui permettront aux pays de répondre « aux besoins de tout système d'information sanitaire ». L'objectif visé par l'OMS, au profit des États, est la possibilité d'utiliser les données sanitaires de façon efficace, tout en les analysant pour

(83) Ameli.fr, *Le Sniiram est le système national d'information interrégimes de l'assurance maladie*, 14 mai 2019 (www.ameli.fr/l-assurance-maladie/statistiques-et-publications/sniiram/etudes-realisees-avec-le-sniiram.php).

(84) IRSN, Institut de radioprotection et de sûreté nucléaire, *La certification des logiciels d'IA/ML en tant que dispositifs médicaux est en marche aux USA* (www.thema-radiologie.fr/actualites/2861/la-certification-des-logiciels-d-ia-ml-en-tant-que-dispositifs-medicaux-est-en-marche-aux-usa.html).

(85) FDA, *Artificial Intelligence/Machine Learning (AI/ML) – Based Software as a Medical Device (SAMD Action plan January 2021)* (www.fda.gov/media/145022/download).

répondre aux problématiques posées sur le plan sanitaire et agir rapidement[86]. Finalement, la pandémie de Covid-19 a renforcé l'usage du numérique, et il semble difficile désormais de limiter son expansion dans les usages en santé. Les prescriptions, les demandes d'autorisations de mise sur le marché, les téléconsultations, les bases de données, les négociations, tous ces éléments et bien plus sont désormais réalisés en ligne. La praticité de cette évolution n'est plus à démontrer, seulement le digital est soumis à une menace qui se perfectionne grâce à son évolution.

## § 2. – Les « effets indésirables » de cette immersion du numérique dans le monde de la santé

En dépit du progrès certain apporté par l'utilisation du numérique dans le secteur de la santé, il n'en demeure pas moins que ces outils doivent être utilisés avec prudence et avoir une législation stricte afin d'éviter certains débordements et abus dans leur manipulation.

Malgré toutes les optimisations qu'apporte l'utilisation du numérique au niveau de la mise sur le marché des médicaments, il n'en reste pas moins que des problématiques associées à leur maniement peuvent apparaître. À titre d'exemple, la ressource numérique des bases de données met en exergue des complexités notamment liées à leur protection. Selon la CNIL, les données de santé sont des données à caractère personnel particulières qui font l'objet d'une protection particulière par les textes dont principalement le règlement européen de protection des données (RGPD). Ce texte donne une définition large des données de santé et il convient d'apprécier si une donnée recueillie entre dans son champ d'application. Pour cette raison, ces données sont considérées comme sensibles et le législateur ainsi que les autorités compétentes y accordent une importance particulière et s'emploient à les protéger. En effet, la récolte de ces données est soumise à l'obligation d'obtenir le consentement du patient dont les données vont être utilisées. Cependant, il y a plusieurs exceptions à ce principe en fonction de la finalité poursuivie pour le traitement des données. Ces finalités peuvent soit porter sur des intérêts publics, comme la gestion des systèmes de santé ou la préservation de la santé publique dans le but d'éviter la propagation de maladie ; soit porter sur les intérêts privés des personnes comme l'appréciation médicale telle que la médecine préventive ou la préservation des intérêts vitaux d'une personne en incapacité de donner son consentement.

Les données relatives au secteur médical sont sous une menace croissante selon plusieurs études. Une récente étude tirée du journal *Health Insurance Portability and Accountability Act* (HIPAA) note une progression non négligeable dans la mise en péril de documents de santé divulgués au fil des ans. Entre 2017 et 2019, une

(86) OMS, *Rapport mondial, l'OMS souligne le besoin urgent de meilleures données pour renforcer la riposte à la pandémie et améliorer les résultats en matière de santé*, 1er févr. 2021 (www.who.int/fr/news/item/01-02-2021-who-score-global-report-highlights-urgent-need-for-better-data-to-strengthen-pandemic-response-and-improve-health-outcomes).

progression de 32 millions de documents divulgués sur Internet a été notée[87]. Ceci concerne également les données des fabricants de produits de santé qui sont transmises numériquement aux agences qui délivrent les autorisations de mise sur le marché. En décembre 2020, l'Agence européenne des médicaments a été la cible d'une cyberattaque en pleine délibération pour les autorisations de mise sur le marché des vaccins Pfizer et BioNTech[88]. Effectivement, des documents concernant ces mêmes vaccins ont été piratés, ce qui soulève énormément de questions quant à la fiabilité même des systèmes de sécurité d'une des plus importantes agences du médicament au monde. Les pratiques de piratage se sont développées de manière exponentielle pendant la crise de la Covid-19, constituant une épidémie au sein de l'épidémie.

Le problème des cyberattaques touche également les dispositifs médicaux. En effet, ces dernières années, plusieurs établissements français ont été piratés, donnant accès aux données des patients contenues dans les dispositifs médicaux. En 2016, une pompe à perfusion avec WiFi commercialisée par Johnson et Johnson a été retirée du marché, car elle était vulnérable aux cyberattaques. Quant aux algorithmes et aux intelligences artificielles, la CNIL[89] a souligné des problématiques pouvant s'y raccorder, telles que la délégation excessive aux machines qui pourrait mettre en péril l'autonomie humaine, la discrimination ou l'exclusion qui constitue des effets précédemment identifiés de ces outils. Selon Christine Balaguée, membre du Comité d'éthique de la recherche sur le numérique (CERNA) et de l'Institut DATAIA spécialisé sur les sciences des données, l'intelligence artificielle et la société : « La pertinence des résultats d'un algorithme dépend des informations qui lui sont fournies pour son apprentissage, de la manière dont il fonctionne, des paramètres configurés », ce qui peut poser un réel problème d'éthique et qui appelle à une vigilance extrême[90].

Un autre aspect est à considérer dans l'intégration du numérique en santé. En effet, les outils connectés nécessitant une certaine traçabilité des comportements pour être fonctionnels vont parfois empiéter sur certaines libertés individuelles. Cette problématique est loin d'être théorique, car la Cour de cassation a dû trancher un litige[91] au sein duquel une caisse de sécurité sociale souhaitait suspendre la prise en charge d'un traitement contre l'apnée du sommeil du fait que le patient ne l'utilisait pas suffisamment. Cet appareil disposait d'un dispositif d'observance intégré, signalant ainsi de manière indirecte quand il était utilisé ou non. Cette solution n'a pas été acceptée et la cour a finalement jugé cette hypothèse abusive. Toutefois,

(87) Portail d'Accompagnement Cybersécurité des Structures de Santé, *Neuf fuites de données liées à des acteurs de la santé répartis dans le monde* (www.cyberveille-sante.gouv.fr/cyberveille-sante/1475-neuf-fuites-de-donnees-liees-des-acteurs-de-la-sante-repartis-dans-le-monde, consulté le 8 avr. 2021).

(88) *Cyberattaque en Europe : l'Agence du médicament a été piratée : Le Figaro* (www.lefigaro.fr/flash-eco/l-agence-europeenne-des-medicaments-se-dit-victime-d-une-cyberattaque-20201209, consulté le 8 avr. 2021).

(89) CNIL, *Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 15 déc. 2017 (www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de).

(90) S. Balfagon, *Algorithmes éthiques en santé : un défi technologique et societal*, 15 janv. 2015 (https://imtech.wp.imt.fr/2019/01/15/algorithmes-ethique-sante/).

(91) Cass. 2e civ., 18 juin 2015, n° 14-18.285, publié au bulletin.

la question de la surveillance malveillante des patients à travers des produits de santé connectés demeure et ne doit pas être négligée.

Le numérique met à la disposition du monde de la santé des outils formidables qui permettent de jouer un rôle essentiel. Il convient de les perfectionner pour rendre les bases de données et les documents informatiques moins vulnérables aux cyberattaques, mais également de respecter deux principes dégagés par la CNIL concernant les algorithmes et les intelligences artificielles qui sont : loyauté et vigilance[92]. De cette façon, une conscience des risques, une utilisation responsable et sécurisée de ces outils pourrait révolutionner le monde de la santé et permettre à la France d'envisager un programme tel que le projet « vision for eHealth » pour 2025[93]. Ce projet, révélateur de la place de l'innovation suédoise dans l'économie de la santé, a pour objectif de faire de la Suède « le pays n° 1 au monde dans l'utilisation des opportunités offertes par la digitalisation et la santé numérique d'ici 2025 », et ceci dans le but de « faciliter l'accès à une santé et à une protection égale pour les gens »[94]. Le pays est actuellement en pleine création d'une infrastructure numérique de pointe afin de simplifier l'utilisation coordonnée et efficace des banques de données ainsi que des registres nationaux. Les pays nordiques étant pionniers dans le domaine de la santé numérique, leur exemple pourrait donc permettre une avancée rapide, mais également une anticipation des risques dans le domaine de l'innovation en santé.

Cette approche devrait permettre à la Commission européenne de s'engager dans une démarche de contrôle des critères de mise sur le marché des produits connectés, applicable à l'ensemble des États membres, afin de rendre cohérentes et sécurisées tout à la fois la mise sur le marché et la qualification juridique du produit, mais aussi la surveillance de son impact dans la vie de l'utilisateur et du patient, concernant la protection des données de la vie privée, et des libertés fondamentales. Par ailleurs, et surtout, la mise sur le marché donne l'autorisation de distribution du produit ou service numérique et, en conséquence, implique la détermination précise des responsabilités résultant de son utilisation, qu'il s'agisse du fabricant, du concepteur du logiciel, de la plateforme, voire de l'utilisateur, peu ou mal formé, ou encore du patient qui détourne le produit de son usage initial. Parce que ces produits sont spécifiques, innovants, et en permanente évolution, l'approche juridique et réglementaire se doit d'être appréhendée avec agilité en s'adaptant, voire en anticipant les conditions, modalités et risques de ces usages.

(92) CNIL, *Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle*, 15 déc. 2017 (www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de).

(93) Ehalsa, *Vision for ehealth 2025* (https://ehalsa2025.se/wp-content/uploads/2018/03/Handlingsplan-e-hälsa-engelsk-version.pdf).

(94) École de guerre économique, *L'innovation suédoise dans l'économie de la santé et ses limites*, 2020, (www.ege.fr/sites/ege.fr/files/uploads/2020/01/EconomieSanteSuede.pdf).

## Bibliographie

### Articles


• H. Alami et a., *Cadre stratégique pour soutenir l'évaluation des projets complexes et innovants en santé numérique : Santé publique* 2020/2-3, vol. 32, p. 221 à 228 (www.cairn.info/revue-sante-publique-2020-2-page-221.htm?contenu=article).

• Alcimed, *Comment l'IA peut-elle accélérer la découverte des médicaments ?*, 31 mars 2020 (www.alcimed.com/fr/les-articles-d-alcim/comment-ia-peut-elle-accelerer-la-decouverte-de-medicaments).

• S. Balfagon, *Algorithmes éthiques en santé : un défi technologique et sociétal* (https://imtech.wp.imt.fr/2019/01/15/algorithmes-ethique-sante).

• M. Bernelin, *La médecine connectée : interrogations et renouveau pour le droit international de la santé : RD sanit. soc.* 2018, p. 1007 et s.

• D. Bradburry, *Johnson and Johnson, 4 Ways Johnson & Johnson Is Leading the Fight Against Cyberattackers*, 8 oct. 2017 (www.jnj.com/innovation/johnson-and-johnson-leading-fight-to-prevent-cyberattacks).

• *Cyberattaque en Europe : l'Agence du médicament a été piratée : Le Figaro*, 9 déc. 2020 (www.lefigaro.fr/flash-eco/l-agence-europeenne-des-medicaments-se-dit-victime-d-une-cyberattaque-20201209).

• J. Declinat, *Les innovations dans la santé se focalisent sur l'accessibilité des soins et le bien-être*, Twelve-consulting (www.twelve-consulting.com/ces-2017-episode-34-les-innovations-dans-la-sante-se-focalisent-sur-laccessibilite-des-soins-et-le-bien-etre-by-jeremy-daclinat).

• N. Devillier, *Chapitre 5. Santé et Big data : l'émergence d'un droit d'infrastructure dans l'espace numérique : Journal international de bioéthique et d'éthique des sciences* 2017/3, vol. 28, p. 51 à 56 (www.cairn.info/revue-journal-international-de-bioethique-et-d-ethique-des-sciences-2017-3-page-51.htm).

• *ECommerce : l'IA peut maintenant prédire si vous allez retourner un produit*, 2 juill. 2019 (www.lebigdata.fr/ecommerce-ia-retour-produit).

• C. Fitaire, A. Geissbuhler, M.-L. Kaiser, J. Demeulemeester et J. Sommer, *Comment l'intelligence artificielle va-t-elle bouleverser la médecine ? : Rev. méd. Suisse* 2018, vol. 14, 2178-2180, RMS n° 629 (www.revmed.ch/RMS/2018/RMS-N-629/Comment-l-intelligence-artificielle-va-t-elle-bouleverser-la-medecine).

• E. de Gastines et N. Collet, *Les experts du numérique, santé, l'usine de santé, Optimiser les budgets marketing : le casse-tête de la pharma digitale : L'Usine digitale* 19 juin 2015 (www.usine-digitale.fr/article/optimiser-les-budgets-marketing-le-casse-tete-de-la-pharma-digitale.N337096).

• S. Goldstein, *Le RGDP et les données de santé*, LegalPlace, 5 juill. 2021 (www.legalplace.fr/guides/rgpd-donnees-sante).

• J. Le Gat, *Logiciels d'aide à la décision : quels enjeux pour l'accès au marché ?* (https://dumas.ccsd.cnrs.fr/dumas-02455018/document).

• A. Mahmoudi, *Booster l'efficacité et accélérer la mise sur le marché de médicaments* (www.docusign.fr/blog/booster-lefficacite-et-accelerer-la-mise-sur-le-marche-de-medicaments).

• A.-C. Maillols-Perroy, *LFSS pour 2021 : les points clés dans le domaine des médicaments* (www.editions-legislatives.fr/actualite/lfss-pour-2021-les-points-cles-dans-le-domaine-des-medicaments).

• D. Mascret, *L'inhumanité des algorithmes en santé agite le monde médical*, 4 janv. 2019 (www.lefigaro.fr/sciences/2019/01/04/01008-20190104ARTFIG00259-l-inhumanite-des-algorithmes-en-sante.php) ; *Les nouvelles règles juridiques de la prise en charge de l'innova-*

*tion des technologies en santé par l'assurance maladie : LPA* 17 avr. 2015, n° 77, p. 4 (www.labase-lextenso.fr/petites-affiches/PA201507703?em=dispositif%20médical%20technique).

• G. Morisse et G. Hochard, *Vers un standard d'évaluation des dispositifs médicaux embarquant de l'IA*, Quantmetry, 8 janv. 2020 (www.quantmetry.com/blog/standard-devaluation-dispositifs-medicaux-embarquant-lia).

• J. Peigné, *La notion de dispositif médical issue du règlement (UE) n° 2017/745 : RD sanit. soc.* 2018, p. 5.

• M.-P. Planel, *L'évaluation des produits de santé par le CEPS*, *Appraisal of medicinal products by the French CEPS : Med Sci* (Paris) 2018, 34, hors-série n° 1, 50-51 (www.medecines-ciences.org/en/articles/medsci/full_html/2018/05/medsci180156s/medsci180156s.html).

• Prnewswire, *Le premier médicament commercial fabriqué à l'aide de la technologie AJIPHASE d'Anijomoto Biopharma services reçoit l'approbation de la FDA*, 7 oct. 2020 (www.prnewswire.com/news-releases/le-premier-medicament-commercial-fabrique-au-moyen-de-la-technologie-ajiphase-d-ajinomoto-bio-pharma-services-recoit-l-approbation-de-la-fda-840409091.html).

• V. Raimond, F. Midy, C. Thébaut et C. Rumeau-Pichon *L'évaluation économique des produits de santé innovants : quelle interprétation pour quel usage ? : RF aff. soc.* 2016/3, p. 263 à 281 (www.cairn.info/revue-francaise-des-affaires-sociales-2016-3-page-263.htm).

• M.-P. Serre et D. Wallet-Wodka, *Stratégie d'accès au marché – Médicaments remboursables, selfcare, cosmétiques et aliment santé* (http://unr-ra.scholarvox.com/catalog/book/docid/88821993?searchterm=AMM).

## Thèses

• A. Feroyard, *Constitution d'un dossier d'autorisation de mise sur le marché d'un médicament à usage humain et ses différentes procédures d'enregistrement en Europe*, thèse pour le diplôme d'état de docteur en pharmacie (https://dumas.ccsd.cnrs.fr/dumas-01064013/document).

• C. Strub, *Contribution de la Blockchain au management des données de santé : Researchgate* (thèse d'exercice) (www.researchgate.net/publication/342871864_Contribution_de_la_Blockchain_au_management_des_donnees_de_sante_-_These_d%27_Exercice_Cedric_Strub_-_final).

## Rapports, études, communications, avis

• AEM, *Retrait de la demande d'autorisation de mise sur le marché* (www.ema.europa.eu/en/medicines/human/withdrawn-applications/abilify-mycite).

• Ameli.fr, *Le Sniiram est le système national d'information interrégimes de l'assurance maladie* (www.ameli.fr/l-assurance-maladie/statistiques-et-publications/sniiram/etudes-realisees-avec-le-sniiram.php).

• ANS, *Les solutions labellisées e-santé* (https://esante.gouv.fr/labels-certifications/label-e-sante/solutions-labellisees) ; *Esanté – Label e-santé logiciel maisons et centres de santé, agence du numérique en santé* (https://esante.gouv.fr/labels-certifications/label-e-sante-logiciel-maisons-centres-de-sante).

• ANSM :

– *Soumission électronique CESP (Common European Submission Platform)* (www.ansm.sante.fr/Activites/Autorisations-de-Mise-sur-le-Marche-AMM/Soumission-des-demandes/(offset)/9).

– *Algorithme electron Monte Carlo (eMC) du logiciel de radiothérapie Eclipse-Varian-information de sécurité* (https://ansm.sante.fr/S-informer/Informations-de-securite-Autres-mesures-de-securite/Algorithme-Electron-Monte-Carlo-eMC-du-logiciel-de-radiotherapie-Eclipse-Varian-Information-de-securite).

– Communiqué de presse, *S'engage dans l'accès plus rapide et plus sûr aux médicaments innovants pour les patients* (www.ansm.sante.fr/S-informer/Communiques-Communiques-Points-presse/L-ANSM-s-engage-dans-l-acces-plus-rapide-et-plus-sur-aux-medicaments-innovants-pour-les-patients-Communique).

– *E-Saturne : demande d'ATU nominative* (www.ansm.sante.fr/Activites/Autorisations-temporaires-d-utilisation-ATU/e-saturne-demande-d-ATU-nominative/(offset)/2).

– *Évaluation des demandes de mise sur le marché* (www.ansm.sante.fr/Dossiers/COVID-19-Vaccins/Evaluation-des-demandes-de-mise-sur-le-marche/(offset)/2).

– *Mise sur le marché des dispositifs médicaux et dispositifs médicaux de diagnostic in vitro (DM/DMIA/DMDIV)* (www.ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Logiciels-et-applications-mobiles-en-sante/(offset)/3).

– *Optimisation des délais d'instruction d'une demande d'AMM soumise en procédure nationale, Optimisation des délais d'instruction d'une demande d'AMM…* (www.ansm.sante.fr).

– *Programme de travail de 2019* (https://ansm.sante.fr/var/ansm_site/storage/original/application/485b914bc398277585b267955cd8ad92.pdf).

– Rapport, Recommandation ANSM, *Cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie*, juill. 2019 (https://ansm.sante.fr/var/ansm_site/storage/original/application/2a6e925f1c47a2b829570af405a9bc31.pdf).

• ASIP-Santé, *Règlement du label « e-santé Logiciel Centres de santé »* (https://esante.gouv.fr/sites/default/files/media_entity/documents/label_e-sante_centres_de_sante_v2_reglement_version_v4.0_du_31_mars_2016.pdf).

• Assemblée nationale, Rapport d'information sur les objets connectés, enregistré à la présidence le 10 janvier 2017 (www2.assemblee-nationale.fr/documents/notice/14/rap-info/i4362/%28index%29/rapports-information).

• Association médicale mondiale, *Prise de position de l'AMM sur l'utilisation de l'intelligence augmentée dans les soins médicaux*, adoptée par la 70e assemblée générale, Tbilissi, Géorgie, oct. 2019 (www.wma.net/fr/policies-post/prise-de-position-de-lamm-sur-lutilisation-de-lintelligence-augmentee-dans-les-soins-medicaux).

• CNC, avis sur les objets connectés en santé, 7 juill. 2017 (https://wikipe.has-sante.fr/WikiPE/PHP/Multimedia.php?Concept=128834&langue=fr).

• CNIL :

– *Comment permettre à l'Homme de garder la main ?*, Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, 15 déc. 2017 (www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de).

– *Objets connectés n'oubliez pas de les sécuriser !* (www.cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser).

– *Santé – les données de santé* (www.cnil.fr/fr/sante).

• CNOM, *Livre blanc du Conseil national des médecins : de la e-santé à la santé connectée* (www.conseil-national.medecin.fr/sites/default/files/external-package/edition/lu5yh9/medecins-sante-connectee.pdf).

• CNS :

– Avis, 8 févr. 2018, adopté en assemblée plénière, *Faire en sorte que les Applications et objets connectés en santé bénéficient à tous* (https://solidarites-sante.gouv.fr/IMG/pdf/avis_cns_aoc_adopt_plen_0802_contrib_cnle_cncph_220218.pdf).

• Cour des comptes, Rapport, *Chapitre VIII sur la fixation du prix des médicaments : des résultats significatifs, des enjeux toujours majeurs d'efficience et de soutenabilité, un cadre d'action à fortement rééquilibrer*, sept. 2017 (www.ccomptes.fr/sites/default/files/2017-09/20170920-rapport-securite-sociale-2017-fixation-prix-medicaments.pdf).

• DGCCRF, Avis pour les objets connectés à la santé (www.vie-publique.fr/en-bref/20041-objets-connectes-pour-la-sante-lavis-de-la-dgccrf).

• DREES, *Les dépenses de santé en 2019 – Résultats des comptes de la santé* (https://drees.solidarites-sante.gouv.fr/publications-documents-de-reference/panoramas-de-la-drees/les-depenses-de-sante-en-2019-resultats).

• École de guerre économique, *L'innovation suédoise dans l'économie de la santé et ses limites* (www.ege.fr/sites/ege.fr/files/uploads/2020/01/EconomieSantéSuède.pdf).

• Ehalsa, *Vision for ehealth 2025* (https://ehalsa2025.se/wp-content/uploads/2018/03/Handlingsplan-e-hälsa-engelsk-version.pdf).

• EMA, *Guideline on the use of the CTD format in the preparation of a registration application for traditional herbal medicinal products* (www.ema.europa.eu/en/guideline-use-ctd-format-preparation-registration-application-traditional-herbal-medicinal-products).

• Fédération nationale de l'information médicale, *Les nouvelles données du market access* (www.lafnim.com/actualite/les-nouvelles-donnees-du-market-access-39.htm).

• Food *and Drug Administration* (FDA)

– *Artificial Intelligence/Machine Learning (AI/ML) – Based Software as a Medical Device (SAMD) Action plan*, janv. 2021 (www.fda.gov/media/145022/download).

– *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter : FDA Safety Communication*, 9 janv. 2017 (www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-identified-st-jude-medicals-implantable-cardiac-devices-and-merlinhome).

– *FDA approves pill with sensor that digitally tracks if patients have ingested their medication* (www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication).

– *Coronavirus (Covid-19) Update : FDA Authorizes Monoclonal Antibody for Treatment of Covid-19* (www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-authorizes-monoclonal-antibody-treatment-covid-19).

– *Guide des standards pour la prise en compte d'intelligences artificielles dites « évolutives »* (www.fda.gov/media/122535/download?utm_campaign=2019-04-02%20Discussion%20Paper%20on%20Regulating%20Artificial%20Intelligence&utm_medium=email&utm_source=Eloqua).

– *Guide permettant d'ébaucher un standard pour la prise en compte d'intelligences artificielles dites « évolutives »* (www.fda.gov/media/122535/download?utm_campaign=2019-04-02%20Discussion%20Paper%20on%20Regulating%20Artificial%20Intelligence&utm_medium=email&utm_source=Eloqua).

• Haute Autorité de santé (HAS)

– Commission de la transparence (www.has-sante.fr/jcms/c_412210/fr/commission-de-la-transparence).

– *Consultation publique sur le projet de grille d'analyse destinée à être utilisée par la CNEDiMTS pour contribuer à son évaluation de dispositifs médicaux embarquant des systèmes décisionnels s'appuyant sur des procédés d'apprentissage automatique (« Intelligence artificielle »)* (www.has-sante.fr/upload/docs/application/pdf/2019-11/notice_consultation_algorithmes.pdf).

– *Dépôt d'un dossier en vue d'un avis économique de la commission d'évaluation économique et de santé publique (CEESP)* (www.has-sante.fr/jcms/c_1627022/fr/depot-d-un-dossier-en-vue-d-un-avis-economique).

– *Évaluer les dispositifs médicaux avec intelligence artificielle* (www.has-sante.fr/jcms/p_3119829/fr/evaluer-les-dispositifs-medicaux-avec-intelligence-artificielle).

– *Évaluation des dispositifs médicaux, principes d'évaluation de la CNEDiMTS relatifs aux dispositifs médicaux à usage individuel en vue de leur accès au remboursement*, mai 2019

(www.has-sante.fr/upload/docs/application/pdf/2017-11/principes_devaluation_de_la_cnedimts-v4-161117.pdf).

– *Élaboration d'une grille d'analyse des algorithmes faisant appel à l'intelligence artificielle (IA) et intervenant dans les DM qui font l'objet d'une évaluation par la CNEDiMTS* (www.has-sante.fr/upload/docs/application/pdf/2019-12/cadrage_algorithmes.pdf).

– *Forfait innovation* (www.has-sante.fr/jcms/c_2035788/fr/forfait-innovation).

– *Médicaments : une évaluation rigoureuse et scientifique par la HAS* (www.has-sante.fr/jcms/pprd_2974176/en/medicaments-une-evaluation-rigoureuse-et-scientifique-par-la-has).

– *La commission d'évaluation économique et de santé publique* (www.has-sante.fr/upload/docs/application/pdf/2012-11/brochure_imprimablea3rectoverso.pdf).

– *La e-santé et la m-santé, des avantages concrets pour vos patients* (www.has-sante.fr/upload/docs/application/pdf/2019-10/e_sante_essentiel_en_4_pages.pdf).

– *Le service médical rendu (SMR) et l'amélioration du service médical rendu (ASMR)*, 16 avr. 2013 (www.has-sante.fr/jcms/r_1506267/fr/le-service-medical-rendu-smr-et-l-amelioration-du-service-medical-rendu-asmr).

– *Plan d'action pour l'évaluation des médicaments innovants* (www.has-sante.fr/upload/docs/application/pdf/2020-01/plan_daction_pour_les_medicaments_innovants_27.01.2020.pdf).

– *Projet de grille d'analyse pour l'évaluation de dispositifs médicaux avec intelligence artificielle* (www.has-sante.fr/jcms/p_3118247/fr/projet-de-grille-d-analyse-pour-l-evaluation-de-dispositifs-medicaux-avec-intelligence-artificielle).

– Rapport d'analyse prospective 2019, *Numérique quelle révolution ?* (www.has-sante.fr/upload/docs/application/pdf/2019-07/rapport_analyse_prospective_20191.pdf).

– *Un nouvel outil pour l'évaluation des dispositifs médicaux embarquant de l'intelligence artificielle*, 14 oct. 2020 (www.has-sante.fr/jcms/p_3212876/fr/un-nouvel-outil-pour-l-evaluation-des-dispositifs-medicaux-embarquant-de-l-intelligence-artificielle).

• Hellobiz, *La FDA approuve le premier médicament avec traqueur numérique* (https://hellobiz.fr/2017/12/12/fda-approuve-premier-medicament-traqueur-numerique-integre, www.fda.gov/news-events/press-announcements/fda-approves-pill-sensor-digitally-tracks-if-patients-have-ingested-their-medication).

• IEEE Xplore, 2019, 41e conférence internationale annuelle de la société d'ingénierie en médecine et de biologie de l'IEEE (EMBC), *Prévision de la défaillance des implants à l'aide de l'analyse discriminante* (https://ieeexplore.ieee.org/document/8856783).

• INSERM, *Intelligence artificielle et santé, des algorithmes au service de la médecine* (www.inserm.fr/information-en-sante/dossiers-information/intelligence-artificielle-et-sante).

• Inspection générale des affaires sociales, *Révision des critères d'évaluation des produits de santé en vue de leur prise en charge par l'assurance maladie, Analyse de l'index thérapeutique relatif ITR proposé par la HAS*, Mission d'appui à la direction de la sécurité sociale, Rapport de M. Dahan, oct. 2013 (www.apmnews.com/documents/201503231621510.Rapport_ITR.pdf).

• Institut Mines-Télecom I'M Tech, L'actualité scientifique et technologique de l'IMT, *Algorithmes éthiques en santé, un défi technologique et sociétal*, 15 janv. 2019 (https://blogrecherche.wp.imt.fr/2019/01/15/algorithmes-ethique-sante).

• Institut Montaigne, *Le prix des médicaments : des spécificités nationales dans un marché global* (www.institutmontaigne.org/blog/le-prix-des-medicaments-des-specificites-nationales-dans-un-marche-global).

• IRSN (Institut de radioprotection et de sûreté nucléaire), *La certification des logiciels d'IA/ML en tant que dispositifs médicaux est en marche aux USA* (www.thema-radiologie.fr/actualites/2861/la-certification-des-logiciels-d-ia-ml-en-tant-que-dispositifs-medicaux-est-en-marche-aux-usa.html).

• C. Kilchenmann, *Comparaison de prix avec l'étranger 2018, Prix et coûts des médicaments – de quoi parlons-nous ?*, SantéSuisse (www.santesuisse.ch/fileadmin/sas_content/Pressemappe-FR-final_01.pdf).

• LEEM, *Comment se décide une autorisation de mise sur le marché ?* (www.leem.org/comment-se-decide-une-autorisation-de-mise-sur-le-marche-amm) ; *Les entreprises du médicament, économie, accès au marché*, 6 oct. 2020 (www.leem.org/acces-au-marche).

• Medissimo, *Imedipac, le pilulier connecté*, www.medissimo.fr/wp-content/uploads/2015/05/imedipac_fr.pdf.

• Ministère de l'Économie, *Les objets connectés sont-ils fiables ?*, www.economie.gouv.fr/dgccrf/objets-connectes-sante-et-bien-etre-sont-ils-fiables.

• Ministère des Solidarités et de la Santé :

– *Les médicaments orphelins* (https://solidarites-sante.gouv.fr/soins-et-maladies/medicaments/le-circuit-du-medicament/article/les-medicaments-orphelins).

– *Base de données publique des médicaments* (http://base-donnees-publique.medicaments.gouv.fr).

– Comité économique des produits de santé, 25 sept. 2020 (https://solidarites-sante.gouv.fr/ministere/acteurs/instances-rattachees/article/ceps-comite-economique-des-produits-de-sante).

– *La fixation des prix et du taux de remboursement*, mis à jour le 10 nov. 2016 (https://solidarites-sante.gouv.fr/soins-et-maladies/medicaments/le-circuit-du-medicament/article/la-fixation-des-prix-et-du-taux-de-remboursement).

• Mutualité Française, *Innovation mutuelle, Cancer une intelligence artificielle prévoit le succès d'un médicament*, 20 déc. 2019 (www.innovation-mutuelle.fr/actualite/cancer-une-intelligence-artificielle-prevoit-le-succes-dun-medicament).

• OMS :

– *L'observance des traitements prescrits pour les maladies chroniques pose problème dans le monde entier*, www.who.int/mediacentre/news/releases/2003/pr54/fr.

– *Dans un rapport mondial, l'OMS souligne le besoin urgent de meilleures données pour renforcer la riposte à la pandémie et améliorer les résultats en matière de santé*, www.who.int/fr/news/item/01-02-2021-who-score-global-report-highlights-urgent-need-for-better-data-to-strengthen-pandemic-response-and-improve-health-outcomes.

• Portail d'Accompagnement Cybersécurité des Structures de Santé, *Neuf fuites de données liées à des acteurs de la santé répartis dans le monde* (www.cyberveille-sante.gouv.fr/cyberveille-sante/1475-neuf-fuites-de-donnees-liees-des-acteurs-de-la-sante-repartis-dans-le-monde).

• SANTÉPERSO, *Comprendre les algorithmes : alors que les algorithmes prédictifs prennent de plus en plus de place dans nos vies et la gestion de notre santé, comment être sûr qu'ils sont à la fois efficaces et sûrs ?* (https://santeperso.ch/Pour-comprendre/Algorithmes-l-epineuse-question-de-la-validation).

• Sénat :

– *Médicaments innovants : consolider le modèle français d'accès précoce* (www.senat.fr/rap/r17-569/r17-5693.html).

– Rapport d'information sur la réglementation américaine du médicament (www.senat.fr/rap/r96-196/r96-19682.html).

• Science Direct – Elsevier, Therapies, *« Intelligence artificielle » : quels services, quelles applications, quels résultats et quelle valorisation aujourd'hui en recherche clinique ? Quel impact sur la qualité des soins ? Quelles recommandations ?* (www.sciencedirect.com/science/article/pii/S0040595718302518).

• Techniques Hospitalières, *Évaluer les dispositifs médicaux avec l'intelligence artificielle, Service public hospitalier conseil* (www.techniques-hospitalieres.fr/content/6-editeur).

• Ticpharma, *L'OCDE encourage le recours au numérique pour renforcer le suivi du médicament (rapport)* (www.ticpharma.com/story/881/locde-encourage-le-recours-au-numerique-pour-renforcer-le-suivi-du-medicament-(rapport).html).

• Vie-publique, *Les nouvelles technologies au service de la santé* (www.vie-publique.fr/parole-dexpert/38509-nouvelles-technologies-sante).

• C. Villani, *Donner un sens à l'intelligence artificielle* (www.vie-publique.fr/sites/default/files/rapport/pdf/184000159.pdf#xd_co_f=MmNmMjRmMGMxNTJiZjM5MGVlMDE1ODE5NzI1NDAxMzc=~ ; www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf).

• W. Zirar, Rapport, *L'OCDE encourage le recours au numérique pour renforcer le suivi du médicament* (www.ticpharma.com/story/881/locde-encourage-le-recours-au-numerique-pour-renforcer-le-suivi-du-medicament-(rapport).html).

## Textes réglementaires et législatifs

Europe

– PE et Cons. UE, dir. 2004/27/CE, 31 mars 2004, modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ :L :2004 :136 :0034 :0057 :FR :PDF).

– PE et Cons. UE, règl. (CE) n° 1223/2009, 30 nov. 2009, relatif aux produits cosmétiques (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32009R1223&qid=1614121975600).

– PE et Cons. UE, règl. (UE) n° 528/2012, 22 mai 2012, concernant la mise à disposition sur le marché et l'utilisation des produits biocides (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ :L :2012 :167 :0001 :0123 :fr :PDF).

– Règl. (UE) n° 2017/745, 5 avr. 2017 (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32017R0745).

– PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32017R0745).

– PE et Cons. UE, règl. (UE) n° 2018/1718, 14 nov. 2018, portant modification du règlement (CE) n° 726/2004 en ce qui concerne la fixation du siège de l'Agence européenne des médicaments (https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX :32018R1718&from=EN).

– Comm. UE, Recomm. n° 2019/243, 6 févr. 2019, relative à un format européen d'échange des dossiers de santé informatisés (https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX :32019H0243&from=EN).

France

• D. n° 2019-855, 20 août 2019, relatif à la prise en charge précoce de certains produits de santé (www.legifrance.gouv.fr/jorf/id/JORFTEXT000038940078).

• L. n° 2020-1576, 14 déc. 2020, de financement de la sécurité sociale pour 2021 (www.legifrance.gouv.fr/jorf/id/JORFTEXT000042665307).

## Jurisprudence

• Cass. 2e civ., 18 juin 2015, n° 14-18.285, publié au bulletin (www.legifrance.gouv.fr/juri/id/JURITEXT000030759992).

• CJUE, 7 déc. 2017, aff. C-329/16, *Réglementation nationale soumettant les logiciels d'aide à la prescription médicamenteuse à une procédure de certification établie par une autorité nationale* (http://curia.europa.eu/juris/document/document.jsf?text=&docid=197527).

CHAPITRE 5

# L'IMPACT DU NUMÉRIQUE DANS LA PRODUCTION DES PRODUITS DE SANTÉ

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Leïla GUÉRIN
Laurène MIGNOT

La production du produit de santé est la phase la plus sensible, bien que la moins connue[1]. Elle est stratégique dans la mise sur le marché du produit. La pandémie a permis de faire la lumière sur cette phase qui exige des procédures de bonnes pratiques de fabrication (BPF)[2] et de distribution (BPD), et une stratégie sans faille afin d'assurer la livraison des produits au bénéfice du patient dans les temps, afin d'éviter les risques de ruptures d'approvisionnement ou encore les tensions d'approvisionnement.

L'OMS définit les Bonnes pratiques de fabrication (BPF) comme « un des éléments de l'assurance de la qualité, garantissant que les produits sont fabriqués et contrôlés de façon uniforme et selon des normes de qualité adaptées à leur utilisation et spécifiées dans l'autorisation de mise sur le marché ». Les BPF ou cGMP (*current Good Manufacturing Practices*) évoluent en permanence ainsi que leur interprétation, du fait de l'évolution des pratiques, des processus industriels, de l'intégration de nouvelles technologies et de l'amélioration continue. Ces normes sont d'autant plus importantes que les chaînes de valeur dans le domaine sont mondiales et fragmentées. La phase Covid-19 a démontré la très forte dépendance des industries à la Chine. La production pharmaceutique a donné lieu à une externalisation massive qui

(1) A. Alla, J. Beuve et B. Savatier, *Le cycle de vie de l'innovation pharmaceutique : le retard français*, Conseil d'analyse économique, janv. 2021, n° 053-2021. – LEEM (Les entreprises du médicament), *Production du médicament : comment retrouver une autonomie stratégique ?*, nov. 2020. – Observatoire 2016 des investissements productifs pharmaceutiques et biotechnologiques en France, *Restaurer l'attractivité du territoire pour les investissements de santé*, LEEM-KPMP-Polepharma, 20 juin 2017.

(2) BPF 2011, Eudralex « The rules governing Medicinal Products in the EU vol 4 – EU guidelines to GMP Medicinal Products for Human and Veterinary Use », GMP 21 CFR Parts 210 and 211.

provoque des risques majeurs de tensions d'approvisionnement et ruptures d'approvisionnement. Ces situations conduisent les politiques de santé à repenser le mode de production afin de favoriser la relocalisation de la production pharmaceutique sur le territoire européen. Toutefois, cet objectif est complexe à atteindre car la production des principes actifs et matières premières issues des ressources asiatiques notamment, demeure dans ces pays. Par ailleurs, la chaîne de production se caractérise par une grande fragmentation de l'activité globale répartie dans de nombreux territoires. Si le processus d'innovation repose sur la R&D, la production reste quant à elle la phase fondamentale. Les tensions dans l'approvisionnement de vaccins dans la phase de pandémie Covid-19 démontrent toute l'importance stratégique de l'organisation de la chaîne de production des produits pharmaceutiques.

La phase de production exige la contractualisation avec de nombreux fournisseurs du produit principal, matières premières sensibles, mais des produits de conditionnement de la matière. Elle exige donc une organisation particulièrement complexe en raison des risques liés à la fabrication elle-même pouvant entraîner des produits défectueux, ou encore des risques d'introduction dans la chaîne de produits falsifiés ou contrefaits. Ces dangers augmentent avec les tensions et ruptures d'approvisionnement. La falsification des médicaments est un fléau mondial qui s'est accru au cours des dernières années, et qui s'aggrave avec la phase de pandémie. Ainsi, le Conseil de l'Europe a adopté la Convention Medicrime[3], premier instrument juridique international érigeant en infraction pénale la fabrication de produits médicaux contrefaits. De plus, l'Organisation mondiale de la santé (OMS) indiquait, en 2018, qu'un médicament sur dix serait falsifié dans le monde[4]. Le produit falsifié a une définition bien spécifique qui a été adoptée en mai 2017, par l'OMS au cours de l'Assemblée mondiale de la santé[5].

L'OMS définit donc le produit falsifié comme un produit sciemment conçu pour sembler identique au produit d'origine. Il est souvent conçu sous la même forme et empaqueté dans un emballage similaire et présentant les mêmes caractéristiques que le produit authentique. Néanmoins la composition du produit falsifié est différente et présente un autre principe actif, un principe actif identique mais autrement dosé ou même aucun principe actif. Les produits médicamenteux falsifiés représentent donc un véritable danger pour la santé des individus.

C'est pour lutter contre l'intensification de ce fléau en Europe que le Parlement européen et le Conseil de l'Union européenne ont adopté le 8 juin 2011 la directive 2011/62/UE[6], ayant pour objectif de prévenir l'introduction de médicaments falsifiés dans la chaîne d'approvisionnement légale. Cette directive apporte une définition du médicament falsifié et le distingue notamment du médicament authentique présentant un défaut et du médicament contrefait. Elle prévoit de mettre en place des dispositifs permettant de sécuriser la chaîne pharmaceutique et des

(3) Cons. UE, Convention sur la contrefaçon des produits médicaux et les infractions similaires menaçant la santé publique, signée le 28 octobre 2011, ratifiée par la France le 21 septembre 2016 et entrée en vigueur en France le 1er décembre 2017.
(4) OMS, 2018.
(5) Dispositif des États membres concernant les produits médicaux de qualité inférieure/faux/faussement étiquetés/falsifiés/contrefaits, p. 38, 70e Assemblée mondiale de la santé, 20 mars 2017.
(6) PE et Cons. UE, dir. 2011/62/UE, 8 juin 2011.

dispositifs d'inviolabilité. Il est également prévu un renforcement du contrôle de la chaîne de distribution, ainsi que de la qualité des matières premières et les excipients utilisés. Enfin, la directive prévoit un meilleur encadrement de la vente des médicaments en ligne, Internet étant un mode de distribution très courant en ce qui concerne la vente de médicaments falsifiés.

Dès lors, l'expansion du nombre de produits de santé falsifiés, notamment due au développement de la vente en ligne, est un véritable problème de santé publique mondiale(7). Internet permet aux contrefacteurs de conserver leur anonymat et leur offre une certaine flexibilité(8) afin de s'adapter très rapidement à la demande. Ainsi, la pandémie de Covid-19 a entraîné une flambée des contrefaçons de masques chirurgicaux, de solutions hydroalcooliques ou encore de médicaments antiviraux, voire de vaccins vendus par Internet notamment aux USA. De plus, les trafics de médicaments sont par nature transfrontaliers, ce qui complexifie l'identification de ces réseaux très structurés. Ainsi, les États agissent collectivement, comme dans le cadre de l'opération Pangea III qui réunit près de 90 pays à travers le monde, coordonnée par Interpol(9). Dans le cadre de la Covid-19, cette opération a permis de saisir plus de 14 millions de dollars de produits pharmaceutiques potentiellement dangereux(10).

La production des produits de santé est inévitablement impactée et se trouve confrontée à de nouveaux défis. La réglementation européenne sur la sérialisation a pour objectif de renforcer la traçabilité des produits de santé, tout comme la réglementation sur les dispositifs médicaux imposant un marquage UDI. Toutefois, ces systèmes sont perfectibles grâce aux outils numériques aux différents stades de la production. L'intégration du numérique dans l'organisation de la chaîne de distribution est un élément particulièrement efficace, qui permet d'améliorer la surveillance et la traçabilité du produit, tout en accélérant la cadence de production (Section 1). Néanmoins, pour aller plus loin dans la sécurisation de la *supply chain*, il faut amorcer la transition numérique dans la production des produits de santé. Le développement du numérique dans la *supply chain* pharmaceutique avec l'introduction de la *blockchain* et de l'intelligence artificielle offre de nouvelles perspectives (Section 2).

SECTION 1

## LA SÉRIALISATION ET LA *BLOCKCHAIN*, DES OUTILS DE TRAÇABILITÉ, DE FIABILITÉ ET DE TRANSPARENCE

Le dispositif de sérialisation(11), qui vise à empêcher que des médicaments falsifiés ne soient introduits dans la chaîne logistique (§ 1), pourrait être complété par la technologie *blockchain* afin de renforcer le suivi des produits de santé (§ 2).

(7) LEEM, Rapport, *Contrefaçon des médicaments, une atteinte à la santé publique*, juin 2017.
(8) LEEM, Rapport, *Contrefaçon des médicaments, une atteinte à la santé publique*, juin 2017.
(9) Ordre des pharmaciens, 28 mai 2020.
(10) Interpol, *Une opération mondiale met au jour une augmentation des faux produits médicaux dans le contexte de la Covid-19*, 19 mars 2020.
(11) D. n° 2018-291, 20 avr. 2018, relatif à la sécurité de la chaîne d'approvisionnement des médicaments.

## § 1. – Entre sécurisation et alourdissement de la *supply chain*

En France, depuis le 9 février 2019[12], tous les médicaments soumis à prescription médicale obligatoire doivent être sérialisés et munis d'un dispositif anti-effraction. Ceci a pour objet de renforcer la vérification de l'intégrité et de l'authenticité des médicaments.

La sérialisation consiste à apposer un identifiant unique sur chaque boîte de médicaments afin d'en assurer la traçabilité tout au long de la chaîne de production et de distribution. Cet identifiant unique prend la forme d'un code Datamatrix[13] et contient de nombreuses informations telles que le code produit, le numéro de lot, la date de péremption et le numéro de série du médicament. Les laboratoires titulaires des autorisations de mise sur le marché transmettent toutes ces informations à un *hub* européen sécurisé qui se synchronise ensuite avec les systèmes nationaux. En France, le système FMVS[14] répertorie toutes les informations contenues dans le code Datamatrix.

Le code Datamatrix se distingue des codes-barres linéaires comportant une succession de barres noires parallèles. En effet, le code Datamatrix se rapproche du QR code et est composé de plusieurs rangées de pixels noirs et blancs. Ce code-barres bidimensionnel peut contenir plus d'informations que les codes-barres classiques et l'information contenue dans le code Datamatrix est lisible malgré une altération partielle de la zone d'impression.

Lors de la dispensation, le pharmacien doit s'assurer de la traçabilité du médicament et consulter le statut de la boîte de médicaments (boîte activée ou désactivée, boîte périmée, retrait de lot…). Le pharmacien interroge alors le système FMVS en scannant le code Datamatrix. Ceci permet de vérifier que les informations contenues dans le code Datamatrix correspondent avec celles renseignées dans la base de données.

Si les informations sont concordantes, la boîte de médicaments est dispensée et l'identifiant unique désactivé. En revanche, si les informations ne sont pas concordantes ou que l'identifiant unique a été désactivé avant la dispensation, la boîte de médicaments ne peut pas être remise au patient. Il est alors nécessaire d'en informer le fabricant, car un dysfonctionnement est probablement intervenu dans la chaîne de production du médicament.

La désactivation du code Datamatrix est une étape clé dans la traçabilité du médicament : lorsque l'identifiant unique est désactivé, le circuit du médicament n'est plus renseigné dans les bases de données de sérialisation. C'est pour cette raison que la désactivation du code Datamatrix est strictement encadrée. À titre d'exemple, les grossistes peuvent désactiver l'identifiant unique lorsque les produits sont distribués en dehors de l'Union européenne (UE)[15] ou à des structures ne disposant pas de pharmacien ou délivrant des médicaments dans des situations d'urgence[16].

(12) Comm. UE, règl. délégué (UE) n° 2016/161, 2 oct. 2015, art. 50.
(13) *Comment est constitué le système de code ? : France MVO* 10 janv. 2018.
(14) *France Medicines Verification System*.
(15) Comm. UE, règl. délégué (UE) n° 2016/161, 2 oct. 2015, art. 22.
(16) D. n° 2019-592, 14 juin 2019.

La mise en place de la sérialisation constitue une nouvelle contrainte réglementaire, technique mais aussi informatique. En effet, tous les acteurs de la *supply chain* ont dû s'adapter face à la mise en place des codes Datamatrix. Tout d'abord, les lignes de conditionnement des médicaments ont été équipées de nouvelles imprimantes capables de retranscrire un code Datamatrix et de nouveaux outils de contrôle d'impression pour vérifier que le code imprimé soit lisible. Ensuite, afin de retranscrire un code Datamatrix, des logiciels ont dû être développés afin de générer des codes alphanumériques aléatoires sur la base des données de sérialisation. La sérialisation impose donc que tous les équipements des circuits de production et les bases de données de sérialisation interagissent, échangent des données afin d'imprimer un code Datamatrix, puis centralisent toutes les informations de sérialisation.

Une première limite à l'efficacité de la sérialisation apparaît avec la désactivation du code Datamatrix des médicaments. En effet, deux boîtes de médicaments ne peuvent pas disposer d'un même identifiant. Si tel est le cas, il est possible que l'identifiant apposé sur une boîte de médicaments conforme aux bonnes pratiques de fabrication ait été assigné à une boîte de médicaments falsifiés. L'une des deux boîtes est donc falsifiée. Néanmoins, si la boîte de médicaments falsifiés est délivrée avant la boîte de médicaments conforme, le logiciel contenant les informations de sérialisation n'émettra aucune alerte. Une difficulté apparaît alors pour identifier la boîte de médicaments falsifiés si celle-ci dispose d'un identifiant unique généré grâce aux informations de sérialisation.

Une seconde limite apparaît, car la sérialisation est réservée à certains médicaments. En effet, le règlement délégué n° 2016/161 a établi deux listes permettant d'identifier les médicaments devant respecter la sérialisation. Ainsi, les médicaments soumis à prescription médicale obligatoire doivent être sérialisés, à l'exception des médicaments homéopathiques, de certains produits de contraste[17]. En revanche, par principe, les médicaments en vente libre sont dispensés de la sérialisation[18]. Or, tous les médicaments sont concernés par la falsification. Pour endiguer la falsification, la sérialisation devrait être appréhendée de manière globale et s'imposer à tous les médicaments et produits de santé.

En effet, les dispositifs médicaux, qui doivent disposer du marquage CE[19] sont également susceptibles d'être falsifiés. Par exemple, le recours en urgence à des dispositifs médicaux tels que des masques chirurgicaux, des tests virologiques et sérologiques durant la pandémie de Covid-19 a conduit à une augmentation des falsifications. Un arrêté ministériel[20] a alors précisé que l'évaluation des dispositifs médicaux par le Centre national de référence (CNR) devait prendre en compte le cahier des charges de la Haute Autorité de santé[21].

(17) *Cf.* Comm. UE, règl. délégué (UE) n° 2016/161, 2 oct. 2015, ann. I.
(18) *Cf.* Comm. UE, règl. délégué (UE) n° 2016/161, 2 oct. 2015, ann. II.
(19) Cons. CE, dir. 93/42/CEE, 14 juin 1993, relative aux dispositifs médicaux ; C. santé publ., art. R. 5211-12.
(20) A. 20 mai 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de Covid-19 dans le cadre de l'état d'urgence sanitaire.
(21) Cahier des charges définissant les modalités d'évaluation des performances des tests sérologiques détectant les anticorps dirigés contre le SARS-CoV-2, 16 avr. 2020.

Après le scandale des prothèses mammaires PIP, les exigences de mises sur le marché et de surveillance des dispositifs médicaux ont été renforcées aux plans national et européen.

Le règlement n° 2017/745 relatif aux dispositifs médicaux[22] prévoit la mise en place d'un système UDI[23] consistant à apposer un identifiant unique sur chaque dispositif médical. Toutes les informations renseignées dans le code UDI sont disponibles sur la base de données EUDAMED.

Le code UDI doit être lisible lors de l'utilisation normale du dispositif médical et durant toute sa durée de vie. En revanche, l'apposition de l'UDI n'est pas obligatoire si cela compromet la sécurité du dispositif médical.

L'objectif du système UDI est de suivre les dispositifs médicaux tout au long de la chaîne de distribution et au cours de leur utilisation. En effet, l'identifiant UDI garantit « un partage continu des données spécifiques au dispositif médical visé »[24] entre le fabricant, le professionnel de santé, le patient, en passant même par les établissements de santé. Ceci permet de renforcer la matériovigilance en facilitant le retrait des dispositifs médicaux défectueux et le partage des informations relatives à la sécurité du dispositif médical suite à des incidents par exemple.

Le système UDI va donc plus loin que la sérialisation des médicaments, la sérialisation prenant fin avec la dispensation. Le système UDI permet de suivre tout le cycle de vie des dispositifs médicaux, et ne se limite pas au suivi de la *supply chain*.

Bien que présentant une première étape dans le suivi et l'organisation du traçage numérique du produit de santé, la mise en place de la sérialisation pour le médicament et du système UDI pour le dispositif médical constitue une avancée importante permettant d'assurer la traçabilité du circuit des produits de santé. Ces mesures sont largement perfectibles et pourraient être renforcées et étendues à l'ensemble des produits. Le recours aux outils numériques tels que la mise en place de la *blockchain* ou encore l'implantation de l'intelligence artificielle dans la chaîne logistique du produit pourrait renforcer la fiabilité et la transparence de la *supply chain* pharmaceutique.

## § 2. – La *blockchain*, un outil complémentaire pour sécuriser la chaîne logistique pharmaceutique

L'enjeu principal de la *supply chain* des produits de santé est de rester imperméable à toute contrefaçon ou falsification. La traçabilité des produits de santé est donc primordiale pour protéger efficacement la *supply chain*. La *blockchain* permet de répondre à cet objectif en complétant les finalités poursuivies par la sérialisation et par le système UDI.

La *blockchain* est une technologie permettant de stocker et de partager des informations de manière sécurisée et transparente. Chaque échange d'informations, aussi appelé transaction, est enregistré dans un bloc. Grâce au hachage, ce bloc

(22) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017.
(23) *Unique Device Identification*.
(24) SNITEM, Rapport sur la nouvelle réglementation des dispositifs médicaux, mars 2020, mise à jour en mai 2020.

renferme toutes les informations contenues dans les blocs précédents. Le tout forme alors une chaîne permettant de retracer tout l'historique des échanges d'informations.

Tout l'intérêt de la *blockchain* réside dans le hachage. En effet, un algorithme va créer un *hash* à partir des informations renseignées dans chaque bloc. Chaque bloc est alors associé à une suite de chiffres et de lettres unique. Ainsi, si un bloc est modifié, un nouveau *hash* est généré. Néanmoins, celui-ci ne coïncidera pas avec les blocs suivants. Ceci permet alors d'identifier le bloc modifié dans la *blockchain*. Pour passer inaperçue, la modification d'un bloc suppose de recalculer les *hashs* des blocs suivants et de modifier la copie des nœuds du réseau simultanément, ce qui est très compliqué à mettre en œuvre.

Par ailleurs, la *blockchain* est un système décentralisé et distribué[25] : la *blockchain* fonctionne sans organe central de contrôle. Ainsi, tous les ordinateurs du réseau *blockchain*, appelés nœuds, peuvent distribuer et recevoir des données.

Les *blockchains* peuvent être classées en différentes catégories selon leurs modalités d'accès. En effet, certaines sont publiques, et donc ouvertes à tous. Néanmoins, il existe des *blockchains* de permission, qui se déclinent selon deux modèles. Tout d'abord, les *blockchains* privées sont placées sous le contrôle d'un acteur du réseau *blockchain :* cet acteur est chargé de valider les transactions. Ensuite, les *blockchains* de consortium supposent que les membres de la *blockchain* aient validé la transaction en nombre suffisant pour qu'un bloc soit ajouté à la *blockchain*[26]. Les projets en cours laissent penser que ce dernier modèle a été retenu pour s'appliquer dans le secteur de la santé. Dès lors, cela suppose l'adoption d'un consensus au sein de la *blockchain* pour la validation de nouveaux blocs. En effet, les échanges d'informations s'opèrent entre les nœuds du réseau *blockchain*, sans avoir recours à un serveur central : chaque nœud contient un exemplaire de la *blockchain*. Dès lors, si un nœud du réseau est défaillant, ceci n'empêche pas la *blockchain* de fonctionner.

La *blockchain* n'est pas qu'une technologie et apparaît comme une véritable base de données transparente, infalsifiable et distribuée. Son utilisation permet de s'assurer que les informations échangées n'ont pas été altérées et repose sur la coopération de tous ses utilisateurs. La *blockchain* est alors vectrice de confiance en garantissant à la fois l'origine et l'inaltérabilité de l'information. Elle fonctionne sur le principe de *smart contracts* (données codées) représentant la relation contractuelle, qui ne pourra être modifiée dès lors qu'elle est intégrée dans un bloc, et provoquera une alerte en cas de réalisation d'opérations non conformes aux données contenues dans le *smart contract*. Outre l'agilité et la rapidité, la *blockchain* confère la confiance et la sécurisation des opérations logistiques entre les différents acteurs au niveau international.

Ainsi, la *blockchain* peut être utilisée pour le suivi des produits de santé tout au long de la *supply chain*[27].

(25) *Building value with blockchain technology : how to evaluate blockchain's benefits*, World Economic Forum, 2019.
(26) I. Poirot-Mazères, *Blockchain et santé. Cas d'application et premiers questionnements juridiques*, Séminaire IFERISS-IMH, 12 oct. 2018.
(27) J. Verny, *La* blockchain *au service de l'amélioration de la compétitivité des entreprises et de l'attractivité des territoires. Application à la filière pharmaceutique de la vallée de la Seine : Annales de géographie* 2018/5-6, n$^{os}$ 723-724, p. 492 à 513.

Tout d'abord, la *blockchain* permet de garantir un meilleur contrôle des données de chacun des blocs à chaque étape de la *supply chain*. Par rapport à la sérialisation, ce dispositif comprend plus de données et un accès facilité à celles-ci pour les personnes autorisées, ce qui sécurise davantage la chaîne de production.

En effet, la *blockchain* favorise le partage des données en apportant plus de fluidité et de flexibilité. Si une anomalie apparaît lors de la production ou de la distribution d'un produit de santé, il est très facile d'identifier l'étape défaillante en visualisant l'ensemble des transactions effectuées sur la *blockchain*, sans interrompre la *supply chain*. À titre d'exemple, le transport à température dirigée des produits de santé thermosensibles peut reposer sur la *blockchain*. En effet, les enregistrements de température *via* des capteurs présents dans les véhicules frigorifiques peuvent être automatiquement téléchargés dans le registre de la *blockchain*. Les données enregistrées sont alors immédiatement transmises de manière sécurisée et visible par tous les acteurs de la *supply chain*.

La *blockchain* permet de faciliter la traçabilité et de renforcer la sécurité des produits de santé lors de leur transport et de leur distribution. La *blockchain* constitue de plus un atout réel pour lutter contre la falsification des produits de santé ; puisque celle-ci est hermétique et inaltérable, les produits falsifiés ne peuvent en principe y être intégrés, sauf à ce que la *blockchain* soit constituée dans un objectif illicite, contenu dans la réalisation du *smart contract*.

La *blockchain* a vocation à alléger les process existants en facilitant la gestion et le partage de données, mais ne peut pas fonctionner sans l'intervention manuelle des utilisateurs. Davantage d'autonomie peut être apportée à la *blockchain* grâce à l'utilisation de *smart contracts*. En effet, un *smart contract* désigne un « transfert automatisé de valeurs fondé sur un accord préalable entre deux personnes et qui s'exécute au moyen d'une *blockchain* »[(28)]. Ainsi, un code informatique est inscrit sur la *blockchain* sur la base d'actions définies à l'avance par les parties[(29)]. Dès que toutes les conditions figurant dans le *smart contract* sont réunies, celui-ci s'exécute automatiquement, sans l'intervention d'un tiers de confiance[(30)]. L'intérêt principal des *smart contracts* est que les termes du contrat ne peuvent en aucun cas être altérés. À titre d'exemple, un *smart contract* pourrait être mis en place pour le transport de produits de santé thermosensibles. En effet, grâce aux données enregistrées et téléchargées dans le registre de la *blockchain*, le *smart contract* pourrait générer une alerte et bloquer la livraison en présence d'importantes variations de température, dont les seuils auraient été déterminés au préalable par les parties. Cette procédure de contrôle pourrait s'avérer particulièrement pertinente dans le secteur des vaccins soumis à des exigences de températures strictes tout au long de la chaîne de circulation du produit jusqu'à l'inoculation au patient.

La mise en place de la *blockchain* permet d'assurer une plus grande traçabilité des produits de santé tout au long de la *supply chain*. Mais elle présente

(28) B. Barraud, *Les blockchains et le droit : RLDI* 2018, p. 48-62.
(29) C. Berbain, *La* blockchain *: concepts, technologies, acteurs et usages : Annales des mines – Réalités industrielles* août 2017, p. 6 à 9.
(30) T. Menissier, *Peut-on réinventer technologiquement la confiance ? La* blockchain *ou les ambiguïtés de la transaction dématérialisée*, 2018. – A. Ribeiro, *La* blockchain *est ses potentielles applications*, 2016.

deux faiblesses qui expliquent le peu d'engouement de l'industrie des produits de santé : d'une part, son coût, puisque cela suppose que tous les acteurs impliqués dans la chaîne de production disposent de l'outil numérique et de l'installation nécessaire et, d'autre part, son risque de désuétude par rapport à l'avancée fulgurante des technologies numériques. La *blockchain* risque d'être rapidement dépassée comme technique face notamment à l'arrivée des ordinateurs quantiques à superpuissance de calcul, venant perturber les fondements numériques sur lesquels la *blockchain* est construite. Cette technologie n'est pas la seule à pouvoir apporter plus de productivité et de transparence. L'intelligence artificielle revêt de nombreuses perspectives qui pourraient venir compléter les finalités poursuivies par la *blockchain*.

SECTION 2

## LA *BLOCKCHAIN* ET L'INTELLIGENCE ARTIFICIELLE, DES OUTILS CONVERGENTS POUR OPTIMISER LA PRODUCTION DES PRODUITS DE SANTÉ

La *blockchain* peut permettre de renforcer la fiabilité et la compréhension de l'utilisation de l'intelligence artificielle autonome et d'en contrôler les usages dans l'organisation de la production de produits de santé (§ 1). Néanmoins, bien que la *blockchain* soit une technologie prometteuse, sa mise en place engendre de nouvelles difficultés (§ 2).

### § 1. – La *blockchain*, un renforcement de la confiance accordée à l'intelligence artificielle

L'intelligence artificielle analyse des données d'entrée grâce à un ensemble d'algorithmes et une puissance de calcul considérable afin « de comprendre comment fonctionne la cognition humaine et la reproduire »[(31)]. Grâce à l'analyse répétitive de données et à l'auto-apprentissage, l'intelligence artificielle est capable de modifier son raisonnement afin de s'adapter à son environnement. Les données se trouvent alors au cœur du fonctionnement et de l'entraînement des algorithmes ayant recours à l'intelligence artificielle[(32)]. L'intelligence artificielle se différencie de l'automatisation qui a simplement vocation à exécuter des actions mécaniques préalablement programmées par l'Homme.

Associer la *blockchain* et l'intelligence artificielle n'est pas évident au premier abord. Néanmoins, ces deux technologies sont très complémentaires.

(31) C. Villani, *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, Rapport de la mission parlementaire, mars 2018.

(32) Rapport du Conseil national numérique et de France Stratégie, *Anticiper les impacts économiques et sociaux de l'intelligence artificielle*, mars 2017.

L'intelligence artificielle permet d'analyser l'ensemble des données enregistrées dans le registre de la *blockchain* afin d'effectuer des prévisions précises. Appliquée à la production des produits de santé, l'intelligence artificielle permet déjà d'optimiser la gestion des stocks et anticiper la fabrication de médicaments afin d'éviter toute rupture d'approvisionnement et de distribution. En effet, l'intelligence artificielle s'appuie sur les données relatives aux prévisions de ventes et de planification et les combine avec les données portant sur le stock des officines et celles issues de la logistique. La combinaison de l'ensemble de ces données, renseignées dans la *blockchain*, permet d'avoir une visibilité en temps réel des stocks et des médicaments produits afin que l'intelligence artificielle émette des prévisions de commandes adaptées à la demande(33). Cela permet d'anticiper et de prévenir les tensions d'approvisionnement et ruptures de stock.

Ainsi, la mise en place de la *blockchain* et de l'intelligence artificielle est particulièrement intéressante dans les pays où il n'existe pas de système de suivi tel que celui mis en place par l'assurance maladie et les autorités de santé en France. À cet égard, les États-Unis ont mis en place un système électronique interopérable afin de sécuriser la chaîne d'approvisionnement en médicaments(34).

L'intelligence artificielle pourrait améliorer le fonctionnement de la *blockchain*. En effet, le traitement de blocs de données requiert une puissance de calcul très importante. De plus, tous les nœuds du réseau contiennent une copie de l'ensemble de la *blockchain*. La *blockchain* pourrait rapidement atteindre ses limites, la puissance de calcul étant insuffisante pour traiter l'ensemble des données enregistrées dans le réseau. L'intelligence artificielle pourrait augmenter la performance de la *blockchain* en optimisant le stockage de données grâce à la technique du *sharding*(35). Cette technique consiste à fragmenter les données afin de faciliter le traitement et la gestion de l'information. Dès lors, une même *blockchain* pourrait être divisée en plusieurs sous-*blockchains*. Ainsi, seuls certains nœuds du réseau conserveraient une copie intégrale de la *blockchain*, permettant alors aux autres nœuds de stocker un nombre limité de données. L'intelligence artificielle serait chargée de répartir le stockage des données entre les différents nœuds du réseau *blockchain*. Ceci permettrait de réduire les besoins en puissance informatique des réseaux *blockchain*. L'interaction est alors un moyen de résoudre en partie la difficulté de l'obsolescence de la *blockchain*.

Par ailleurs, la *blockchain* pourrait apporter plus de lisibilité aux processus décisionnels de l'intelligence artificielle. En effet, il est assez difficile de comprendre comment l'intelligence artificielle exploite les données d'entrée avant de prendre une décision(36). Cette opacité pourrait être amoindrie grâce à la *blockchain*.

(33) *Building value with blockchain technology : how to evaluate blockchain's benefits : World Economic Forum* 2019.
(34) *Drug Supply Chain Security Act*, 2013. FDA takes new steps to adopt more modern technologies for improving the security of the drug supply chain through innovations that improve tracking and tracing of medicines, févr. 2019 (www.fda.gov/news-events/press-announcements/fda-takes-new-steps-adopt-more-modern-technologies-improving-security-drug-supply-chain-through).
(35) M. El Malki *Modélisation NoSQL des entrepôts de données multidimensionnelles massives*, thèse, Université de Toulouse, 2016.
(36) HAS, Rapport d'analyse prospective, *Numérique : quelle (R)évolution ?*, 2019.

Si l'intelligence artificielle s'appuie sur les données enregistrées dans une *blockchain*, une piste d'audit apparaît très clairement, permettant à l'Homme de connaître la combinaison de blocs, et donc d'informations, ayant abouti à la prise de décision. Grâce à la *blockchain*, les données prises en compte par l'intelligence artificielle sont immuables et infalsifiables, ce qui permet de donner de la valeur à la prise de décision opérée par l'intelligence artificielle. Il serait donc possible de contrôler la construction de l'intelligence artificielle et l'analyse des informations stockées dans la *blockchain*.

L'intelligence artificielle apporte plus d'agilité aux entreprises pharmaceutiques, en offrant une visibilité de bout en bout de la *supply chain* en temps réel. L'intelligence artificielle et la *blockchain* offrent de nouvelles perspectives pour la lutte contre la falsification des produits de santé. En effet, alors que la *blockchain* permet d'enregistrer la provenance géographique des matières premières, l'intelligence artificielle peut se servir de cette donnée afin d'identifier l'existence d'un risque de défaut de qualité. Ainsi, l'association de la *blockchain* et de l'intelligence artificielle permet aux industries pharmaceutiques de concentrer leurs contrôles sur les points critiques identifiés par l'intelligence artificielle.

L'association de la *blockchain* et de l'intelligence artificielle peut être le remède au manque de confiance et de transparence reproché aux laboratoires pharmaceutiques, qui s'explique principalement par les différents scandales sanitaires qui ont touché la France ces dernières années. L'approche prédictive de l'intelligence artificielle et la confidentialité assurée grâce à la *blockchain* permettent aux industries de la santé de rationaliser et d'optimiser les processus de fabrication et de production, dans la perspective d'une médecine « 6P » qui change les paradigmes en santé. Elle permet de s'adapter aux besoins de prévisibilité, prédictibilité dans la production des produits de santé, afin d'éviter les crises telles que celles rencontrées pendant la phase Covid-19. Elle permet aussi d'assurer la confidentialité, la sécurisation et la traçabilité des opérations, dans un contexte d'augmentation des risques concernant la sécurité des produits. Elle permet enfin de s'adapter à l'évolution des productions sur différents territoires.

Mais cette utilisation reste confrontée à de nombreux défis, qu'elle doit surmonter avant de s'imposer comme une solution efficace.

## § 2. – Les défis de la *blockchain*

L'implémentation de la technologie *blockchain* dans le domaine de la santé apporterait une solution à la problématique de la traçabilité des produits pharmaceutiques, offrant ainsi une protection renforcée en matière de production. La complexité technique de cette technologie pourrait également représenter une solution en matière de lutte contre le piratage des circuits d'approvisionnement et le vol des données de santé.

Cependant, la mise en place opérationnelle de la *blockchain* soulève certaines problématiques à la fois juridiques, éthiques et techniques, qu'il convient d'étudier de manière approfondie.

Sur le plan juridique, la *blockchain* a une valeur légale qui lui a été attribuée par l'ordonnance du 28 avril 2016 introduisant la notion de minibons[37]. En théorie, les règles de droit commun régissent la technologie *blockchain*, notamment le droit des obligations, le droit de la santé, le droit de la propriété intellectuelle, le droit du numérique et également les règles relatives à la protection des données personnelles[38]. En pratique, l'application du droit positif à la *blockchain* peut soulever certaines questions.

L'utilisation de *smart contract* dans la *blockchain* peut être assez délicate au regard du droit des contrats français. Le *smart contract* est seulement une technologie de transfert. Il est donc nécessaire que celui-ci soit en amont relié à un contrat possédant une valeur juridique[39]. Le *smart contract* ne se suffit pas à lui-même. Cette modalité a par ailleurs été précisée dans l'étude réalisée par le Conseil d'État en 2017[40]. À ce sujet, le Conseil a indiqué que le *smart contract* pouvait permettre un versement automatique des fonds, à partir du moment où les conditions prévues dans le contrat initial sont remplies. Il reste cependant à déterminer le régime de responsabilité applicable en cas de problèmes liés à la *blockchain* affectant le *smart contract*[41]. De plus, dans le rapport du Conseil d'État de 2017, certains questionnements sont soulevés en matière de contrôle de la *blockchain* par les autorités étatiques, notamment en ce qui concerne le contentieux pouvant résulter des *smart contracts*. Avec la *blockchain*, il est en effet délicat de vérifier que l'utilisateur réalisant la transaction est bien agréé à la réaliser en vertu du contrat. En d'autres mots, il peut être épineux de vérifier que l'identité numérique de la personne agissant sur la *blockchain* correspond bien à son identité physique[42]. Ensuite, la rapidité et l'automatisation des opérations *via* la *blockchain* peuvent en effet apporter une plus grande performance dans les échanges entre les parties. Cependant, les autorités ne pourront pas, en l'état actuel des choses, être aussi rapides que les algorithmes de la *blockchain*. Ceci pourrait s'avérer problématique dans le cas où une opération serait amenée à être bloquée sur décision de justice par exemple. Il se pose donc la question du remaniement du système actuel afin que celui-ci puisse s'adapter et être effectif pour répondre aux problématiques de la *blockchain*. Cette mise en œuvre pourrait s'avérer relativement complexe. Il ne sera pas toujours possible de contrôler la volonté illicite des acteurs impliqués dans la *blockchain*[43], et la réponse juridique à apporter à ces usages de l'outil numérique est complexe. Certains risques, comme ceux relevant de l'« obfuscation », c'est-à-dire la publication intentionnelle d'informations fausses, sans possibilité évidente d'effacement, sont à prendre en considération.

(37) J. Verny, *La* blockchain *au service de l'amélioration de la compétitivité des entreprises et de l'attractivité des territoires. Application à la filière pharmaceutique de la vallée de la Seine : Annales de géographie* 2018/5-6, n^os^ 723-724, p. 492 à 513.
(38) I. Poirot-Mazères, Blockchain *et santé. Cas d'application et premiers questionnements juridiques*, Séminaire IFERISS-IMH, 12 oct. 2018.
(39) *Ibid*.
(40) CE, *Étude annuelle 2017. Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, Paris, pub. CE, 2017, 190 p.
(41) J. Verny, *La* blockchain *au service de l'amélioration de la compétitivité des entreprises et de l'attractivité des territoires. Application à la filière pharmaceutique de la vallée de la Seine : Annales de géographie* 2018/5-6, n^os^ 723-724, p. 492 à 513.
(42) *Ibid*.
(43) *Comprendre les* blockchains *: fonctionnement et enjeux de ces nouvelles technologies*, Rapp. Sénat n° 584 (2017-2018) de M^me^ V. Faure-Muntian et MM. C. de Ganay et R. Le Gleut, fait au nom de l'OPECST, déposé le 20 juin 2018.

Parmi les problèmes juridiques que pose plus spécifiquement le développement de la *blockchain*, il convient de noter le risque de faciliter l'organisation du crime organisé, de favoriser la circulation des produits contrefaits pharmaceutiques, mais aussi le risque de diffuser des contenus illicites. Au niveau international, les États recherchent des solutions concernant l'organisation d'un régime de responsabilité des acteurs. Plusieurs propositions ont été avancées, notamment en vue de sécuriser les *blockchains* publiques financières. Dans le domaine de la *blockchain* privée, les failles juridiques semblent pouvoir être résolues par des solutions techniques, toutes cependant supposent une forme de transparence de la *blockchain* et de connaissance des utilisateurs. Or, cette transparence semble en contradiction totale avec les solutions techniques apportées à la question de la protection des données personnelles. Il s'agit alors, afin de répondre à ces inquiétudes, de trouver une solution permettant d'assurer une sécurisation des contrats sans en révéler le contenu, et donc de sécuriser les produits sans révéler les caractéristiques des contrats unissant les parties. L'analyse des failles doit conduire à décortiquer l'organisation du circuit et des dispositions strictement confidentielles afin d'en assurer la protection tout en garantissant la traçabilité et la conformité des opérations.

La *blockchain* contient énormément de données parmi lesquelles se trouveront forcément des données personnelles. Il faudra donc s'assurer de la conformité de cette technologie au RGPD[(44)] et aux autres lois en matière de protection des données personnelles, notamment la loi Informatique et Libertés[(45)]. Si la *blockchain* est mise en place au niveau de la *supply chain* dans le secteur pharmaceutique, elle peut dans ce cas l'être également dans la phase de recherche, d'essais cliniques, dans le processus de remontée des cas relevant de la pharmacovigilance, *etc.* Cela permet par ailleurs de compléter le processus de sérialisation actuel qui prend fin lors de la dispensation du produit.

La *blockchain* a l'avantage d'être composée de blocs cloisonnés, ainsi cela rend facilement applicable le principe de minimisation des données imposé par le RGPD. La CNIL distingue trois types d'acteurs intervenant dans la *blockchain* au niveau des données personnelles : les « accédants », les « participants » et les « mineurs ». En fonction du type d'acteur, les droits sur la *blockchain* sont différents. Les « accédants » ont un droit de lecture et peuvent obtenir une copie de la chaîne. Les « participants » peuvent ajouter des éléments, ils ont un droit d'écriture soumis à validation. Cette validation est effectuée par les « mineurs » qui créent ensuite les différents blocs de la chaîne[(46)]. Tous les acteurs intervenants sur la *blockchain* n'ont donc pas les mêmes droits d'accès aux données, ni les mêmes pouvoirs de modification. Ainsi, l'implémentation de la *blockchain* dans la chaîne pharmaceutique permet de s'assurer que seules les personnes autorisées puissent accéder, modifier ou valider un bloc et d'identifier les données enregistrées par chaque acteur. Dans le cas de la *supply chain*, les données qui sont contenues dans des blocs lui étant dédiés ne peuvent contenir de données de santé, comme ce sera le cas pour les

(44) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 2016.
(45) L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés.
(46) CNIL, Blockchain *et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ?*, 24 sept. 2018.

essais cliniques. Cependant des données personnelles sont tout de même présentes dans ces blocs, comme l'identité du fournisseur, du transporteur, l'immatriculation et le *tracking* du véhicule de transport, *etc.*

Du point de vue du RGPD, il convient donc de s'assurer du respect des principes généraux relatifs aux traitements des données, notamment s'assurer de la licéité, de la transparence, de la sécurité, de la limitation des finalités, de la détermination des durées de conservation et de la loyauté des traitements(47). De nombreuses autres questions se posent sur la manière de garantir aux personnes concernées l'accès, la modification et la suppression de leurs données. L'avantage de la *blockchain* réside dans la difficulté de modifier ou supprimer une information une fois celle-ci entrée dans un bloc. De ce fait, est-il possible de répondre de manière effective et efficace aux demandes d'exercice de droits des personnes ? En effet, l'un des principaux avantages de la *blockchain* réside dans son immuabilité, mais cela peut s'avérer être un obstacle lorsqu'il s'agit de faire application du droit à l'oubli prévu par le RGPD. Il existe une solution qui consiste à ajouter une nouvelle transaction au sein d'un bloc. Cette technique permet de rectifier une donnée déjà présente et par conséquent de modifier ou de supprimer des données personnelles(48). Une seconde option réside dans l'anonymisation des données personnelles au sein de la *blockchain* dès l'inscription de celles-ci dans les blocs. Cependant, en matière probatoire, cette solution risque de poser certaines difficultés.

Le sujet du transfert des données en dehors de l'Union européenne est également important, au titre du RGPD. Le transfert des données ne pourra se faire que dans des conditions définies et nécessite la mise en place de mesures particulières, lorsque le transfert a lieu vers un pays qui n'est pas reconnu comme équivalent par la Commission européenne. Or, le marché pharmaceutique est international, de nombreux échanges ont lieu entre les pays et les continents. De manière globale, la question qui se pose est celle de l'homogénéisation des règles de droit et de l'encadrement juridique de la *blockchain*. En l'espèce, quel sera le droit applicable, quelle juridiction sera compétente alors que les blocs seront probablement dispersés à travers le monde ? Il conviendra de s'adapter aux règles du droit international privé et de faire le choix des juridictions compétentes dans les conventions en amont de la création d'un bloc.

Sur le sujet de la *blockchain*, la question de l'homogénéisation ne se pose pas qu'en termes de législations applicables. En effet, elle se pose également de manière effective dans la mise en place même de la *blockchain*. Pour que cette technologie soit efficace et rentable, il convient que les acteurs de la filière pharmaceutique fassent majoritairement usage de la *blockchain*. Il est difficile pour le moment d'imaginer tous les industriels se doter de la *blockchain* au niveau mondial. Le risque est que les entreprises qui ne s'approprient pas cette technologie perdent en compétitivité et en parts de marché(49). Les entreprises qui feront le choix de la *blockchain*

(47) G. Chassang et J. Béranger, *La* blockchain *pour la recherche en santé ? Potentiels, enjeux juridique et éthique.* Blockchain *et Santé : Perspectives d'applications et enjeux juridiques*, France, Toulouse, Séminaire IFERISS, oct. 2018.

(48) H. Gabadou et J. Camilleri, *La technologie* Blockchain *à l'heure du RGPD ; conforme ou incompatible*, blog Business de Deloitte, 13 déc. 2019.

(49) J. Verny, *La* blockchain *au service de l'amélioration de la compétitivité des entreprises et de l'attractivité des territoires. Application à la filière pharmaceutique de la vallée de la Seine : Annales de géographie* 2018/5-6, nos 723-724, p. 492 à 513.

finiront par former un réseau hermétique duquel seront exclues celles qui n'utiliseront pas cette technologie[50]. Cette technique deviendrait alors en elle-même un outil concurrentiel très efficace. La qualification d'une entente entre les acteurs de la *blockchain* pourrait alors permettre la sanction des pratiques, par l'objet.

Un des principaux défis de la *blockchain* est justement de mobiliser le plus d'entreprises afin que celle-ci soit efficace. Mais, en pratique, l'usage de la *blockchain* nécessite la mise en place d'un modèle collaboratif qui est difficile à mettre en œuvre dans un secteur aussi concurrentiel et réglementé.

La mise en place de la *blockchain* constitue un véritable bouleversement des pratiques actuelles, qui est majoritairement inhérent au fait qu'elle fonctionne sans autorité de contrôle. De ce fait, par son usage, l'intervention de tiers de confiance est fortement réduite. En effet, la traçabilité offerte par la *blockchain* assure que le produit fabriqué sera bien le produit reçu. Le besoin de vérification par un tiers des transactions afin d'assurer la confiance entre tous les acteurs de la chaîne sera donc moindre[51]. Cette pratique offre un gain de temps considérable du fait de la réduction des intermédiaires qui supprime certains délais de traitement et également un allégement des coûts supportés par la *supply chain*. Autre avantage de la *blockchain*, l'utilisation de cette technologie peut permettre de valoriser et de réinstaurer la coopération au niveau local. La mise en place de la *blockchain* à une échelle réduite est plus aisée à imaginer. L'un des principaux obstacles à la mise en place de la *blockchain* de manière efficace réside dans le fait que cela nécessite une refonte du système actuel tant sur le plan des relations entrepreneuriales, que sur le modèle économique, bancaire et coopératif. De plus, la mise en œuvre de départ de la *blockchain* reste très onéreuse et elle ne peut donc pas être mise en place de manière effective de manière homogène.

Il convient enfin de souligner que le développement de la *blockchain* peut avoir un impact environnemental important[52], difficile à appréhender pour le moment. Cette technologie est très énergivore, les algorithmes utilisés pour garantir son fonctionnement nécessitent un nombre de calculs très important et le stockage l'est tout autant[53]. Bien que la *blockchain* soit une technologie se vantant de rapidité, le temps nécessaire à la prise en compte d'une transaction n'est pas instantané et peut aller de quelques minutes à plusieurs heures. Ainsi, comment assurer une mise à jour directe et continue des différentes étapes[54] ? Enfin, la *blockchain* est réputée infalsifiable et inviolable, mais qu'en est-il lorsque les données entrées sont falsifiées, et ce dès le début de la chaîne ? Le principal avantage à la mise en place de la *blockchain* serait alors caduc. Une solution pour contrer ce problème est d'accentuer la vérification par plusieurs personnes responsables tout au long de la chaîne, qui se chargent d'assurer la véracité et la qualité des données entrées dans chaque bloc.

(50) *Ibid.*
(51) J. Verny, *La* blockchain *au service de l'amélioration de la compétitivité des entreprises et de l'attractivité des territoires. Application à la filière pharmaceutique de la vallée de la Seine : Annales de géographie* 2018/5-6, nos 723-724, p. 492 à 513.
(52) *Les enjeux technologiques des* blockchains *(chaînes de blocs)*, Rapp. Sénat n° 584, au nom de l'OPECST, par V. Faure-Muntian, C. de Ganay et R. Le Gleut.
(53) M. Ahmed Mohamed, C. Taconet et M. Ould Mohamed Lemine, *La traçabilité dans les chaînes logistiques en utilisant l'IOT et la* Blockchain*. Évolution des SI : vers des SI Pervasifs ?*, Paris, France, Université Paris 1 Panthéon-Sorbonne, juin 2019, p. 1-10.
(54) *Ibid.*

Ces critères sont donc à analyser et à prendre en compte, en cas d'implémentation de la *blockchain* dans la *supply chain*. Concrètement, cette technologie peut offrir aux industriels et aux acteurs du monde de la santé une solution de performance et de traçabilité non négligeable. Cependant, sa mise en place nécessite de repenser certaines règles de manière collective, et une coopération importante entre acteurs et entre pays est nécessaire.

## CONCLUSION

Le numérique va inévitablement continuer à se développer dans le domaine de la santé et notamment dans la *supply chain* au cours des prochaines années. Si la sérialisation limite certains risques de falsifications, elle n'est plus suffisamment optimale et ne protège pas de nombreux produits. La *blockchain* et l'intelligence artificielle permettent d'optimiser de manière considérable la *supply chain*. Ces nouvelles technologies offrent de nombreux avantages. Elles permettent de lutter de manière plus efficace contre la criminalité qui touche le secteur de la santé, d'apporter plus de transparence, une plus grande fiabilité des produits, un meilleur traçage, de prévenir les ruptures de stock et de favoriser un meilleur rendement. Néanmoins, certaines limites doivent être prises en compte, notamment l'adaptation des législations à ces nouvelles technologies, les coûts de mise en place, ou encore la nécessité d'une coopération et d'une homogénéisation des pratiques à grande échelle. L'implémentation de la *blockchain* engendre un vrai bouleversement des pratiques de travail des acteurs de la *supply chain*. En conséquence, il est nécessaire d'accompagner financièrement et techniquement toutes les parties prenantes dans la transformation digitale de la *supply chain* afin de révolutionner le partage et le stockage des données. Le programme *EU4Health* est une voie permettant aux entreprises d'optimiser leur circuit logistique, afin notamment d'en assurer la localisation prioritaire et sécurisée sur le territoire de l'UE.

CHAPITRE 6

# L'INTELLIGENCE ARTIFICIELLE ET LA *BLOCKCHAIN* AU SERVICE DE LA SÉCURISATION LOGISTIQUE DES PRODUITS DANS LE SECTEUR PHARMACEUTIQUE

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Pierre MORGON

La *supply chain*, ou management logistique, est une phase spécifique et capitale dans la mise sur le marché des produits pharmaceutiques dans les meilleures conditions de sécurité pour le patient, et dans les meilleures conditions économiques pour le laboratoire qui va rationaliser et optimiser son mode de production et de distribution au niveau international. Dans la plupart des cas, les laboratoires pharmaceutiques sous-traitent les questions de logistique auprès des grossistes et distributeurs spécialisés, qui possèdent l'infrastructure, les procédures et le personnel nécessaires à la réalisation de ces activités dans le respect de la réglementation pharmaceutique. Dans des situations spécifiques ou exceptionnelles, les laboratoires pharmaceutiques interviennent directement dans la gestion de la chaîne logistique, notamment en cas de produits nécessitant des conditions très spécifiques de stockage et de transport, ou en période de pandémie, comme actuellement pour ce qui concerne la distribution des vaccins.

La rationalisation de cette organisation – depuis la fabrication jusqu'à la distribution – est particulièrement importante en période de crise sanitaire, et la pandémie de Covid-19 a malheureusement démontré toutes les limites existantes liées à une organisation extrêmement dépendante des pays asiatiques, et notamment de l'Inde et de la Chine, où la fabrication de nombreux principes actifs a été délocalisée depuis de nombreuses années, pour des raisons économiques. Au-delà des contraintes techniques d'acheminement des produits, c'est aussi toute la

question de la sécurisation de la fourniture des produits et de leur traçabilité qui est en cause[1]. La pandémie de Covid-19 a mis en évidence l'extrême vulnérabilité des circuits d'approvisionnement de certains principes actifs et matières premières (articles de conditionnement, réactifs destinés au contrôle de qualité), conduisant le monde politique au constat d'une nécessaire relocalisation de la production de ces produits et matières dans les pays occidentaux. En parallèle, la pandémie a souligné les limites du modèle d'implantation industrielle reposant sur un petit nombre d'usines ayant une capacité importante. Les limitations en matière de capacité et de gestion de pics de demande poussent à explorer un modèle d'implantation différent, et plusieurs initiatives visent à multiplier les sites de production ayant une capacité plus modeste dans les pays émergents, mais en étant implantés plus près des bassins de population.

Avec la multiplication des sites de production, et de sous-traitance, le recours à de nouvelles technologies permettant de gagner en rapidité, en traçabilité et en sécurisation dans la circulation du produit depuis le fabricant de principes actifs ou de matières premières jusqu'à la mise sur le marché ou mise en service du produit au profit du patient-consommateur ou de l'utilisateur, est devenu une priorité[2]. L'adaptation en urgence et avec agilité à ces nouveaux process est fondamentale dans le secteur des produits de santé[3], et sera déterminante pour l'avenir de ce secteur, dans un contexte sanitaire chaotique frappé par les risques de piratage et de cybercriminalité. Dans le contexte de la pandémie de Covid-19, les vaccins ne sont pas encore produits en quantités suffisantes pour répondre à la demande, ce qui crée une opportunité pour des trafiquants et des spéculateurs malfaisants qui vendent des vaccins contrefaits. Les solutions de type RFID (Radio Fréquence Identification) sont déployées par les fabricants pour prévenir ce type de risque. Mais il importe que tous les acteurs de la chaîne de distribution soient également vigilants, avec des procédures de contrôle très rigoureuses, afin de ne créer aucune faille qui pourrait être exploitée par les trafiquants. De fait, les produits contrefaits sont le plus souvent détectés dans les pays émergents, où les moyens et procédures de contrôle ne sont pas aussi performants que dans les pays développés.

L'activité des laboratoires pharmaceutiques est soumise à une forte réglementation fondée sur la nécessité d'assurer la sécurité des patients, un enjeu majeur. La production de produits pharmaceutiques, de plus en plus complexes et notamment biotechnologiques, suppose de nombreuses étapes au cours desquelles interviennent différents acteurs situés au niveau international. Ceci explique le recours à une réglementation pharmaceutique européenne extrêmement rigoureuse (Section 1).

Cette organisation suppose d'assurer la sécurité, la traçabilité, la rapidité, la transparence chez tous les opérateurs impliqués dans la chaîne de vie des produits en tenant compte des diversités de réglementations nationales, sources de risques

(1) V. Rabassa, *Pandémie de la Covid-19 et* supply *chains mondiales : repenser une stratégie de gestion de crise*, Outre-Terre, 2019, vol. 57, n° 2, p. 47-54.

(2) B. Espesson-Vergeat, *Impact de la pandémie sur la gestion internationale de produits de santé, entre pénurie et innovation : Droit, Santé et Société* 2020, n° 2, p. 77 à 92 (cairn.info).

(3) M.-N. Sinapin, *L'agilité n'est plus un slogan : enquêtes exploratoires et étude du cas Sanofi en temps de crise du Covid-19 : l'agilité est-elle un slogan ? : Cahiers Risques et Résilience*, L'Harmattan, à paraître.

face auxquels l'encadrement normatif européen présente toutefois des faiblesses. C'est donc dans une approche de prudence et de précaution que s'organise la réponse de l'industrie pharmaceutique face aux risques que présente cette activité.

L'intérêt d'avoir un recours couplé à l'intelligence artificielle, la puce RFID, et la *blockchain* (« outils numériques ») dans la *supply chain* pharmaceutique réside dans la nécessité de protéger l'entreprise et le consommateur contre, d'une part, la perte ou la fuite des données recueillies tout au long du circuit du produit, mais aussi d'assurer la protection des patients et utilisateurs contre le fléau de la falsification des produits et la criminalité visant à introduire sur le marché des produits contrefaits. Le recours à ces « outils numériques » répond aux exigences économiques et concurrentielles, ainsi qu'aux enjeux de protection de la santé publique dans la circulation internationale de ces produits spécifiques.

Le recours à ces « outils numériques » fondés sur l'exploitation des données, sur le principe d'autoapprentissage de la machine ou *machine learning*, vient compléter le dispositif réglementaire rigoureux existant dans le secteur pharmaceutique. L'exploitation de ces outils tout au long du cycle de vie du produit, depuis l'identification et le suivi des matières premières, articles de conditionnement et réactifs pour le contrôle de qualité, jusqu'à la traçabilité du produit tout au long de sa distribution jusqu'au patient, exige un aménagement de l'encadrement juridique et réglementaire dans une approche agile du droit conditionnée par la vitesse d'évolution scientifique et technologique.

Si le recours aux « outils numériques » est déjà très présent dans la phase de recherche et développement ou dans la phase finale de marketing et suivi du produit sur le marché, en revanche l'apport de ces outils dans le secteur de la *supply chain* est plus récent et suppose un investissement économique massif pour mettre en place les outils et procédures de suivi et de contrôle, une compatibilité des « outils » sur le terrain international, et un encadrement juridique des procédures. Toutefois, les enjeux économiques et de santé publique poussent l'industrie à intégrer massivement ces avancées technologiques dans les process de suivi et surveillance des produits. De ce fait, on constate d'ores et déjà un décalage technologique grandissant entre les moyens mis en place par les laboratoires pharmaceutiques et ceux déployés par les instances administratives en charge de la surveillance dans les pays, notamment les pays émergents.

Confrontée à l'évolution technologique et scientifique dans le domaine numérique, à la complexification des produits de santé, et aux exigences de surveillance d'un marché contre les risques de falsification, contrefaçons, ruptures de stocks, dont les conséquences peuvent être sévères en termes de santé publique pour les patients victimes, l'industrie s'engage activement dans l'implémentation des outils numériques dans son organisation (Section 2). Dans ce contexte, le recours aux « outils numériques » permet de renforcer, organiser, prévenir les risques identifiés et offre une solution dont l'encadrement juridique reste à préciser. Par ailleurs, l'écart technologique entre les solutions proposées par l'industrie pharmaceutique et les moyens déployés par les autorités de santé publique de certains pays soulève la question de la responsabilité de chacun des acteurs en cas de contrefaçon ou de falsification de produits pharmaceutiques entraînant des dommages pour des patients.

SECTION 1

# L'ENCADREMENT RÉGLEMENTAIRE DE LA PRODUCTION DES MÉDICAMENTS ET DES RISQUES LIÉS À LA SÉCURITÉ ET AUX STOCKS

La production regroupe l'ensemble des opérations de transformation des matières premières en produits finis. Elle répond à des normes de qualité nationales, européennes et internationales très strictes, et garantit le respect de l'hygiène, de l'environnement et de la sécurité du produit.

La mise sur le marché et la commercialisation d'un produit de santé suivent un processus très réglementé au plan européen et international. L'objectif visé réside dans la maîtrise et la surveillance des fournisseurs de matières premières à usage pharmaceutique et des produits et réactifs destinés au contrôle de qualité, des sous-traitants, façonniers, exploitants, par le fabricant jusqu'au contrôle de qualité final et à la mise sur le marché du produit, et sa distribution depuis le site de production jusqu'à l'utilisateur final.

En conséquence, les fabricants de matières premières pharmaceutiques, destinées aux produits princeps comme aux produits génériques doivent, pour pouvoir percer le marché européen, présenter les mêmes garanties de sécurité, de reproductibilité et de niveaux de contrôle de qualité. La procédure de contrôle des matières premières à l'entrée sur le territoire européen, et lors de la circulation au sein de l'Union européenne, est strictement encadrée, en droit dérivé par la réglementation applicable aux médicaments, ou aux produits de santé autres, par la réglementation douanière et par les principes fondamentaux énoncés dans le Traité sur le fonctionnement de l'Union européenne (TFUE). Lorsque le produit est destiné à plusieurs usages, il convient d'ajouter la possibilité de contrôle par les autorités européennes compétentes dans le secteur des produits chimiques et alimentaires et par les autorités nationales. Cela conduit le fabricant à intégrer, vis-à-vis de son fournisseur, un millefeuille réglementaire national, européen, international et à exiger l'adhérence sans faille à l'ensemble des exigences de qualité.

La production par les industries de santé est donc le premier maillon de la chaîne de vie du médicament et suppose de prévoir une architecture contractuelle avec tous les acteurs impliqués, la responsabilité finale reposant sur le fabricant[4]. Les bonnes pratiques de fabrication donnent pour les médicaments, comme pour les autres types de produits, un guide que suivent les fabricants afin de rester en conformité avec les dispositions européennes[5].

Toutefois, en dépit de cette réglementation, le Parlement et le Conseil de l'Union européenne reconnaissent que « la falsification des médicaments est un problème

(4) LEEM, *Repères sur la production pharmaceutique*, janv. 2018.

(5) Dir. 2001/82/CE. – PE et Cons. UE, dir. 2001/83/CE, 6 nov. 2001, mod. par Dir. 2011/62/UE, instituant un code communautaire relatif aux médicaments à usage vétérinaire et un code communautaire relatif aux médicaments à usage humain, ensemble le guide des bonnes pratiques de fabrication publié par la Commission européenne. – Comm. CE, dir. 2003/94/CE, 8 oct. 2003, établissant les principes et lignes directrices de fabrication concernant les médicaments à usage humain et les médicaments expérimentaux à usage humain et notamment C. santé publ., art. L. 5121-5, L. 5124-1, L. 5138-1, L. 5138-3, R. 5124-1 et R. 5138-1 et s.

mondial qui appelle une coordination et une coopération internationales ». C'est pourquoi a été adoptée en 2011 la directive européenne « Médicaments falsifiés »[6]. Elle définit pour la première fois les médicaments falsifiés. Elle améliore ainsi la qualité des vérifications, de la détection, de la traçabilité et des contrôles sur la chaîne de production. Ceci est réalisé par l'obligation de mettre en œuvre des dispositifs de sécurité et d'inviolabilité des emballages extérieurs.

Malgré une forte réglementation pour encadrer la production des médicaments, les industries de santé connaissent parfois des failles, telles que la rupture des stocks dont les causes sont multiples. Il peut s'agir de la rupture d'approvisionnement d'une matière première, d'un réactif, d'un consommable de production (par ex., une résine de chromatographie) ou d'un article de conditionnement (par ex., les flacons pour les vaccins), ou d'une défaillance technique conduisant à un problème de qualité (les lots échouent les contrôles de qualité), ou enfin d'une mauvaise anticipation de la part des acheteurs et/ou d'une augmentation imprévue de la demande pour des produits qui ont des temps de cycle industriel très longs (notamment pour les produits biologiques en général et les vaccins en particulier).

Adopté fin 2015, le règlement sur la sérialisation[7] complète la directive 2011/62/EU sur les médicaments falsifiés et fixe les dispositifs de sécurité qui doivent figurer sur l'emballage des médicaments afin de lutter contre la contrefaçon.

Afin de garantir la qualité des médicaments, la directive européenne 2011/62/UE a imposé un régime d'autorisation aux fabricants, importateurs et distributeurs de substances actives dans l'Union européenne et une base de données « Eudra GMP » qui répertorie les sites de production validés.

Au niveau international, la *Convention internationale Médicrime*[8] incrimine les fabricants et distributeurs de produits médicaux contrefaits et les infractions similaires[9]. Adoptée par le Comité des Ministres du Conseil de l'Europe[10], cet instrument juridique contraignant dans le domaine du droit pénal criminalise la contrefaçon, mais aussi la fabrication et la distribution de produits médicaux mis sur le marché sans autorisation ou en violation des normes de sécurité. La convention prévoit l'application de sanctions dissuasives pour punir le trafic de faux produits médicaux menaçant la santé publique et dont la diffusion massive par Internet constitue une circonstance aggravante. L'OMS est également un acteur déterminant dans la lutte contre les produits falsifiés. Depuis plusieurs années, des actions internationales de grande ampleur, telles que les opérations PANGEA, sont menées régulièrement pour lutter notamment contre la vente illicite de médicaments par Internet.

La question de la sécurisation des médicaments s'accroît avec les risques de ruptures de stock et tensions d'approvisionnement, largement conditionnés aux

(6) Dir. *Falsified Medicines Directive* 2011/62/UE, modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain.

(7) Comm. UE, règl. délégué n° 2016/161, 2 oct. 2015, complétant la directive 2001/83/CE du PE et du Conseil en fixant les modalités des dispositifs de sécurité figurant sur l'emballage des médicaments à usage humain.

(8) Cons. UE, Convention sur la contrefaçon des produits médicaux et les infractions similaires menaçant la santé publique, entrée en vigueur le 1er janvier 2016.

(9) Complicité, tentative, fabrication, stockage, trafic et offre à la vente de produits médicaux en s'affranchissant délibérément des autorisations et contrôles officiels obligatoires.

(10) Comité des Ministres du Cons. UE, Convention sur la Médicrime adoptée le 8 décembre 2010 et entrée en vigueur en janvier 2016.

massives délocalisations de l'industrie pharmaceutique en Asie, ainsi qu'à la rationalisation des implantations industrielles conduisant à un petit nombre d'usines de grande capacité représentant autant de goulets d'étranglement, et créant une excessive dépendance économique et sanitaire. La dramatique pandémie de Covid-19 concrétise toutes les faiblesses du secteur pharmaceutique et pousse l'Union européenne et les États membres à instaurer un système législatif et réglementaire visant la relocalisation des activités dans les territoires européens.

Afin de pouvoir mieux coordonner leurs efforts dans la prévention et la gestion des tensions d'approvisionnement, les États membres de l'Union européenne devraient s'accorder sur une stratégie concertée encourageant la relocalisation en Europe des sites de production tant des substances pharmaceutiques actives que des produits finis pour des médicaments identifiés comme indispensables à la sécurité sanitaire du continent. Cette relocalisation devrait viser les produits les plus sensibles (médicaments essentiels ou d'intérêt thérapeutique majeur et médicaments et substances pharmaceutiques actives stratégiques pour la sécurité sanitaire européenne). La mise en œuvre de ces procédures suppose le recours aux techniques industrielles et aux technologies numériques innovantes permettant la simplification des processus de production par automatisation (suppression de certaines interventions humaines et des risques d'erreur associés), l'accélération des process de fabrication, de surveillance et de contrôle de la complexe chaîne de production des produits pharmaceutiques, et l'utilisation d'outils numériques pour faciliter les transferts de technologie et assurer la transmission de la qualité des processus industriels d'origine. Il convient de viser la mise en place d'un cadre réglementaire et scientifique de la technologie du processus de fabrication en continu, en lieu et place du processus traditionnel de fabrication par lots. Cette évolution pourrait contribuer à mieux gérer les risques de ruptures d'approvisionnement de médicaments et à réduire les rappels liés à des problèmes de qualité des produits ou des installations.

Si la réglementation au niveau national et européen apporte un début de réponse aux questions des ruptures de stocks, c'est dans la relation des acteurs que doit être trouvée la réponse juridique à la sécurisation des flux de produits. Cela suppose un encadrement juridique dont l'efficacité repose sur son agilité à s'adapter aux constantes évolutions numériques.

SECTION 2

## LE RECOURS COMBINÉ À L'INTELLIGENCE ARTIFICIELLE ET LA *BLOCKCHAIN* DANS L'ENCADREMENT JURIDIQUE DE LA PRODUCTION DES MÉDICAMENTS

Afin de répondre aux problématiques liées aux ruptures de stock, à la lutte contre les produits falsifiés, l'utilisation des outils numériques intelligents est une solution. Mais elle présente d'autres formes de risques liés à la sécurité des systèmes,

à la confidentialité des informations qui circulent, à la protection des données collectées en interne et externe, à la protection du secret des affaires, à la sécurisation des données de propriété intellectuelle et industrielle, à la responsabilité des acteurs de la chaîne.

En conséquence, l'utilisation de ces « outils numériques » dans la *supply chain* soulève de nombreuses questions juridiques portant non seulement sur la conformité des schémas adoptés avec les réglementations européennes, mais aussi et surtout sur la construction d'une architecture contractuelle sécurisée pour les différents acteurs tout au long du circuit.

Elle suppose une révision de la politique économique et éthique de l'industrie pharmaceutique sur le terrain international, une formation globale des équipes de la *supply chain*, et entraîne une révolution numérique et économique dans les modes de circulation du produit.

C'est désormais une nouvelle technologie qui s'impose et dont va dépendre la sécurisation des chaînes d'approvisionnement internationales qui deviennent de plus en plus complexes et difficiles à garantir en détail. La crise Covid-19 sera un accélérateur d'innovation dans la mise en œuvre de ces innovations au service de la sécurisation du marché européen notamment.

Les autorités de santé en charge de la surveillance du circuit des produits de santé s'investissent sur le sujet. La Direction européenne de la qualité du médicament & soins de santé (EDQM) fait état dans son rapport 2019[(11)] des actions menées en vue de la sécurisation du produit pharmaceutique, et de l'évolution dans la sécurisation des produits, notamment par l'application de la convention Médicrime. La *Food and Drug Administration* américaine a publié deux projets de directives visant à renforcer la mise en œuvre de la loi sur la sécurité de la chaîne d'approvisionnement des médicaments (*Drug Supply Chain Security Act* – DSCSA), qui décrivent les étapes à suivre pour créer un système électronique interopérable. Ce système, qui sera pleinement mis en œuvre d'ici 2023, renforcera la capacité de la FDA d'aider à protéger les consommateurs contre les médicaments susceptibles d'être contrefaits, volés, adultérés ou nuisibles. Le système améliorera également la détection et l'élimination des médicaments potentiellement dangereux de la chaîne d'approvisionnement en médicaments afin de protéger les consommateurs américains.

L'approche juridique consiste alors à identifier les mécanismes de responsabilité portant sur l'organisation de cet encadrement numérique de la *supply chain* et plus particulièrement sur l'encadrement des responsabilités liées à la construction et à l'apprentissage des algorithmes qui permettent l'organisation et la surveillance de la *supply chain*, et des conséquences qui peuvent en découler. Les intérêts sont nombreux, depuis la gestion des contrats avec les fournisseurs qui permet de s'assurer de la qualité et de la reproductibilité des matières premières pharmaceutiques fournies (API) et du respect des réglementations y afférentes, jusqu'à la gestion des contrats distributeurs, qui permettent l'approvisionnement des États, et des structures privées sur les différents territoires, ainsi que la gestion en temps réel par les industries pharmaceutiques des tensions d'approvisionnement, des risques

(11) edqm_rapport_annuel_2019.pdf.

de ruptures et des signalements d'effets indésirables auprès des autorités de santé nationales (ANSM en France) et européenne (EMA).

Grâce à ces solutions d'IA, les contrats peuvent être vérifiés avec une totale fiabilité en quelques secondes tandis que cette tâche réalisée par des experts serait bien plus longue, plus onéreuse et assortie d'un risque d'erreur humaine supérieur. L'IA permet d'intégrer l'ensemble des critères de surveillance et les points critiques sur les matières premières selon leur provenance internationale, et par conséquent de mettre en avant des zones d'alerte. Elle permet d'actualiser des informations sur les clients ; ces informations sont précieuses pour l'industrie et permettent d'avancer rapidement en économisant la perte de temps liée à la mise à jour des fichiers.

Mais l'une des principales spécificités de l'intelligence artificielle est de permettre **d'effectuer des prévisions** très précises à partir de l'ensemble des données collectées au niveau international, et de pouvoir en déduire des besoins de santé publique, afin de permettre l'adaptation et la réponse de l'industrie. Cette gestion prédictive est désormais fondamentale dans l'industrie des produits de santé, et ce d'autant plus dans un contexte de pandémies auquel sont exposées toutes les sociétés. L'un des piliers fondamentaux de la prévisibilité de la demande est la sécurisation de contrats de fourniture de produits – le plus souvent par l'engagement des autorités de santé publique des pays – pour des durées de plusieurs années. C'est en particulier le cas pour les vaccins, afin d'inciter les producteurs à créer ou à maintenir la capacité de production. Plus que dans tout autre domaine, elle permet d'étudier le taux et la vitesse de propagation des pathologies et des besoins de traitements, et par conséquence l'importance d'anticiper les fabrications et gestions des stocks à travers le monde. Elle permet d'optimiser les transports de produits de santé en s'assurant que les produits soient acheminés dans le respect notamment des règles de froid, telles qu'elles apparaissent notamment dans la réglementation européenne concernant les produits thermosensibles comme les vaccins. Concrètement, l'IA est utilisée dans les lignes de production de l'ingénierie et de l'industrie. Elle aide à gérer la maintenance et la rationalisation de la production, notamment grâce à la reconnaissance d'images. L'intelligence artificielle aide la *supply chain* à devenir proactive et prédictive ; elle accroît les compétences humaines et permet d'éviter les tâches répétitives sans valeur ajoutée et présentant un risque élevé d'erreur humaine.

Les solutions d'analyse prédictive combinant *big data* et *machine learning* annoncent une vraie révolution à tous les niveaux de la *supply chain* et des organisations. Elles favorisent la prise de décision et maximisent la performance et l'agilité des entreprises.

Le but de la *blockchain* est de permettre aux différentes entreprises pharmaceutiques, aux régulateurs et aux particuliers d'utiliser la même base de données, sans qu'une seule entreprise ou institution en soit propriétaire.

Au sein des circuits de production des industries de santé, la *blockchain* a deux avantages en sus de la transparence. La *blockchain* est un outil de traçabilité et de vérification d'authenticité des médicaments. Elle permet aux entreprises pharmaceutiques de tenter d'éviter les médicaments contrefaits, en enregistrant les empreintes de chaque action et les différentes phases du processus de fabrication

et de distribution d'un médicament. Elle permet de stocker les preuves d'existence de documents qui sont aujourd'hui l'objet de fraudes. D'autre part, la *blockchain* peut apporter de la fluidité à la *supply chain* du secteur pharmaceutique soumis à un grand nombre de procédures administratives en regroupant les acteurs de la vie du médicament au sein d'un même registre.

Les nouvelles technologies deviennent une opportunité de création de valeur et une ouverture vers de nouveaux marchés. Toutefois, elles portent en elles, comme toutes techniques, des risques de détournement au profit d'usages non conformes et soulèvent au plan juridique des questions sensibles portant sur la protection des données de santé, des données personnelles de l'entreprise, la fiabilité des résultats issus de l'IA, dotée d'une intelligence forte, ou encore l'organisation de pratiques anticoncurrentielles dont il convient d'identifier les critères de qualification. À ces questionnements s'ajoute toute la question de la redéfinition des responsabilités au sein de la *supply chain*, sans outrepasser les dispositions relatives à l'encadrement des relations internationales entre les acteurs.

Si l'IA combinée à la *blockchain* est un outil d'optimisation, elle doit toutefois être conçue, maîtrisée et utilisée dans le respect des principes de prudence afin d'éviter de basculer, au-delà de l'objectif d'optimisation de la *supply chain* dans un intérêt économique et sanitaire, dans l'exploitation excessive des analyses prédictives tant au niveau concurrentiel qu'au niveau éthique de santé publique.

L'ensemble de ce système soulève, au plan juridique, de multiples questions et parmi les plus importantes la question de la captation et du retraitement des données, et celle de la sécurisation numérique de l'ensemble face à un risque de cybercriminalité.

L'architecture de la relation contractuelle dans la *supply chain* fait apparaître de nouveaux acteurs, qui assurent la prestation informatique, qui deviennent les pivots du fonctionnement de l'ensemble de la chaîne logistique, depuis les unités de production, jusqu'à l'utilisateur final.

Une dépendance technique, économique et juridique se met en place qu'il convient d'arbitrer. Il en découle une exploitation de situation concurrentielle nouvelle à laquelle le fabricant est confronté. Cette exploitation du numérique, dans son ensemble, comprenant la gestion des algorithmes, l'utilisation des objets connectés, l'utilisation de l'intelligence artificielle, le déploiement des *blockchains* dans le secteur de la santé, crée une modification, voire une rupture dans les mécanismes de régulation tels qu'ils sont analysés par les acteurs. La régulation du secteur de la santé dans son ensemble est bouleversée par l'entrée en force du numérique et conduit les autorités de santé et de concurrence à se pencher sur ces pratiques.

CHAPITRE 7

# L'IMPACT DU NUMÉRIQUE DANS LA DISTRIBUTION DES PRODUITS DE SANTÉ

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Inès AGGOUNE
Étienne BARA
Sasha LAVERNHE

L'organisation de la distribution des produits de santé a connu de profondes évolutions.

Les schémas classiques de distribution pharmaceutique passent par le circuit entre les fabricants, grossistes répartiteurs et officines, par la vente directe, par le circuit hospitalier.

Tous ces schémas sont fortement touchés par le numérique, mais ce qui est le plus marquant est l'organisation de la vente en ligne des produits de santé. L'impact de la crise Covid-19 a mis en exergue ce besoin d'organisation du circuit numérique, et pointé la nécessité d'une évolution vers une organisation fluidifiée du circuit de distribution. La dématérialisation de l'acte d'achat touche de plus en plus de produits du quotidien, dont les produits de santé, soins et beauté ; la pharmacie d'officine se doit donc d'opérer le virage de la transformation numérique. Le marché des produits de santé comprend les produits soumis au monopole pharmaceutique, et vendus en pharmacie, et les produits assimilés qui n'entrent pas dans le monopole pharmaceutique et peuvent être vendus en parapharmacie ou en magasins spécialisés comme les magasins biologiques. En France, le marché des médicaments est encore peu soumis au e-commerce, alors que pour les produits voisins comme les cosmétiques et compléments alimentaires, la concurrence fait rage entre les distributeurs sur Internet et les plateformes de distribution se multiplient.

Bien que le marché des produits de santé soit régulé partout dans le monde, sous des formes plus ou moins sévères, il est, en France, très sévèrement réglementé dans le cadre du monopole pharmaceutique et monopole officinal. En effet, la vente

de médicaments sous ordonnance en ligne est réservée aux pharmaciens d'officine, et seuls les médicaments sans prescription obligatoire sont autorisés à la vente en ligne sous de strictes conditions. Par ailleurs, certains produits de santé entrent dans le monopole officinal et ne peuvent être vendus que par une officine, ce qui est le cas de certaines plantes officinales, huiles essentielles notamment.

À la différence de la France, de nombreux pays comme l'Allemagne, la Grande-Bretagne ou encore les Pays-Bas vendent déjà des médicaments sur prescription en ligne. Ces disparités réglementaires très importantes entre les différents pays s'expliquent par un cadre législatif non harmonisé au niveau européen concernant la vente en ligne, en vertu du principe de souveraineté des États membres en matière de santé (TFUE, art. 168). Si la jurisprudence de la Cour de justice de l'Union européenne, dans la célèbre affaire *Doc Morris*(1) du 11 décembre 2003, est venue poser le principe de la vente en ligne des produits de santé en reconnaissant la possibilité pour les États membres souverains dans leur politique de santé (TFUE, art. 168 et 114)(2) de réduire cette vente en ligne aux seuls médicaments non prescrits, justifiant ainsi le monopole pharmaceutique français(3), ce qui est le cas de la France, elle autorise les États à mettre en place une vente en ligne des produits prescrits et remboursés, ce qui est donc le cas dans plusieurs États membres. Face au développement de la vente en ligne des produits et à la prolifération des produits contrefaits et falsifiés au sein de l'UE, la directive 2011/62/UE du Parlement européen et du Conseil du 8 juin 2011 a enjoint les États membres de l'UE à autoriser ce commerce sur Internet, mais en l'encadrant strictement(4). La France a saisi cette occasion pour limiter les conditions de vente par Internet en réservant la vente aux seuls produits en accès libre et en vente libre en officine, ce qui représentait quatre cents références. Cette position a été contestée et le Conseil d'État(5) s'est prononcé en faveur d'une ouverture de la vente en ligne à tous les produits en vente libre, c'est-à-dire qui ne nécessitent pas une prescription médicale ; autrement dit, sont visés les produits de prescription médicale familiale (PMF). Le Conseil d'État, garant de l'application du droit européen en matière de libre circulation des produits, est venu encadrer la position trop stricte de la France concernant la vente en ligne des produits, notamment en annulant l'arrêté relatif aux bonnes pratiques de dispensation adopté le 20 juin 2013(6). Enfin, deux arrêtés en date du 28 novembre 2016(7) sont venus préciser l'ensemble des contraintes techniques et des obligations imposées

(1) CJCE, 11 déc. 2003, aff. C-322/01, *Deutscher Apothekerverband eV c/ 0800 Doc NV et Jacques Waterval : Rec. CJCE* 2003, I, p. 14887.

(2) B. Espesson-Vergeat, *Le périmètre des dérogations pour raison de santé aux règles du marché intérieur de l'Union européenne*, *Mél. Bélanger*, *LEH*, 2015.

(3) B. Espesson-Vergeat, *La distribution en ligne du médicament au regard du droit de la concurrence, panorama de droit pharmaceutique*, *RGDM*, janv. 2014, p. 155.

(4) PE et Cons. UE, dir. (UE) 2011/62, 8 juin 2011, modifiant la directive (CE) n° 2001/83, instituant un code communautaire relatif aux médicaments à usage humain, en ce qui concerne la prévention de l'introduction dans la chaîne d'approvisionnement légale de médicaments falsifiés : *JOUE* n° L 174, 1er juill. 2011, p. 74.

(5) CE, 17 juill. 2013, nos 365317, 366195, 366272 et 366468.

(6) CE, 16 mars 2015, nos 370072, 370721 et 370820.

(7) A. 28 nov. 2016, relatif aux bonnes pratiques de dispensation des médicaments dans les pharmacies d'officine, les pharmacies mutualistes et les pharmacies de secours minières, mentionnées à l'article L. 5121-5 du Code de la santé publique : *JO* 1er déc. 2016, n° 279, texte n° 25. – A. 28 nov. 2016, relatif aux règles techniques applicables aux sites Internet de commerce électronique de médicaments prévues à l'article L. 5125-39 du Code de la santé publique : *JO* 1er déc. 2016, n° 279, texte n° 26.

aux pharmaciens concernant la vente en ligne. Ces conditions ont été encore alourdies par ces deux arrêtés entrés en vigueur le 1er février 2017 : en premier lieu, celui du 28 novembre 2016 relatif aux règles techniques applicables aux sites Internet de commerce électronique de médicaments de l'article L. 5125-39 du Code de la santé publique et, en second lieu, celui du 28 novembre 2016, relatif aux bonnes pratiques de dispensation des médicaments dans les pharmacies officines, les pharmacies mutualistes et les pharmacies de secours minières.

Cette position stricte a été considérée par l'Autorité de la concurrence comme excessive, et limitant la possibilité pour les officines de se positionner sur le terrain concurrentiel européen. Au travers de plusieurs avis rendus concernant les arrêtés en question, l'Autorité de la concurrence est venue développer une argumentation sur l'intérêt d'assouplir ces conditions de vente en ligne afin de permettre aux officines françaises de rester compétitives face au déploiement des plateformes pharmaceutiques européennes(8). Ces arguments n'ont pas été entendus, la profession pharmaceutique, et notamment l'Ordre des pharmaciens, arguant de la nécessité de préserver le monopole pharmaceutique dans un intérêt général de protection de la santé publique, et ce dans un contexte marqué par la multiplication des produits contrefaits et falsifiés sur le marché en ligne, par l'augmentation de la consommation des médicaments par les patients en automédication, et par la dangerosité de cette surconsommation qui a pu conduire le ministère de la Santé à modifier les conditions de vente de certains produits en accès libre, en officine ou en ligne (et notamment les produits utilisés par les mineurs à usage récréatif). Ces arguments de protection de la santé publique ont prévalu en France. Toutefois, ces contraintes, dont certaines ne sont pas imposées aux pharmaciens étrangers, y compris au sein de l'Union européenne, sont en effet à l'origine d'un déséquilibre disproportionné par rapport aux objectifs de santé publique poursuivis. Des assouplissements s'avéraient nécessaires. L'Autorité de la concurrence a émis des préconisations en ce sens, dans son avis de 2019(9), reprises dans le projet de loi « ASAP »(10).

En effet, le commerce en ligne représente donc une part infime de la vente des médicaments en France, et le nombre de sites est très faible ; en revanche, les plateformes de ventes de médicaments abondent dans d'autres territoires, notamment les Pays-Bas.

L'assouplissement avait pour objectif de permettre le développement de la vente en ligne des médicaments de prescription médicale familiale en France, en passant d'un régime d'autorisation à un régime de déclaration préalable pour la création de pharmacies en ligne, en favorisant le développement de plateformes mutualisées entre officines afin de réduire les coûts pour les officines, et en permettant la vente en ligne de médicaments au sein de l'officine et au sein d'un local rattaché, tout en offrant de nouveaux services aux patients avec le maintien d'exigences de sécurité

(8) Aut. conc., avis n° 16-A-09, 9 avr. 2016, relatif à deux projets d'arrêtés concernant le commerce électronique de médicaments.
(9) Avis n° 19-A-D8, 4 avr. 2019, relatif aux secteurs de la distribution du médicament en ville et de la biologie médicale privée.
(10) L. n° 2020-1525, 7 déc. 2020, d'accélération et de simplification de l'action publique, dite « ASAP ».

élevées, afin de lever l'obstacle des locaux de stockage rattachés à l'officine obligatoirement, ce qui constitue un frein au développement de la vente en ligne faute de pouvoir organiser une activité logistique efficiente. Le Conseil d'État[11] a d'ailleurs considéré que, par la combinaison des articles L. 5125-33 et R. 5125-9 du Code de la santé publique, un local situé à 3,6 kilomètres de l'officine n'est pas à proximité immédiate de l'officine. Sous l'impulsion de l'Autorité de la concurrence, la loi « ASAP » devait aller plus loin et autoriser les entrepôts de stockage, qui aurait permis de faire concurrence aux activités déployées notamment aux Pays-Bas. En l'état actuel, la France reste dans une position visant à privilégier la protection de la santé publique par le contrôle des modalités de vente en ligne des médicaments. L'argument de la concurrence n'est pas retenu comme suffisant pour modifier la position de protection des officines. Les pharmaciens français doivent, en outre, continuer à composer avec l'interdiction de référencer le site sur des moteurs de recherche et annuaires contre rémunération[12], ce qui pose une question importante concernant l'impact concurrentiel des sites étrangers sur le marché national. Les pharmacies en ligne françaises ne sont pas autorisées à faire de la publicité comme du référencement payant ou des comparateurs de prix malgré l'énorme levier de croissance que représentent ces stratégies *on-line*. À l'occasion d'un recours direct contre l'arrêté du 26 novembre 2016[13], le Conseil d'État avait alors confirmé la légalité de la disposition interdisant le référencement payant des sites Internet de pharmacie. Mais la situation vient d'évoluer, et par un revirement de jurisprudence, le Conseil d'État, dans un arrêt du 17 mars 2021, juge illégale l'interdiction de référencement payant des sites de vente en ligne de médicaments et enjoint au ministre de la Santé d'abroger la disposition litigieuse figurant dans l'arrêté du 26 novembre 2016. La situation semble donc évoluer en faveur d'un assouplissement des règles de vente et publicité sur Internet, dans un contexte Covid-19 fortement marqué par la nécessité de promouvoir la vente en ligne. Le Conseil d'État était saisi d'un recours pour excès de pouvoir dirigé contre la décision ministérielle refusant d'abroger une disposition figurant en annexe de l'arrêté du 26 novembre 2016 relatif aux règles techniques applicables aux sites Internet de commerce électronique de médicaments, dans la mesure où elle interdit la recherche de référencement dans des moteurs de recherche ou des comparateurs de prix contre rémunération. Le Conseil d'État a estimé que l'interdiction de référencement payant des sites de vente en ligne de médicaments, applicable aux seules officines situées en France, ne repose pas sur un motif d'intérêt général suffisant, en rapport avec l'objectif de lutte contre la surconsommation des médicaments, et qu'elle porte, dès lors, une atteinte injustifiée au principe d'égalité. La décision ministérielle refusant d'abroger l'annexe de l'arrêté du 28 novembre 2016, en tant qu'elle interdit le référencement payant de ces sites dans des moteurs de recherche ou des comparateurs de prix, est donc annulée, et le Conseil d'État a enjoint au ministre chargé de la santé d'abroger la disposition litigieuse dans le délai de deux mois. Cette position du Conseil d'État fait suite

(11) CE, 28 mars 2018, n° 408886.
(12) CJUE, 1er oct. 2020, aff. C-649/18.
(13) CE, 4 avr. 2018, n° 407292.

à la position adoptée par la Cour de justice de l'Union européenne dans une affaire de novembre 2020 et qui marque un tournant avec la possibilité de faire de la publicité en ligne pour les médicaments à partir d'un site établi hors de France.

La Cour de justice(14) a estimé qu'un État membre ne peut pas interdire aux pharmacies proposant un service de commerce électronique de médicaments de recourir au référencement payant dans des moteurs de recherche et des comparateurs de prix, à moins qu'il ne soit dûment établi devant la juridiction nationale qu'une telle restriction est apte à garantir la réalisation de l'objectif de protection de la santé publique et qu'elle ne va pas au-delà de ce qui est nécessaire pour atteindre cet objectif.

La jurisprudence est donc régulièrement sollicitée sur la question de l'ouverture des modalités de distribution des produits de santé qui connaissent une concurrence féroce sur le marché européen.

En effet, les études économiques démontrent qu'en 2019, le total des ventes sur Internet en France a dépassé les 100 milliards d'euros. Une croissance de +11 % des sites e-commerce en 2020 a été constatée. Le volume des achats en ligne, tous secteurs confondus, a augmenté de 39 % depuis le confinement, visant tout spécifiquement l'alimentaire et les produits de parapharmacie de 63 %. Cet accroissement des ventes est à la fois dû à la demande conjoncturelle de produits relatifs au coronavirus (masques chirurgicaux, savons, gels hydroalcooliques, vitamines…), mais également au confinement qui entraîne de fait des changements de mode de consommation des clients, ces derniers favorisant de plus en plus les plateformes d'e-commerce. L'évolution de la distribution en ligne des produits de santé, à l'échelle européenne, est donc une réalité à laquelle sont confrontées les officines françaises. Le secteur de la santé est le dernier secteur qui va et doit prendre ce tournant du digital pour répondre aux besoins des consommateurs. Pour les pharmacies, le virage numérique est complexe à mettre en œuvre, non seulement au plan des contraintes déontologiques et réglementaires, mais aussi au plan technique et financier. Car, au-delà du fait que la réglementation encadre très strictement la vente en ligne, l'organisation technique de la vente en ligne suppose la création d'un site Internet, le recours à une personne compétente pour le faire fonctionner, une organisation logistique concernant le stockage et la distribution des produits au patient, dans un contexte de sérialisation de certains médicaments. Selon l'Autorité de la concurrence, en France, en 2019, la vente en ligne des médicaments représentait 1 % du chiffre d'affaires de la vente de médicaments contre 15 % en Allemagne. Sur les plus de 21 000 officines existantes, seules 720 disposent d'un site Internet et 400 d'une véritable activité en ligne, d'après l'Ordre national des pharmaciens qui tient à jour la liste des sites Internet autorisés.

Cette transformation profonde qui touche la vente en ligne concerne également la digitalisation de multiples services et conseils proposés par les professionnels de santé. En effet, la vente en ligne de produits et prestations de services par le pharmacien constitue l'avenir de l'officine qui doit se rapprocher du patient en gardant sa confiance et en assurant la sécurité, la traçabilité et la sécurité des opérations.

(14) CJUE, 1er oct. 2020, aff. C-649/18, A.

Désormais, et pour le futur, il convient d'appréhender le numérique comme un allié et un canal additionnel de vente qui permettra à l'officine de mieux répondre aux attentes du patient-consommateur, mais aussi de fluidifier les stocks de produits, et d'entrer dans la concurrence européenne avec, notamment, un impact sur le prix. Ceci s'inscrit par ailleurs dans une évolution plus globale qui affecte tout le secteur de la santé digitale dans lequel la pharmacie de demain devra faire partie.

Toutefois, l'organisation de l'e-pharmacie suppose la révision de la réglementation historiquement ancrée dans le concept français du monopole pharmaceutique[15]. Cela suppose donc une révision législative et réglementaire qui ne sera pas sans soulever de nombreuses oppositions, dans un contexte marqué par l'augmentation des risques de falsifications et contrefaçons de produits, ou encore des risques de mésusage, surconsommation des produits par les patients-consommateurs, et enfin des risques d'usages médicamenteux à visée récréative, qui ont conduit le ministère de la Santé français à réagir plusieurs fois en interdisant la vente aux mineurs de certains médicaments, ou en sortant certains produits de la possibilité d'être placés en accès libre. Cette évolution s'inscrit dans l'idée générale du programme « Ma santé 2022 », et est préconisée dans la mission pilotée par Dominique Pon et Laura Létourneau, respectivement responsable et déléguée ministériels du numérique en santé, dans la feuille de route qui met en avant vingt-six actions autour de cinq orientations dont l'évolution du numérique dans l'activité des professions de santé dont les pharmaciens.

L'impact du numérique dans la distribution des produits de santé suppose donc un encadrement plus ouvert de l'e-pharmacie, des effets de la publicité et promotion du produit sur les pratiques d'automédication du patient (Section 1), mais aussi une surveillance renforcée concomitante de la circulation des produits par Internet, notamment par un renforcement du contrôle des douanes, de la DGCCRF et de l'ANSM (Section 2).

SECTION 1

## UN ÉLARGISSEMENT CONTRÔLÉ DE LA E-PHARMACIE

La vente de produits de santé en ligne est strictement encadrée par la loi. En France, seuls les pharmaciens titulaires de leur propre officine peuvent proposer ce type de service. Toujours selon le droit français, les pharmacies en ligne sont également tenues de mettre à la disposition de leur clientèle un moyen technique (téléphone, e-mail ou encore formulaire de contact) lui permettant de bénéficier d'une consultation pharmaceutique.

Les officines qui s'engagent dans la vente en ligne doivent assurer être en conformité avec les règles ; les sites sont validés par l'Ordre des pharmaciens en France,

(15) B. Espesson-Vergeat, La *e-Pharmacie, entre sécurité et concurrence*, Lamy concurrence Wolters-Kluwer, janv. 2014.

ce qui garantit leur fiabilité. Nombreux sont les rapports de l'Ordre des pharmaciens[16] et de l'Académie de pharmacie[17] concernant la sécurisation des sites Internet. Toutefois, l'évolution des règles doit porter sur les normes à respecter.

La vente en ligne permet d'organiser une relation de fidélisation des patients-consommateurs à certaines plateformes qui proposent notamment des bons de fidélisation, des livraisons gratuites de produits à partir d'un certain montant, d'une certification garantissant un service de qualité et des achats sécurisés. Ce label est doublé d'un enregistrement auprès de l'EAMSP, une association européenne centralisant les officines digitales reconnues pour leur fiabilité. La multiplication des sites européens de vente en ligne des médicaments et publicité à destination du public français est marquante, tout particulièrement dans le contexte de pandémie.

En France, l'état d'urgence sanitaire lié à la crise Covid-19 a ouvert des possibilités nouvelles dérogatoires, mais toute la question sera de savoir si ces nouvelles missions pourront être pérennisées par une révision de l'encadrement réglementaire des missions des pharmaciens.

Sont concernées, d'une part, la relation du patient avec les professionnels de santé, et notamment la prescription et la délivrance des médicaments et, d'autre part, les conditions de vente des produits et réalisation des services en ligne, ainsi que la livraison au domicile du patient.

## § 1. – L'organisation de la prescription et délivrance des produits sur ordonnance

La phase de pandémie a contraint la population au confinement, et de ce fait les consultations numériques ont été utilisées de façon exponentielle. Le recours à ce mode de consultation et donc de transmission en ligne des ordonnances implique une organisation de la transmission de l'ordonnance à l'officine. La réglementation, en l'état actuel du droit, n'autorise pas en France la transmission directe du médecin au pharmacien puis la livraison au patient. En revanche, le médecin peut transmettre sur un espace Internet dédié et sécurisé une ordonnance au patient, lequel devra ensuite transmettre cette ordonnance à l'officine de son choix. Ce process permet de garantir, d'une part, la confidentialité des données et le secret médical, dans la relation entre le patient et le médecin et, d'autre part, le libre choix du pharmacien par le patient, ces règles relevant des codes de déontologies du médecin et du pharmacien.

La mise en œuvre de l'e-prescription n'est aujourd'hui pas totalement opérationnelle.

Toutefois, et compte tenu du contexte, le patient ou le médecin doivent théoriquement envoyer ou présenter une ordonnance *via* un système de transmission

(16) www.ordre.pharmacien.fr/Les-patients/Vente-de-medicaments-sur-Internet-en-France.

(17) Académie nationale de pharmacie, *Ventes de médicaments à partir de sites Internet*, 2007 ; *À propos de l'automédication*, 2006.

sécurisée : par mail, fax ou encore application mobile (par l'intermédiaire du médecin le cas échéant).

Les prescriptions émises dans ce cadre devront se faire en conformité avec les règles de droit commun de prescription/délivrance et de remboursement, afin d'éviter tout abus et mésusage.

À l'instar d'une dispensation classique, le pharmacien devra vérifier que l'ordonnance est bien authentique et qu'elle comporte bien les mentions légales ; procéder aux vérifications telles que prévues par l'arrêté du 28 novembre 2016 relatif aux bonnes pratiques de dispensation des médicaments dans les pharmacies d'officine ; reporter sur l'ordonnance les mentions légales habituelles.

Cette évolution vers une nouvelle relation entre le médecin, le pharmacien et le patient-consommateur est déjà prise en compte dans certains territoires européens, et l'évolution de la réglementation française au bénéfice de la crise, devrait s'engager dans cette voie.

Par ailleurs, il convient de préciser que la crise a permis l'émergence de nouvelles activités déployées par les grossistes répartiteurs, les distributeurs, les groupements de distribution, et notamment dans les États voisins de la France. Ainsi, le distributeur espagnol de médicaments Cofares, associé à l'ESN Viseo, a mis en place une solution numérique de *Distributed Order Management* (DOM) de Fluent Commerce. La nouvelle plateforme e-commerce de Cofares s'adresse aux professionnels des officines et aux particuliers. Elle offre aux pharmaciens une vision globale et en temps réel de leurs stocks ; elle permet également aux clients particuliers de se faire livrer à domicile, de récupérer leurs achats dans une pharmacie grâce au *click and collect*, ou encore de renvoyer les médicaments achetés sur Internet.

Cette approche innovante du service en ligne offert aux patients et aux pharmaciens est encore loin d'être admise en France, et notamment sur la question du retour du médicament, qui n'est pas un produit de consommation classique, mais un produit particulier. Pour des raisons tenant à la protection et la sécurité du produit, le retour du produit acheté en ligne n'est pas possible lorsqu'il s'agit d'un médicament.

Dans une perspective d'ouverture de la relation de soins globale en télémédecine, l'inscription du parcours pharmaceutique devra donc être intégrée, et la fusion du dossier médical et pharmaceutique dans un seul espace de santé dédié du patient permettra d'avancer dans cette direction. Il reste toutefois de nombreux obstacles à surmonter, en modifiant et adaptant la réglementation, mais surtout en favorisant l'organisation numérique de l'officine. Cela suppose des accompagnements financiers indispensables à la sécurisation du parcours du médicament dans le cadre de l'e-prescription.

## § 2. – La réalisation de services en ligne

Hors de la période d'état d'urgence sanitaire, la question des services en ligne des officines n'est pas encore prise en compte dans la réglementation du rôle du pharmacien, ni du fonctionnement de l'officine.

Certaines mesures dérogatoires en vigueur durant l'État d'urgence[18] autorisent des télésoins (soins à distance par vidéotransmission) pour les actions d'accompagnement des patients sous traitement anticoagulant oral (AOD ou AVK) et des patients sous antiasthmatiques par corticoïdes inhalés, et les bilans partagés de médication. Le rôle du pharmacien dans sa relation virtuelle avec le patient va au-delà de la dispensation du produit, et peut conduire à la reconnaissance de services de premier recours, tels qu'ils sont rendus en officine physique.

Cela revient à revoir le contenu du site ou de l'espace numérique dédié entre le patient et le pharmacien afin d'assurer la réalisation des actes dans le respect des dispositions déontologiques qui nécessiteront une révision. Qu'il s'agisse d'actes en officine physiques ou virtuels, il convient de constater l'évolution, au bénéfice de la pandémie du rôle du pharmacien, et son importance dans l'organisation du réseau de premier recours. La vaccination en est une représentation, mais cela va bien au-delà avec la possibilité pour le pharmacien d'accompagner le patient par son conseil en e-consultation, sans toutefois que cette relation soit assimilée à une e-consultation dans le cadre de la télémédecine par le médecin. Il conviendra, dans l'organisation du parcours de soins, de redéfinir clairement le positionnement du pharmacien, et de saisir l'occasion donnée par l'urgence sanitaire en période de crise, pour rendre pérenne une organisation favorisant la relation numérique avec le patient. Cela suppose d'encadrer la responsabilité des pharmaciens en assurant la limite des services autorisés et les conséquences en matière de réparation des préjudices qui pourraient survenir du fait du défaut ou de l'insuffisance d'information, de l'erreur ou de la faute qui pourraient survenir. Cette vision prospective nécessitera un débat entre les Ordres, le ministère, l'Autorité de la concurrence, et les diverses parties concernées, notamment l'Ordre des médecins, afin de trouver une ligne directrice conforme à l'évolution du parcours numérique de santé, tel qu'il est voulu par la stratégie « *M*a santé 2022 ».

SECTION 2

## UN ENCADREMENT RENFORCÉ DE LA SURVEILLANCE DES ACTIVITÉS NUMÉRIQUES

L'ouverture de l'activité de dispensation du produit par Internet et donc l'ouverture des sites Internet d'officine, rendue concurrentielle par rapport aux officines européennes, *leader* sur le marché, implique nécessairement une surveillance accrue de la circulation des produits et des risques qui y sont attachés (§ 1), ainsi qu'un renforcement du pouvoir de surveillance de l'ANSM concernant les excès dans l'usage des produits pharmaceutiques de PMF qui, sans être considérés initialement comme dangereux, peuvent néanmoins le devenir par le biais du mésusage (§ 2).

(18) Arrêté prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire, DGS URGENT n° 2021_37 et et ses fiches annexe 1 et annexe 3.

Par ailleurs, un contrôle renforcé des conditions de circulation des produits de santé par internet s'impose en raison des risques de circulation de produits contrefaits alimentés par les plateformes (§ 3).

## § 1. – La surveillance de la consommation des produits

La surveillance de la consommation des médicaments passe dans un premier temps par le contrôle des activités de promotion et de publicité des officines en ligne puis, dans un second temps, par un contrôle de la surconsommation des produits en ligne.

Concernant la question de la promotion et de la publicité en ligne, les pharmacies qui se lancent dans la vente en ligne étaient en France limitées dans leur possibilité de faire de la publicité. Or, suivant la position de la Cour de justice de l'Union européenne, qui prône la liberté du commerce et est garante des libertés de circulation des marchandises et services, le Conseil d'État dans une décision du 17 mars a levé l'interdiction pour les pharmaciens de recourir au référencement payant pour accroître leur visibilité sur Internet, afin de vendre des médicaments en ligne.

À compter du 17 mai 2021, les pharmaciens auront le droit de faire de la publicité en ligne en utilisant un référencement payant afin de vendre des médicaments non soumis à une souscription médicale.

« Il n'est pas établi que l'interdiction du référencement payant par les seules officines situées en France soit de nature à préserver la relation de confiance entre le patient et le pharmacien, dès lors qu'elle permet aux clients français d'acheter plus facilement des médicaments auprès de sites qui ne sont pas soumis aux garanties déontologiques applicables aux pharmaciens installés en France », précise la décision.

Cette décision du Conseil d'État est un revirement de jurisprudence. En 2018, la juridiction administrative suprême, déjà saisie de cette question du référencement payant, avait estimé que la vente en ligne était une publicité qui portait atteinte à la protection de la santé publique. En réponse à une action intentée par des pharmaciens français, le bien-fondé de cette interdiction avait été soumis à la Cour de justice de l'Union européenne. Dans un arrêt du 1er octobre 2020, celle-ci a affirmé que le référencement payant des sites Internet était un facteur de développement des pharmacies européennes et avait donc émis un avis favorable au maintien de ces publicités réalisées par des officines établies au sein de l'Union européenne et à destination des patients-consommateurs français. Le Conseil d'État a donc suivi la position de la Cour de justice, qui s'inscrit dans une démarche d'ouverture du marché et notamment d'application large de la réglementation sur la publicité numérique. La question posée était de savoir s'il était possible en France d'interdire à un site étranger de solliciter la clientèle française par des procédés et moyens considérés comme contraires à la dignité de la profession ; l'interdiction d'inciter les patients à une consommation « abusive » de médicaments ; et l'application des bonnes pratiques de dispensation avec « l'insertion d'un questionnaire de santé

dans le processus de commande de médicaments en ligne et interdisant de recourir au référencement payant ».

Il convient de préciser que la Cour de justice de l'Union européenne devait se prononcer sur la question préjudicielle posée de savoir si les articles du Code de la santé publique (C. santé publ., art. R. 4235-22 et R. 4235-64) « constituent des entraves non justifiées au principe de libre circulation des produits et, n'étant pas justifiés et proportionnés à la nécessité de la protection de la santé publique », et seraient contraires aux directives européennes 2001/83/CE (modifiée) du 6 novembre 2001 (art. 85 quater) et 2000/31/CE du 8 juin 2000 prise en son article 3, ainsi qu'à l'article 34 du TFUE relatif aux mesures d'effet équivalent à une restriction quantitative. L'article 3, § 4, a), i) de la directive 2000/31/CE dispose que la protection de la santé publique permet de restreindre, lorsque cela est nécessaire et proportionné, la libre circulation des services de la société de l'information. L'article 85 quater, 2, de cette directive énonce que : « Les États membres peuvent imposer des conditions, justifiées par la protection de la santé publique, pour la délivrance au détail, sur leur territoire, de médicaments offerts à la vente à distance au public au moyen de services de la société de l'information ». La Cour de justice de l'Union européenne s'est prononcée de nombreuses fois sur les limites acceptables à la libre circulation des marchandises et sur l'interprétation de l'article 36 du TFUE[19].

Nombreux sont les commentaires sur cette position du Conseil d'État et sur celle de la Cour de justice qui ouvre une dynamique nouvelle pour les officines françaises, et renforce le pouvoir des officines situées notamment aux Pays-Bas. Mais cela ne change rien au fait que les seuls médicaments concernés par la vente en ligne en France demeurent les produits non prescrits, les produits sur prescription ne peuvent donner lieu à une vente en ligne auprès du public français. Au sein de l'Union européenne, les schémas sont différents avec des niveaux d'analyse variés de la protection de la santé publique. Ainsi, la Grèce restreint la vente aux produits de prescription médicale familiale (PMF), mais autorise les sociétés créées indépendamment des officines, qualifiées de *pure players* ; le Royaume-Uni et les Pays-Bas ouvrent la vente à tous les médicaments et autorisent les *pure players* ; l'Allemagne et l'Autriche autorisent la vente en ligne de produits prescrits. Il convient donc d'étudier au cas par cas la situation législative et réglementaire au sein des États membres qui, en se fondant sur l'article 34 du TFUE, établissent des dispositions spécifiques dans le secteur de la santé, sans porter atteinte à la libre circulation des marchandises, en s'appuyant sur le principe de souveraineté des États en matière de santé, dans la mesure où ces dispositions sont proportionnées à l'objectif de protection de la santé publique. Ainsi la France peut décider de retirer les produits de vente libre aux mineurs, sous la forme physique ou en ligne, en justifiant du risque de mésusage grave constaté sur certains produits de PMF tels que l'ibuprofène.

(19) CJCE, 2 juill. 1974, n° 8/74, *Dassonville : Rec. CJCE* 1974, I, p. 837. – CJCE, 21 mars 1991, n° C-369/88, *Delattre : Rec. CJCE* 1991, I, p. 1487. – CJCE, 21 mars 1991, n° 60/89, *Monteil et Samanni : Rec. CJCE* 1991, I, p. 1547. – CJCE, 24 nov. 1993, n$^{os}$ C-267/91 et C-268/91, *Keck et Mithouard : Rec. CJCE* 1993, I, p. 6097. – CJUE, 19 oct. 2016, n° C-148/15, *Deutsche Parkinson Vereinigung*, ECLI :EU :C :2016 :776, § 23. – CJUE, 9 sept. 2008, n° C141/07, *Commission c/ Allemagne*, EU :C :2008 :492, pt 28.

La vente en ligne des médicaments est donc placée sous un contrôle étroit du pharmacien, peut-être même plus étroit qu'en espace physique, puisqu'il doit mettre en place un espace d'échange interactif avec le patient-consommateur. Cet espace doit permettre un dialogue afin de permettre au pharmacien d'identifier le risque de la délivrance de la commande en ligne. Pour accroître la surveillance de cette activité, la préparation des commandes doit être effectuée au sein de l'officine, sous le contrôle du pharmacien. Le pharmacien doit pouvoir détecter les commandes excessives, le tourisme pharmaceutique qui conduirait à une surconsommation des produits, et il doit pouvoir refuser de délivrer la commande si elle paraît anormale. Enfin il convient de préciser que le médicament commandé en ligne ne pourra pas être retourné à l'officine, à l'instar de ce qui est prévu dans le Code de la consommation concernant la période de réflexion du consommateur.

La question centrale qui survient dans la vente en ligne concerne l'utilisation des plateformes de vente de médicaments, mais aussi d'autres produits de santé.

Au-delà du risque de confusion qu'il convient de lever, et que la DGCCRF surveille activement, le sujet porte sur l'exploitation par les plateformes d'hébergement de leur puissance de mise en relation des officines avec les patients-consommateurs, afin de rendre un service de vente en ligne, ou de mandat de vente en ligne. Sur ce sujet, plusieurs affaires viennent illustrer les risques d'insertion dans la relation entre le pharmacien et le patient d'acteurs du numérique utilisant leur pouvoir sur Internet. Ainsi le Conseil national de l'Ordre des pharmaciens (CNOP) a assigné la société 1001 pharmacies.com servant d'interface entre les consommateurs qui ont recours à la vente en ligne, et les pharmaciens devant le juge des référés du tribunal de grande instance de Paris afin de faire cesser cette activité[20].

Le tribunal a fait droit à la demande du CNOP, la société ayant interjeté appel devant la cour d'appel de Paris. Selon la société qui organise la plateforme, ses activités ne constituent pas une offre de vente, mais en réalité un mandat d'achat pour acquérir, au nom de l'utilisateur, les spécialités souhaitées dans une officine puis procéder à la livraison. L'argumentation est habile, mais ne tient pas devant la cour qui constate que le président de la société commerciale n'est pas pharmacien, qu'aucun responsable n'est inscrit sur un tableau de l'Ordre des pharmaciens, que les données de santé sont stockées chez un hébergeur qui n'est pas agréé, que les produits distribués sont des médicaments soumis à prescription médicale obligatoire, et que la plateforme perçoit directement le prix des médicaments. Or, l'article L. 5125-25, alinéa 2 du Code de la santé publique prohibe toute immixtion d'un tiers dans la relation entre un pharmacien et le patient. Ce trouble est manifestement illicite, car il « viole de manière flagrante les dispositions relatives à la vente de médicaments, au commerce électronique de médicaments et celles réglementant le stockage des données de santé »[21].

En revanche, la cour a considéré dans une autre affaire, que la plateforme, qui était autorisée par l'ARS, et qui ne s'était pas interposée dans la relation entre le patient et le pharmacien mais offrait un service au pharmacien, pouvait être

(20) TGI Paris, réf., 8 août 2014, n° 14/55552.
(21) CA Paris, 25 mars 2016, n° 14/17730.

considérée comme autorisée. La cour d'appel de Versailles a validé les solutions qui s'apparentent à « une simple prestation technique mise à disposition des pharmaciens » dès lors que les sites sont standardisés mais gérés personnellement par les pharmaciens qui reçoivent directement les commandes[22].

Peu à peu le mur infranchissable du monopole pharmaceutique français se fissure et laisse la place à une acceptation de l'activité pharmaceutique en ligne, encadrée toutefois strictement, afin d'assurer la protection du patient-consommateur, et notamment le respect absolu des règles déontologiques du pharmacien envers le patient. Si les formes de distribution évoluent pour s'adapter au commerce Internet et au recours aux plateformes, en revanche l'activité reste placée sous la responsabilité entière du pharmacien, et sur ce point l'exception française demeure un argument acceptable pour la Cour de justice de l'Union européenne.

## § 2. – La surveillance et la protection de l'utilisateur des produits

L'ouverture du commerce en ligne des médicaments engendre un risque de surconsommation ou mésusage des produits de santé. Cela implique donc la mise en œuvre de moyens techniques et humains indispensables au contrôle des commandes.

Cette surveillance peut passer par la mise en place d'un dossier patient-consommateur au sein de l'officine virtuelle, qui permettra de vérifier la consommation des produits et alerter le patient-consommateur, voire refuser la délivrance. Cela peut passer aussi par le contrôle de la consommation au travers du dossier pharmaceutique du patient, qu'il aura au préalable accepté, pour la consommation des produits de PMF. Les produits prescrits et remboursés apparaissent sur cette plateforme, mais ce n'est pas le cas des produits d'automédication. Le recours à une plateforme sécurisée, avec l'accord du consommateur patient, permettrait de vérifier l'état de sa consommation et alerter sur les risques. Cette analyse pourrait être effectuée au travers d'une IA faible de surveillance et alerte, ou d'une *blockchain* dans laquelle les commandes seraient inscrites et sécurisées, garantissant la confidentialité mais aussi la traçabilité infalsifiable. Cela supposerait un engagement financier important que les officines ne sont pas en mesure d'assurer sans accompagnement d'une politique de santé active en ce sens.

Ainsi, pourraient être surveillés les cas de mésusage, surdosage, surconsommation, et donner lieu à une alerte à l'ANSM en cas de risques avérés et signalés pour la santé publique, avec plus d'efficacité. Les signalements actuels d'effets indésirables parviennent à l'ANSM par le médecin, le pharmacien ou par le patient lui-même, mais cela impose le temps de l'intervention humaine pour assurer ce signalement. Le recours à une IA permettrait d'assurer une remontée accélérée des risques et une possibilité pour l'ANSM d'assurer la surveillance des effets indésirables et conduites inappropriées concernant les produits de PMF au plus tôt.

(22) CA Versailles, 12 déc. 2017, n° 16/051671.

Par ailleurs, la gestion des officines en ligne destinées à la vente de médicaments de PMF et d'autres produits voisins, tels que les cosmétiques et compléments alimentaires, suppose une nette distinction entre les produits afin d'éviter tout risque de confusion. La DGCCRF intervient sur la surveillance des pratiques commerciales trompeuses et des modes de distribution illicites[23]. Sans entrer dans le détail des différentes réglementations concernant les produits autres que les médicaments, il convient de préciser que les dispositifs médicaux[24], les cosmétiques et compléments alimentaires sont soumis à des conditions de présentation du produit et de publicité stricte afin d'éviter, d'une part, les risques de santé publique et, d'autre part, la tromperie vis-à-vis du consommateur.

Concernant les DM et DMDIV, la vente des DM ne répond pas à la règle du monopole pharmaceutique et ces derniers peuvent être commercialisés par des personnes autres que des pharmaciens titulaires. En revanche, il est important de noter quelques exceptions. Selon l'article L. 4211-1, § 8 du Code de la santé publique, les DMDIV relèvent du monopole pharmaceutique (des tests destinés au diagnostic de grossesse ainsi que les tests d'ovulation). La plupart des DM accessibles au grand public peuvent donc être proposés sur Internet. Cette mise à disposition du DM sur Internet désigne le titulaire du site web comme un distributeur, au sens du règlement (UE) n° 2017/745. Ce nouveau règlement instaure cette responsabilité du distributeur et définit plus clairement son rôle. Il s'agit de respecter l'ensemble des obligations qui incombent au distributeur, conformément à l'article 14 du règlement.

En France, la surveillance du marché des DM est partagée entre l'ANSM et la DGCCRF, cette dernière contrôlant la sécurité des DM directement vendus aux consommateurs[25]. De fait, toute autre forme d'information visant à promouvoir la vente ou l'utilisation des dispositifs sera qualifiée d'allégation promotionnelle et donc réglementée par les dispositions du Code de la santé publique (art. L. 5213-1 et s.) et les recommandations pratiques de l'ANSM. Une réglementation essentielle encadre également spécifiquement la communication sur Internet des dispositifs médicaux : la Charte pour la communication et la promotion des produits de santé (médicaments et dispositifs médicaux) sur Internet et le e-media de l'ANSM. En effet, cette charte ne s'applique pas uniquement aux médicaments mais également aux dispositifs médicaux ; la présentation des dispositifs dans ce contexte de vente en ligne s'apparente à une promotion et donc à une publicité.

Concernant les produits cosmétiques mis sur le marché, ils sont réglementés par les dispositions du règlement « cosmétiques » et celles du Code de la santé publique (notamment les articles L. 5131-1 à L. 5131-8 et L. 5431-1 à L. 5431-9 issus de la loi n° 2014-201 du 24 février 2014 portant diverses dispositions d'adaptation

(23) J. Bayle, *Environnement réglementaire du e-commerce des médicaments, dispositifs médicaux, produits cosmétiques et compléments alimentaires*, Sciences du Vivant [q-bio], 2020.

(24) Règl. n° 2017/745/CE, applicable aux dispositifs médicaux et modifiant la dir. 2001/83/CE.

(25) B. Espesson-Vergeat, *Quelles articulations de compétences entre les acteurs de la mise en œuvre des politiques de concurrence et de santé ?* : Université de Lille – Webinaire du 6 novembre 2020, *Le secteur pharmaceutique : nouveaux enjeux des questions de concurrence*, Silvia Pietrini (Dir. scientifique), *Revue de jurisprudence commerciale* 2021, n° 1, p. 60 à 77.

au droit de l'Union européenne dans le domaine de la santé). Ils relèvent de fait de cette réglementation spécifique ainsi que des recommandations de plusieurs instances telles que la DGCCRF et l'Autorité de régulation professionnelle de la publicité.

La DGCCRF intervient afin de surveiller, alerter, voire interdire la promotion et la vente de ces produits en ligne sur le fondement des pratiques commerciales trompeuses. Il s'agit de « toute action, omission, conduite, démarche ou communication commerciale, y compris la publicité et le marketing, de la part d'un professionnel, en relation directe avec la promotion, la vente ou la fourniture d'un produit au consommateur » au sens de la directive 2005-29/UE du 11 mai 2005 relative aux pratiques commerciales déloyales. L'article L. 121-1 du Code de la consommation pose un principe général d'interdiction des pratiques commerciales déloyales. Les sanctions pénales sont lourdes[26] et l'ensemble des pratiques est détaillé largement sur le site de la DGCCRF[27].

L'officine qui dès lors opte pour la vente pharmaceutique et parapharmaceutique se doit de respecter l'ensemble de ce *corpus* législatif et réglementaire.

Par ailleurs, toute personne qui exploiterait un site sans avoir la qualité de pharmacien, pour la présentation de produits relevant du monopole pharmaceutique (tels que les huiles essentielles, les plantes médicinales, *etc.*), serait considérée comme développant un exercice illégal de la pharmacie, et encourrait les sanctions pénales afférentes.

## § 3. – Les risques de circulation de produits contrefaits alimentés par les plateformes

La vente en ligne favorise et amplifie le risque de circulation des produits contrefaits et falsifiés qui constitue un fléau de la société au niveau planétaire. En France, les contraintes réglementaires très lourdes concernant la circulation du produit pharmaceutique limitent considérablement les risques de pénétration des produits falsifiés dans la chaîne de distribution des produits. Le contrôle par la sérialisation de certains produits médicamenteux constitue une première étape, prévue par la loi en application de la directive, adoptée en lien avec la convention Médicrime (V. *supra*, Chapitre 5 : « L'impact du numérique dans la production des produits de santé »). Dans ce contexte, la vente en ligne des produits pharmaceutiques en France est soumise à des contrôles stricts identiques à ceux de la vente en officine, ce qui peut ralentir l'activité numérique française au regard de la concurrence européenne. La période de pandémie aggrave considérablement ces risques et ils

(26) Emprisonnement de deux ans et amende de 300 000 €. Le montant de l'amende peut être porté, de manière proportionnée, aux avantages tirés du manquement, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits, ou à 50 % des dépenses engagées pour la réalisation de la publicité ou de la pratique constituant le délit.

(27) Ministère de l'Économie des Finances et de la Relance, DGCCRF, *Pratique commerciales trompeuses : les clés pour les reconnaître et s'en prémunir*, 20, déc. 2019. (www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Pratiques-commerciales-trompeuses).

sont signalés par le Conseil de l'Europe[28], qui invite les États à mettre en œuvre toutes les mesures pour lutter contre ces pratiques. Le contrôle de sites Internet et notamment des sites des officines est un passage obligé dans le contrôle. Le recours à la *blockchain* comme outil numérique doté d'une IA, permettant de contrôler et tracer les produits pharmaceutiques de la fabrication jusqu'au patient, est une solution efficace, mais financièrement lourde et complexe à mettre en œuvre. Certains projets sont en cours, notamment pour la distribution de médicaments sur les territoires sous-dotés en capacité de contrôle de la sécurité des produits et notamment les territoires africains. Mais cette solution est tout à fait adaptable au système français et pourrait dès lors être envisagée entre le fabricant, le grossiste répartiteur et le pharmacien, et dans le cas de la vente directe entre fabricant et officine. Reposant sur la *blockchain* et l'intelligence artificielle, la plateforme permet d'assurer le suivi et l'authentification des médicaments tout au long de la chaîne de distribution. Avec ce dispositif, les pharmaciens et les patients disposent d'une solution respective où ils n'ont qu'à scanner un médicament pour vérifier son authenticité.

Cette surveillance passe par le contrôle des lieux de stockage des produits. En France, la réglementation très stricte ne permet pas aux officines d'avoir un entrepôt de stockage, La réglementation actuelle impose à ces professionnels de disposer d'une officine d'un seul tenant ou d'un local à proximité. La surface des officines ne permet pas pour la plupart des acteurs de créer un espace particulier pour la vente en ligne. Les autorités de santé estiment que la notion de proximité correspond au quartier d'implantation de l'officine, mais laissent le soin aux agences régionales de santé (ARS) de valider ces locaux.

La loi autorise désormais les officines à se regrouper pour le stockage des produits vendus en ligne, mais ces opérations nécessitent un investissement lourd, que les pharmaciens ne sont pas en mesure de faire. La lutte sur le terrain concurrentiel avec les groupements européens est donc très déséquilibrée et justifie la position de l'Autorité de la concurrence française de plaider pour une adaptation de la réglementation aux contraintes économiques actuelles. Ainsi le géant belge de la pharmacie en ligne Newpharma a annoncé l'ouverture prochaine d'un local de stockage de 20 000 mètres carrés près de Liège.

Dans un contexte de pandémie, qui a été marqué par les ruptures de stock et tensions d'approvisionnement, la possibilité pour le patient-consommateur de se fournir en produits sur des plateformes européennes est une tentation. Il est donc particulièrement important d'assurer un renforcement de l'information des patients sur les risques de l'achat des médicaments sur Internet, sur les conditions de contrôles du site par l'Ordre des pharmaciens. Les risques de vente de produits illicites, falsifiés ou contrefaits sont moindres en France. Mais ces pratiques fleurissent sur les marchés non régulés, et notamment aux USA où les ventes de faux vaccins contre la Covid-19 ou encore de faux médicaments contre la pathologie ont été constatées.

(28) CE, *The Medicrime Convention in times of pandemic*, organised by the Criminal law Co-operation Unit Action against Crime, Department Council of Europe 2021. (www.coe.int/fr/web/medicrime/home)

L'avenir de la vente des médicaments par Internet, par les officines et pharmaciens, est donc un sujet sensible qui exige un équilibre difficile entre la sécurité sanitaire, la protection des intérêts des patients-consommateurs, et par ailleurs les enjeux économiques et concurrentiels. Mais il n'est pas assuré que ces enjeux soient en opposition. L'intérêt économique et concurrentiel du pharmacien peut au contraire passer par la communication sur la sécurisation de ses pratiques et sur l'encadrement strict des modes de distribution afin de protéger les patients. La présentation de la protection du patient-consommateur peut être un avantage concurrentiel fort dans ce contexte post-pandémique.

CHAPITRE 8

# L'INTELLIGENCE ARTIFICIELLE ET LES ALGORITHMES COMME NOUVEAU MODE DE CONCURRENCE

Marie KOEHLER DE MONTBLANC
et
Lorye HUGON

L'usage des algorithmes et de l'intelligence artificielle se développe aujourd'hui dans tous les domaines et suscite de nombreuses attentes, notamment dans le secteur de la santé.

Celles-ci concernent tout d'abord l'idée d'une médecine à la fois prédictive, préventive, personnalisée et participative (dite « médecine des 4P »). L'analyse et la confrontation du profil génomique d'un patient à celui d'individus similaires et à leurs parcours de santé peuvent aider au diagnostic précoce, mais également permettre d'évaluer ses chances de développer telle ou telle maladie et dès lors l'inciter à prendre des mesures en conséquence. L'intelligence artificielle se développe notamment en cancérologie. L'un des exemples les plus fréquemment mentionnés à cet égard est celui de Watson conçu par IBM. Watson analyse en effet les données génétiques des patients, les informations les concernant recueillies lors de leur admission, leur historique médical et les compare avec 20 millions de données issues d'études d'oncologie clinique pour établir un diagnostic et proposer un traitement. L'école de médecine de l'Université de Caroline du Nord a ainsi conduit en octobre 2016 une expérience montrant que les préconisations de Watson recoupaient les traitements prescrits par les cancérologues dans 99 % des 1 000 cas de cancer étudiés. Cette expérience a aussi démontré que dans 30 % des cas, Watson était à même de proposer davantage d'options thérapeutiques que les médecins[1]. Un autre exemple connu impliquant des algorithmes

(1) CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une république numérique, déc. 2017, p. 62 (www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf).

est celui de Sanofi et Google qui ont créé une entreprise commune qui utilise les données en temps réel sur l'état de santé d'un patient pour surveiller son taux de sucre et suggérer des actions aux patients diabétiques[2]. L'intérêt de l'application des algorithmes et de l'intelligence artificielle à la médecine réside également dans leurs capacités à traiter une masse d'informations scientifiques et de recherche qu'aucun médecin n'aurait matériellement la possibilité de maîtriser dans la perspective de formuler un diagnostic.

L'intelligence artificielle est aussi susceptible de fournir un appui à la veille sanitaire, les algorithmes étant particulièrement utiles pour « repérer l'élévation de l'incidence de maladies ou de comportements à risque, et alerter les autorités sanitaires »[3]. À titre d'exemple, en France, les liens entre l'utilisation d'une pilule contraceptive de troisième génération et le risque d'AVC ont pu être étudiés grâce au traitement algorithmique de la base du Système national des données de santé (SNDS)[4]. Plus récemment, l'utilisation des algorithmes dans le contexte de la crise sanitaire de la Covid-19 devrait permettre non seulement de réaliser des prévisions sur la propagation de la pandémie, mais qui plus est de repérer les patients atteints grâce au son de leur toux. Une équipe de chercheurs du *Massachusetts Institute of Technology* (MIT), aux États-Unis, a en effet mis au point un algorithme à même de poser un diagnostic sur la simple base d'extraits sonores. En analysant 5 000 enregistrements de toux, ce programme a repéré 98,5 % de malades de la Covid-19 présentant des symptômes. Plus étonnant encore, l'algorithme a repéré 100 % des malades asymptomatiques, dont le son de la toux est différent. Les chercheurs aimeraient que leurs travaux aboutissent à une application pour smartphone qui détecterait la Covid-19 instantanément en écoutant la toux. L'individu identifié comme porteur de la Covid-19 par l'application n'aurait alors plus qu'à se rendre en laboratoire pour qu'un résultat positif lui soit confirmé. Une telle application serait ainsi une véritable solution pour désemplir les laboratoires d'analyses médicales, aujourd'hui surchargés.

Il convient également de rappeler que les algorithmes sont à certains égards déjà bien implantés pour automatiser des tâches du quotidien. Les logiciels d'aide à la prescription (LAP), une fois une maladie déjà diagnostiquée, sont de précieux outils d'aide à la décision pour les médecins au moment de la saisie d'ordonnances. Ils permettent d'utiliser le dossier d'un patient pour repérer des contre-indications, des allergies ou des interactions médicamenteuses dangereuses[5].

Enfin, l'utilité de l'intelligence artificielle est aujourd'hui également mise en avant pour optimiser la mise en place d'essais cliniques grâce à une automatisation de la sélection des patients.

En somme, l'utilisation de l'intelligence artificielle et des algorithmes devient un véritable enjeu en matière de santé publique permettant de mieux répondre tant

(2) T. Schrepel et S. Gal Michal, « *Algorithms & Competition Law : Interview of Michal Gal by Thibault Schrepel* », *e-Competitions Special Issue Algorithms : Concurrences* 14 mai 2020, n° 93929.
(3) INSERM, Dossier d'information « Big data en santé », 2016 (www.inserm.fr/information-en-sante/dossiers-information/big-data-en-sante).
(4) CNIL, préc., p. 63.
(5) CNIL, préc., p. 63.

aux besoins des patients (plus de personnalisation) qu'à ceux des médecins (plus de sécurité), sans oublier ceux des instances publiques (plus de rationalisation). Ceci étant, qu'en est-il du côté des entreprises du secteur ?

La combinaison du *big data* avec des outils technologiquement avancés, tels que les algorithmes ou l'intelligence artificielle, est de plus en plus répandue au sein des entreprises, ce qui modifie la manière dont elles prennent des décisions commerciales et stratégiques.

**Toutefois, si l'utilisation généralisée de l'intelligence artificielle et des algorithmes est sans aucun doute associée à des gains d'efficacité importants (notamment en termes d'amélioration de l'automatisation, d'efficacité et de qualité), elle peut parallèlement susciter des inquiétudes au regard du droit de la concurrence.** Des comportements anticoncurrentiels ne pourraient-ils pas être facilités par l'utilisation des algorithmes et de l'intelligence artificielle ? Le recours à l'intelligence artificielle ne va-t-il pas favoriser les pratiques d'éviction ? De nouveaux acteurs vont ils plus facilement abuser de leur position dominante ? Quels seront les impacts sur le marché des rapprochements inévitables d'opérateurs ?

**Ces questions sont malgré tout bien connues et il convient dès lors d'apprécier dans quelle mesure l'analyse concurrentielle classique pourrait être remise en cause du fait de son application à ce domaine de l'intelligence artificielle appliquée à la santé.**

À cet égard, nous nous intéresserons tout d'abord aux éventuels comportements et risques anticoncurrentiels pouvant être associés à l'utilisation des algorithmes et de l'intelligence artificielle en matière de santé (Section 1), pour ensuite apprécier les problématiques juridiques soulevées par le recours à de telles technologies et les réponses apportées par les autorités de concurrence (Section 2).

SECTION 1

## INTELLIGENCE ARTIFICIELLE ET ALGORITHMES, QUELS RISQUES CONCURRENTIELS ?

Il ne fait aucun doute que les algorithmes et l'intelligence artificielle constituent un outil puissant permettant de valoriser la quantité croissante de données médicales collectées, en favorisant potentiellement l'efficacité du marché, l'innovation et même la concurrence. Néanmoins, chaque fois que de nouveaux outils technologiques révolutionnent profondément le mode de fonctionnement des entreprises et leurs interactions mutuelles, il existe un risque que certains acteurs du marché utilisent leur pouvoir accru pour atteindre des intérêts privés qui ne sont pas alignés sur les objectifs sociaux.

Il convient dès lors de s'intéresser aux risques concurrentiels inhérents à l'utilisation de l'intelligence artificielle et des algorithmes dans le domaine de la santé, dans les champs d'application classiques du doit de la concurrence que sont les ententes (§ 1), les abus de position dominante (§ 2), et enfin les concentrations (§ 3).

## § 1. – IA et algorithmes, quels risques concurrentiels au regard des pratiques d'ententes ?

Le traitement des données massives, les méthodes d'analyse de plus en plus fines et les systèmes d'intelligence artificielle peuvent aujourd'hui permettre aux opérateurs du marché de la santé de coordonner leurs comportements pour maximiser leur profit, et ce au détriment des patients-consommateurs. Une telle pratique est répréhensible au regard du droit des ententes. Rappelons en effet que tout accord ou pratique concertée entre entreprises, ayant un objet ou un effet anticoncurrentiel peut être sanctionné lorsqu'ils ont pour conséquence d'altérer l'incertitude dans laquelle l'entreprise doit se trouver pour **fixer de manière autonome sa politique commerciale**. Il peut s'agir par exemple d'un accord sur les prix, les volumes ou les marchés entre concurrents, mais aussi d'un échange d'informations sensibles, ou encore de la fixation du prix de revente ou d'obligations d'exclusivité avec les revendeurs.

Dans le domaine de la santé plus spécifiquement, tant l'intelligence artificielle que les algorithmes peuvent être utilisés, soit à l'appui d'un **équilibre collusif** pour créer ou maintenir une entente (i), soit comme **vecteur pour s'échanger des données** *a priori* non stratégiques mais qui peuvent finir par devenir cruciales lorsqu'elles sont couplées à d'autres données (ii).

(i) **Dans la première hypothèse, des entreprises concurrentes sur le marché de la santé qui auraient décidé de se coordonner pourraient être tentées de recourir aux algorithmes pour faciliter et sécuriser la mise en œuvre de leur collusion**.

On le sait, l'une des difficultés de la mise en œuvre d'un cartel réside dans le fait que les changements continus de l'offre et de la demande exigent des ajustements, notamment en termes de prix ou de production. Les entreprises, parties à l'entente, doivent alors fréquemment renégocier l'accord collusoire lors de réunions, d'appels téléphoniques, de courriels, autant d'instruments qui présentent un risque évident de détection par les autorités de concurrence[6]. La tentation peut alors être forte de recourir à une automatisation du processus de décision *via* des algorithmes, qui permettra ainsi une réaction automatisée des prix aux changements du marché sans qu'il soit nécessaire aux entreprises d'engager tout autre moyen de communication tels les échanges susvisés. Si le partage d'algorithmes de tarification avec des concurrents constitue une violation des règles de concurrence, il peut exister des moyens plus subtils de coordonner des comportements parallèles sans avoir à s'engager dans une communication explicite, comme en sous-traitant la création d'algorithmes aux mêmes sociétés informatiques et aux mêmes programmeurs par exemple[7].

Un autre rôle que peuvent avoir des algorithmes en tant que facilitateurs de collusion consiste à surveiller les actions des concurrents afin de faire respecter l'accord collusoire. Ce rôle peut inclure la collecte d'informations concernant les

(6) OCDE, *Algorithms and collusion : Competition Policy in the Digital Age*, 2017, p. 27.
(7) OCDE, préc., p. 28.

décisions commerciales des concurrents, le filtrage des données pour rechercher tout écart potentiel et, enfin, la programmation de représailles immédiates. Plus précisément, les données recueillies par les méthodes de collecte automatique sont contrôlées et combinées avec un algorithme de tarification qui se rétracte automatiquement en cas d'écart par rapport à un prix convenu[8].

Dans ces deux cas, que l'algorithme soit utilisé pour mettre en œuvre l'entente ou comme outil de surveillance, il n'élimine souvent pas la nécessité d'une communication explicite lors de l'établissement et de la mise en œuvre de l'entente. Or si les algorithmes peuvent être utilisés pour faciliter une collusion et la stabiliser, une préoccupation particulière tient également en leur capacité de permettre de nouvelles formes de coordination qui n'étaient pas observées auparavant. C'est ce que l'on appelle la « collusion algorithmique »[9].

À l'heure actuelle, de nombreuses entreprises s'appuient sur l'intelligence artificielle pour développer des algorithmes de maximisation des bénéfices. Ces algorithmes, dotés d'une puissante capacité de prédiction, étudient le marché, apprennent d'eux-mêmes au fur et à mesure des interactions passées et se réadaptent constamment aux actions des autres acteurs du marché, qu'il s'agisse d'êtres humains ou d'agents artificiels. Bien que ces algorithmes soient programmés individuellement pour jouer le jeu de la concurrence dans une logique unilatérale non coopérative, dès lors que plusieurs entreprises recourent à ce type d'algorithmes, les intelligences artificielles apprennent réciproquement les unes des autres et anticipent les agissements des concurrents. Ainsi, au fur et à mesure de leurs interactions sur le marché, leurs comportements vont finir par s'aligner jusqu'à atteindre un équilibre tacitement collusoire, sans avoir été programmés pour le faire et donc sans qu'aucune intervention humaine ne soit nécessaire. Il y a là un risque concurrentiel indéniable dont il conviendra d'apprécier le traitement par les autorités de concurrence (*infra*).

(ii) **Dans la seconde hypothèse, des risques concurrentiels peuvent également apparaître lorsque les algorithmes sont utilisés comme vecteur pour s'échanger des données.**

De fait, les algorithmes ont aujourd'hui besoin d'être entraînés sur de grandes quantités de données pour établir des liens entre les différentes variables incluses dans l'analyse, et ainsi s'améliorer. Les entreprises peuvent alors être tentées de s'échanger mutuellement des données passées, non sensibles, pour développer la performance de leurs algorithmes. Cependant, un tel échange de données peut être susceptible de créer une forme de coordination et d'homogénéisation dans l'apprentissage d'algorithmes concurrents[10]. En outre, on peut craindre qu'un partage de données soit constitutif d'une restriction de la concurrence s'il conduit à aligner de manière significative les coûts ou les caractéristiques des produits des concurrents, limitant ainsi la concurrence sur le prix, la qualité ou l'innovation[11]. En matière de santé par exemple, si le fait que deux laboratoires

(8) OCDE, préc., p. 26-27.
(9) OCDE, préc., p. 19.
(10) L. Arcelin, *Le droit de la concurrence mis à l'épreuve par le numérique : JCP* A 7 nov. 2019, n° 45, 1493, § 30.
(11) Commission européenne, Rapport Crémer, *Competition policy for the digital era*, 2019, p. 96-97.

partagent leurs données sur des patients ou des pathologies en vue d'accroître la qualité de leurs produits innovants ne semble à première vue pas soulever de problèmes au regard d'une éventuelle coordination, il en va différemment dès lors que cette mise en commun décourage les concurrents de se différencier et d'améliorer leur propre collecte de données. Dans un tel cas, le partage des données peut avoir un impact sur les incitations à s'engager dans le traitement indépendant des données, et la concurrence dans le domaine de l'analyse des données peut être compromise(12).

Par ailleurs, les données ne sont pas seulement une matière première pour entraîner les algorithmes ou développer de nouveaux produits. Leur contenu informationnel peut également transformer un accord de partage ou de mise en commun de données en un véhicule pour l'échange de données commercialement sensibles telles que les coûts ou les prix(13). Ceci d'autant plus que des données qui peuvent paraître comme non stratégiques *a priori* à un instant donné peuvent le devenir si les algorithmes qui leur sont appliqués permettent d'établir des liens entre ces données « non stratégiques » et d'autres données considérées comme plus sensibles qui pourraient *in fine* en être inférées(14).

## § 2. – IA et algorithmes, quels risques concurrentiels au regard des pratiques constitutives d'abus de position dominante ?

L'intelligence artificielle et les algorithmes peuvent être également l'instrument de pratiques d'abus de position dominante. Dans une telle hypothèse, ils peuvent être mobilisés pour opérer une différenciation tarifaire (abus d'exploitation) ou encore pour évincer les concurrents (abus d'exclusion) *via* un refus d'accès aux données ou un accès discriminatoire, des contrats exclusifs, ou encore des ventes liées de données ou une utilisation croisée de celles-ci.

### I. – Abus d'exploitation

De manière générale, l'intelligence artificielle s'améliore et devient plus performante par l'analyse de données. En conséquence, les données sont aujourd'hui devenues une véritable matière première pour les entreprises qui cherchent à s'affirmer sur le marché et à rester compétitives. Toutefois, l'accès facilité de certaines entreprises à d'importantes bases de données peut parfois se traduire par des risques d'abus d'exploitation dès lors que les entreprises utilisent ces données pour renforcer leur pouvoir de marché et influencer la structure du marché.

En effet, en collectant des données sur leurs clients, les entreprises peuvent obtenir des informations sur leurs habitudes d'achat et ainsi évaluer leur propension

(12) *Ibid*.
(13) *Ibid*., p. 96, b), § 2.
(14) L. Arcelin, préc., § 30.

à payer pour l'achat d'un bien ou d'un service. Or, dans l'hypothèse où ces entreprises détiennent un certain pouvoir de marché, elles sont alors à même d'utiliser ces données comme vecteur de **discrimination tarifaire**, en les utilisant pour fixer des prix différents selon les groupes de clients qu'elles auront identifiés grâce aux données(15).

Appliqué à la santé, on peut imaginer qu'une plateforme combinant de grandes masses de données médicales sur des patients à un algorithme de prix pourrait conduire à une discrimination tarifaire et à une personnalisation des offres pour chaque patient en fonction des données détenues sur son état de santé. À cet égard, il est notamment possible de s'interroger sur l'utilisation future qui sera faite de la plateforme de partage des données *Health Data Hub*, qui a pour mission de permettre de croiser les bases de données de santé issues des organismes publics de santé tels que l'assurance maladie et les hôpitaux et de faciliter leur utilisation par les équipes de recherche et de développement. Car si cette plateforme a pour but de permettre au secteur de la santé d'exploiter le potentiel de l'intelligence artificielle en mettant à disposition des chercheurs d'immenses volumes de données nécessaires au développement de modèles d'intelligence artificielle, dès lors que les entreprises pourront se voir accorder un droit d'accès aux données par la CNIL quand leur projet de recherche présentera un intérêt général, il conviendra de veiller à ce qu'elles ne puissent utiliser ces données pour un tout autre usage, moins vertueux.

La personnalisation algorithmique pourrait également à terme soulever un risque en matière d'assurance. Il est en effet possible d'imaginer dans un futur proche un scénario de tarification des assurances basée sur les données de santé, dans lequel les patients se verraient payer des cotisations d'assurance adaptées à leur état de santé et donc plus onéreuses s'ils ont une forte propension à être malade. Si à l'heure actuelle la tarification basée sur les données médicales est interdite par la loi Évin(16), une étude réalisée pour France Mutuelle par OpinionWay en 2017 pointe le fait qu'une majorité des Français âgés de cinquante-cinq ans et plus craignent « que les assureurs et les mutuelles aient un jour accès à leurs données de santé et s'en servent pour adapter leurs cotisations à leur état de santé »(17). Ceci conduirait alors à une discrimination entre les « bons risques » et les « mauvais risques », qui a des effets ambigus en termes concurrentiels. S'il est vrai qu'une telle situation permettrait un gain net de bien-être social dans la mesure où le prix s'ajusterait aux besoins de soins de chaque patient, il n'en demeure pas moins que l'assureur pourrait alors maximiser son profit en utilisant son pouvoir de marché

(15) Autorité de la concurrence et Bundeskartellamt, rapport « Droit de la concurrence et données », 10 mai 2016, p. 23-24, c).

(16) L. n° 89-1009, 31 déc. 1989 renforçant les garanties offertes aux personnes assurées contre certains risques, art. 6, al. 2 et 3 (www.legifrance.gouv.fr).

(17) Sondage OpinionWay pour France Mutuelle, « Qu'attendent les séniors de leur complémentaire santé ? », 2017 (www.francemutuelle.fr/particuliers/mutuelle-plus-quun-mot/quattendent-seniors-de-complementaire-sante/). L'étude a été réalisée auprès d'un échantillon de 1 016 personnes représentatif de la population française âgée de cinquante-cinq ans et plus, constitué selon la méthode des quotas, au regard des critères de sexe, d'âge, de catégorie socioprofessionnelle et de région de résidence. Les interviews ont été réalisées du 10 au 15 mai 2017 par questionnaire autoadministré en ligne (515 personnes) sur système CAWI (*Computer Assisted Web Interview*) et par téléphone (501 personnes) sur système CATI (*Computer Assisted Telephone Interview*).

pour s'accaparer la totalité du surplus du patient-consommateur[18]. Dans une telle situation, le prix ne serait donc plus corrélé au marché mais dépendrait en réalité de l'état de santé du patient et surtout du pouvoir de marché de l'assureur et de la capacité de son intelligence artificielle à analyser les données de santé.

## II. – Abus d'exclusion

Dans le domaine des abus de position dominante, l'intelligence artificielle et les algorithmes peuvent également être mis en cause dans des abus d'éviction. Il s'agit de pratiques unilatérales par lesquelles un opérateur dominant entrave l'accès au marché d'un concurrent potentiel ou évince ses concurrents actuels en utilisant le levier de sa position de marché[19]. Cette tentative d'éviction peut se faire *via* un refus d'accès aux données ou un accès discriminatoire, des contrats exclusifs, ou encore des ventes liées de données ou une utilisation croisée de celles-ci. De telles pratiques viennent alors affaiblir la concurrence sur le marché, au détriment des consommateurs.

Pour illustrer ce type de pratiques, on pense tout d'abord au **refus d'accès aux données** ou encore à celui d'un **accès discriminatoire**. Conformément à la pratique décisionnelle des autorités de concurrence, le refus d'accès aux données est anticoncurrentiel si ces données constituent une facilité essentielle à l'activité de l'entreprise qui cherche à y accéder. La Cour de justice de l'Union européenne a toutefois circonscrit l'accès obligatoire aux facilités essentielles à un nombre limité de cas, étant entendu que, même dominante, une entreprise ne peut, en principe, être obligée de favoriser l'activité de ses concurrents[20]. D'ailleurs, l'arrêt *IMS Health*[21] pose les conditions cumulatives nécessaires pour que le refus d'accès soit constitutif d'un abus de position dominante. En l'espèce, l'entreprise IMS Health avait pour activité le suivi des ventes dans le secteur des produits pharmaceutiques en Allemagne, et fournissait à ce titre aux laboratoires des données sur leurs ventes régionales de produits pharmaceutiques. Pour ce faire, IMS avait développé une structure modulaire de restitution des données pharmaceutiques collectées qui avait été élaborée en étroite collaboration avec les laboratoires clients d'IMS, afin que cette structure corresponde parfaitement à leurs attentes. Forte de son succès, cette structure modulaire est devenue une sorte de standard sur le marché, à tel point que les entreprises concurrentes d'IMS lui demandaient de leur concéder une licence de cette structure. IMS a clairement refusé, et s'est alors posé la question de l'utilisation abusive ou non de sa structure modulaire pour exclure la concurrence sur le marché de la fourniture de données de ventes. La Cour de justice de l'Union européenne est venue préciser que ce refus opposé par une entreprise en position dominante d'octroyer une licence sur cette structure modulaire à une autre

(18) F. Marty, *Algorithmes de prix, intelligence artificielle et équilibres collusifs : RID éco.* 2017/2, t. XXXI, p. 84, § 3 (www.cairn.info/revue-internationale-de-droit-economique-2017-2-page-83.htm). Autorité de la concurrence et Bunderskartellamt, préc., p. 24-25. V. égal. CNIL, *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, préc., p. 38.

(19) F. Marty, préc., p. 89, § 2.

(20) Autorité de la concurrence & Bundeskartellamt, rapport « Droit de la concurrence et données », préc., p. 20. V. égal. Commission européenne, Rapport Crémer, préc., p. 101, 2).

(21) CJCE, arrêt, 29 avr. 2004, C-418/01, *IMS Health*, dispositif, 2).

entreprise souhaitant également fournir de telles données, constituait un abus de position dominante à condition que (i) la structure modulaire soit indispensable à l'exploitation de l'activité en question, (ii) que le refus d'accès empêche l'émergence d'un nouveau produit ou service pour lequel il existe une demande potentielle, (iii) qu'il ne soit pas justifié par des considérations objectives, et (iv) qu'il soit susceptible d'exclure toute concurrence sur le marché concerné.

Par ailleurs, en dehors du cas d'une facilité essentielle, un refus d'accès à une base de données, même implicite[22], opposé de manière discriminatoire par une entreprise en position dominante peut constituer un abus de position dominante dès lors qu'il fausse de manière sensible le jeu de la concurrence[23]. Dans le domaine de la santé, l'affaire *Cegedim* en est une illustration[24]. Cette société, principal fournisseur sur le marché des bases de données d'informations médicales en France, propose aux laboratoires à la fois une base de données médicales et un logiciel de gestion de clientèle. Elle a été sanctionnée en 2014 à hauteur de 5,7 millions d'euros pour avoir refusé de vendre sa base de données OneKey – la référence du secteur – aux laboratoires utilisant le logiciel de gestion de son concurrent Euris, alors même qu'elle acceptait de la vendre à des laboratoires ayant recours à d'autres logiciels concurrents. Ici, l'Autorité de la concurrence a considéré que cette pratique était purement discriminatoire puisqu'elle visait à faire perdre à Euris toute possibilité de se développer sur le marché des logiciels de gestion. Euris a d'ailleurs perdu 70 % de sa clientèle sur la période concernée par la pratique.

Les risques anticoncurrentiels basés sur les données et leur exploitation *via* l'intelligence artificielle et les algorithmes peuvent également inclure les pratiques visant à limiter l'accès des concurrents aux données de tierces parties au moyen d'**exclusivités** avec les prestataires les fournissant[25]. Prenons, pour les seuls besoins de notre explication, le cas du partenariat de collaboration établi entre Google et Sanofi en juin 2019 *via* la création d'un laboratoire virtuel d'innovation en santé. Le premier groupe pharmaceutique français et le géant mondial du numérique se sont associés pour développer de futurs médicaments et services en tirant parti des technologies de données. Plus précisément, il s'agit, selon Ameet Nathwani, responsable des affaires médicales et du numérique chez Sanofi, de combiner « les innovations biologiques et données scientifiques de Sanofi avec les capacités de premier ordre de Google, de l'informatique en *cloud* jusqu'à l'intelligence artificielle de pointe »[26]. Concrètement, cette collaboration vise à changer la manière dont Sanofi développe de nouveaux traitements, avec trois grands objectifs : mieux comprendre les patients grâce à une analyse poussée de leurs données, améliorer leur expérience avec des produits et services plus personnalisés et accroître l'efficacité opérationnelle du groupe. Pour remplir ce dernier objectif, Sanofi compte notamment

(22) Comm. CE, *Orientations sur les priorités retenues pour l'application de l'article 82 du Traité CE aux pratiques d'éviction abusive des entreprises dominantes*, 2009, § 79.

(23) Aut. conc., déc. n° 14-D-06, 8 juill. 2014, relative à des pratiques mises en œuvre par la société *Cegedim* dans le secteur des bases de données d'informations médicales, § 192 et s.

(24) Aut. conc., déc. n° 14-D-06, préc., § 211 à 220.

(25) Autorité de la concurrence et Bundeskartellamt, rapport « Droit de la concurrence et données », préc., p. 22.

(26) SANOFI, Communiqué de presse, *Sanofi et Google vont développer un nouveau laboratoire d'innovation en santé*, 18 juin 2019.

recourir à des techniques d'intelligence artificielle de Google afin d'établir de meilleures projections des ventes de ses traitements et répercuter ces enseignements sur ses activités commerciales et logistiques. On peut ici imaginer que pour établir les projections des ventes des traitements, Sanofi fasse appel aux requêtes saisies en rapport aux pathologies soignées par ces traitements par les internautes sur Google afin d'obtenir de véritables prédictions épidémiologiques. Si une exclusivité devait alors être accordée, à l'un des *leaders* mondiaux de la santé, sur l'exploitation des requêtes saisies (ce qui n'est pas le cas, notre exemple étant pris pour la seule démonstration de notre propos), une telle exclusivité serait sans doute considérée comme constitutive d'un abus de position dominante puisqu'elle n'aurait d'autre but que de verrouiller le marché pour évincer les concurrents.

Enfin, les données collectées sur un marché peuvent également être utilisées par une entreprise pour développer ou accroître son pouvoir de marché sur un autre marché de manière anticoncurrentielle(27). À cet égard, l'autorité de concurrence britannique a évoqué la possibilité que des entreprises tirent parti des données contrôlées sur certains marchés pour renforcer leur pouvoir sur d'autres marchés connexes, à l'aide de stratégies de **ventes groupées ou liées** par lesquelles elles regroupent l'achat d'un service vendu sur un marché avec un autre service vendu sur un marché connexe(28). À titre d'exemple, une entreprise disposant d'un important pouvoir de marché obtenu grâce à la création d'une série de données peut chercher à pénétrer le marché de l'analyse de données en liant nécessairement l'achat de ses séries de données à l'utilisation de ses propres services d'analyse, soit par une vente groupée pure (obligation pour les clients d'acheter les deux ensemble), soit par une vente groupée technique (la vente est liée du fait de l'intégration de la base de données dans le logiciel d'analyse), soit enfin par une vente groupée mixte (en proposant les deux produits à de meilleures conditions que celles proposées si les produits sont achetés séparément). S'il est vrai que dans certains cas, la vente groupée ou liée peut engendrer des gains d'efficience, tant pour les entreprises que pour les consommateurs, il n'en demeure pas moins que dans d'autres circonstances, elle pourrait nuire à la concurrence, et ce dès lors qu'elle est susceptible d'évincer les entreprises rivales du marché ou qu'elle supprime les incitations à l'entrée de nouvelles entreprises sur le marché (car elles ne peuvent pas être compétitives sans fournir la gamme complète des services fournis par l'entreprise puissante sur le marché).

De manière plus générale, l'Autorité de la concurrence française est venue insister dans un avis de 2010 sur le fait que **l'utilisation croisée de données**, autrement dit l'utilisation sur un marché de données collectées sur un autre marché, peut, dans certains cas, engendrer des effets de forclusion(29).

(27) Autorité de la concurrence et Bundeskartellamt, préc., p. 22.
(28) Competition and Markets Authority, *The Commercial Use of Consumer Data*, 2015, p. 90. V. égal. OCDE, Direction des affaires financières et des entreprises – Comité de la concurrence, *Données massives : adapter la politique de la concurrence à l'ère du numérique*, Note de référence du Secrétariat, nov. 2016, § 68.
(29) Aut. conc., avis n° 10-A-13 sur l'utilisation croisée des bases de clientèle.

## § 3. – IA et algorithmes, quels risques concurrentiels du fait des concentrations d'entreprises ?

Lorsque les données confèrent des avantages concurrentiels significatifs à leurs propriétaires en leur permettant notamment d'entraîner leurs algorithmes et de développer leurs intelligences artificielles, les entreprises cherchent alors à acquérir davantage de données et à mieux les analyser ou les exploiter pour rester compétitives sur le marché. Pour ce faire, l'une des stratégies envisageables est d'acquérir d'autres entreprises possédant d'importantes bases de données et des technologies de pointe permettant de les analyser, ou de fusionner avec elles. Ceci étant, de telles concentrations nécessitent parfois d'être examinées sous l'angle du droit de la concurrence.

En effet, comme l'a affirmé la commissaire chargée de la politique de concurrence au sein de l'Union européenne, M^me^ Margrethe Vestager, « les données sont des éléments essentiels de l'économie numérique. C'est pourquoi nous devons soigneusement examiner les opérations qui débouchent sur l'acquisition de jeux de données importants, notamment de données potentiellement commercialement sensibles, afin de veiller à ce qu'elles ne restreignent pas la concurrence »[(30)]. Le secteur de la santé, tout particulièrement, se caractérise par une forte capacité d'innovation continue et compte dans ses rangs des champions d'envergure mondiale ainsi qu'un important tissu de *startups* et de PME[(31)]. L'acquisition de ces *startups* aux bases de données croissantes et aux intelligences artificielles performantes par les opérateurs dominants du marché constitue alors un moyen efficace pour ces derniers de maintenir leur position de marché, tout en intégrant un futur concurrent[(32)].

Dans de nombreux cas, de telles acquisitions peuvent être pro-concurrentielles. De manière générale, la recherche des limites optimales de l'entreprise – que ce soit par croissance interne ou externe – est une partie importante du processus concurrentiel[(33)]. Dans le domaine du numérique plus particulièrement, les fusions-acquisitions entre des entreprises établies et des jeunes pousses peuvent souvent générer des synergies et des gains d'efficience substantiels. En effet, alors que la *startup* peut apporter des données en masse et des technologies innovantes, l'entreprise établie possède généralement les compétences, les atouts, et surtout les ressources financières nécessaires au déploiement de ces technologies et à la fourniture de nouveaux produits ou services. Dans le domaine de la santé, la recherche pharmaceutique peut par exemple être encouragée par la fusion entre un laboratoire et une *startup* spécialisée en intelligence artificielle qui permet, grâce à sa technologie, d'optimiser l'identification de nouvelles cibles et cellules thérapeutiques. Cependant, il ne faut pas oublier qu'acquérir des structures prometteuses peut avoir pour effet

(30) M. Vestager, Communiqué de presse de la Commission européenne, *Concentrations : la Commission autorise le rachat de Shazam par Apple*, 6 sept. 2019.
(31) Ministère de l'Économie et des Finances, Études économiques, Synthèse « Prospective : Industrie du futur – Enjeux et perspectives pour la filière industries et technologies de santé », 2019, p. 3.
(32) L. Arcelin, *Le droit de la concurrence mis à l'épreuve par le numérique*, préc., § 42.
(33) Commission européenne, Rapport Crémer, préc., p. 111, § 1.

de réduire la concurrence sur le marché par la disparition d'un acteur indépendant. Les entreprises établies sur le marché peuvent en effet décider d'acquérir des entités innovantes dans l'objectif d'éliminer ces dernières qui, malgré un faible pouvoir de marché, risquent de représenter une concurrence réelle dans le futur. Il s'agit alors d'une acquisition prédatrice (ou *killer acquisition*) qui n'a d'autre finalité que d'éviter un effet de substitution[34], tout en augmentant la concentration des données ou des technologies et en empêchant les concurrents d'y avoir accès[35]. Ce type d'acquisition est particulièrement pratiqué dans les secteurs pour lesquels l'innovation occupe une place prépondérante, comme les secteurs pharmaceutique ou numérique. En réduisant ainsi la pression concurrentielle sur le marché, l'entreprise issue de la concentration renforce son pouvoir de marché et peut alors se permettre d'augmenter ses propres prix, en particulier lorsque le marché présente de fortes barrières à l'entrée et un faible nombre d'opérateurs. Cela peut également inciter les concurrents à réagir, en augmentant à leur tour leurs prix, ce qui conduit alors à une hausse inévitable des prix sur le marché dans son ensemble[36]. En outre, au-delà même de la question tarifaire, une fusion-acquisition peut également avoir un impact négatif sur l'incitation à innover des concurrents. À titre d'illustration, le rachat annoncé fin 2019 de Fitbit par Google est particulièrement évocateur de ce phénomène de *killer acquisition*. Fitbit est une société américaine innovante spécialisée dans la conception, le développement et la commercialisation des moniteurs d'activité physique et montres connectées. Son rachat par la société Google offrirait donc à cette dernière une importante quantité de données de santé (nombre de pas, fréquence cardiaque, temps de sommeil, cycles menstruels et informations de localisation), ce qui a suscité l'inquiétude du Bureau européen des unions de consommateurs (BEUC) qui considère que l'accord projeté « représente un cas d'école en ce qui concerne l'analyse des effets que l'accumulation de données peut avoir sur la concurrence »[37]. C'est d'ailleurs la raison pour laquelle il a demandé à la Commission européenne un examen approfondi du rachat. En particulier, le BEUC voyait dans ce rachat l'opportunité pour Google d'éliminer un concurrent potentiel. Il craignait ainsi que Google n'exploite les données collectées par Fitbit à son avantage pour imposer une position dominante sur divers marchés, ce qui entraînerait à terme des dommages à la concurrence en l'empêchant de créer les conditions d'un marché concurrentiel sain, limitant l'innovation et augmentant les prix sur divers marchés, dont celui de la santé. La Commission a toutefois décidé d'approuver l'opération en décembre 2020, après avoir obtenu des engagements de la part de Google, notamment sur la question des données personnelles : « Nous pouvons approuver le projet d'acquisition de Fitbit par Google parce que les engagements garantiront que le marché des objets connectés et le secteur naissant de la e-santé resteront ouverts et concurrentiels. Ces engagements déterminent comment Google peut utiliser les données recueillies à des fins publicitaires, comment

(34) Commission européenne, Rapport Crémer, préc., p. 117, *d)*.
(35) Autorité de la concurrence et Bundeskartellamt, préc., p. 18, 3-a)-§ 2 et p. 19, § 2.
(36) Commission européenne, Rapport au Conseil et au Parlement européen, *Application du droit de la concurrence dans le secteur pharmaceutique (2009-2015)*, p. 28, 4.4.1.
(37) BEUC, *Google-Fitbit merger : Competition concerns and harms to consumers*, 7 mai 2020.

l'interopérabilité entre les objets connectés concurrents et Android (son système d'exploitation mobile) sera sauvegardée, et comment les utilisateurs peuvent continuer à partager des données touchant à leur santé et forme physique s'ils le décident », a déclaré Margrethe Vestager, vice-présidente de la Commission européenne en charge de la concurrence[38].

## Conclusion de la section 1

Les risques concurrentiels qui peuvent être associés à l'utilisation de l'intelligence artificielle et des algorithmes en matière santé sont donc nombreux. Se pose alors la question des réponses adressées par les autorités de concurrence pour y faire face.

SECTION 2

# INTELLIGENCE ARTIFICIELLE ET ALGORITHMES, QUELLES RÉPONSES DES AUTORITÉS DE CONCURRENCE ?

L'utilisation de l'intelligence artificielle et des algorithmes modifie profondément l'approche des marchés, ce qui soulève des problématiques juridiques lorsqu'il est question d'y appliquer le droit de la concurrence (§ 1). Face à des dernières, quelles solutions les autorités de concurrence peuvent-elles développer pour maîtriser les risques concurrentiels (§ 2) ?

## § 1. – Les problématiques rencontrées face à l'intelligence artificielle et aux algorithmes

La croissance actuelle de l'utilisation des algorithmes, combinée aux développements de l'intelligence artificielle, a induit de nombreux changements sur les marchés numériques et alimente aujourd'hui un large débat sur leurs implications pour les autorités de concurrence dans l'application du droit de la concurrence.

Tout d'abord, apprécier l'incidence d'une pratique sous l'angle concurrentiel présuppose de **délimiter le marché pertinent** sur lequel analyser les effets de cette pratique. Or, identifier des marchés bien définis dans un contexte d'économie numérique peut s'avérer complexe compte tenu du fait que les frontières des marchés sont amenées à changer très rapidement, ce qui les rend beaucoup moins claires que ce qu'elles pouvaient être dans l'économie traditionnelle[39]. En effet, l'environnement dynamique des marchés influe sans cesse sur les besoins

(38) M. Vestager, Communiqué de presse de la Commission européenne, *Concentrations : la Commission autorise l'acquisition de Fitbit par Google sous certaines conditions*, 17 déc. 2020.
(39) Commission européenne, rapport Crémer, préc., p. 3-4 et p. 46-47.

des consommateurs, ce qui se traduit par une demande constamment changeante et donc par une perception très volatile à l'égard de ce qui peut ou non être considéré comme un substitut viable à tel ou tel produit pour répondre à un besoin particulier.

Parallèlement, **le pouvoir de marché** qui a une influence sur l'appréciation du caractère anticoncurrentiel de la pratique devient de plus en plus difficile à évaluer. En particulier, la collecte et la détention de données massives peuvent constituer une importante source de pouvoir de marché[40], qu'il est difficile de chiffrer et de traduire en parts de marché. Ceci s'illustre particulièrement en matière de contrôle des concentrations où l'analyse traditionnelle des seuils de contrôlabilité d'une opération est remise en cause par l'émergence et l'importance des données. Traditionnellement, les autorités de concurrence européenne et française appliquent des seuils de contrôlabilité basés sur le chiffre d'affaires des entreprises concernées par l'opération pour isoler les concentrations qui peuvent soulever des problèmes de concurrence et qui doivent, de fait, être portées à la connaissance de l'autorité compétente. Néanmoins, dans le contexte numérique actuel, de tels seuils ne sont pas toujours pertinents, compte tenu du fait que le potentiel concurrentiel d'une entreprise ne se reflète plus seulement dans son chiffre d'affaires. Désormais, les actifs d'une entreprise comptent, qu'il s'agisse de sa clientèle ou d'une série de données, au même titre que sa capacité d'innovation[41]. Ainsi, continuer d'adopter une approche basée uniquement sur les effets d'une opération en termes de chiffre d'affaires risque de conduire à l'approbation sans conditions d'opérations pourtant susceptibles d'avoir de lourdes incidences sur la concurrence à l'avenir. Tel est d'ailleurs le cas de nombreuses *killer acquisitions* dans le secteur du numérique, qui n'ont que peu de fois été soumises aux instances de contrôle parce que le chiffre d'affaires de la *startup* cible n'était pas suffisant pour atteindre les seuils, alors même que le montant de la transaction était conséquent[42].

Par ailleurs, sanctionner une pratique nécessite d'en **qualifier** son **caractère anticoncurrentiel**, ce qui peut s'avérer complexe lorsque algorithmes, données, et intelligence artificielle interviennent.

En matière **d'entente** tout d'abord, la caractérisation d'un accord de volonté ou d'une pratique concertée peut être difficile à apporter lorsqu'il n'y a pas d'échanges directs entre les concurrents et que la collusion est le fait d'un algorithme autonome. La spécificité de ce type d'algorithme tient à leur capacité à s'autonomiser de leur codage initial *via* l'expérience qu'ils accumulent au travers des interactions de marché[43]. Ainsi, le code informatique initial ne peut constituer une preuve d'une stratégie collusive. Parallèlement, la compréhension de son processus de raisonnement interne et donc l'explication des décisions en termes de finalité sont particulièrement difficiles compte tenu du fait que ces algorithmes reposent sur des architectures comparables à des réseaux neuronaux composés de nombreuses interconnexions, ce qui en fait une véritable « boîte noire » pour

(40) Autorité de la concurrence et Bundeskartellamt, préc., p. 13.
(41) OCDE, *Données massives : adapter la politique de la concurrence à l'ère du numérique*, préc., § 61.
(42) L. Arcelin, préc., § 42.
(43) F. Marty, préc., p. 99.

les observateurs extérieurs[44]. De la même manière, se pose la question de la frontière entre parallélisme de comportements et collusion. De nombreux algorithmes ont aujourd'hui la tâche d'analyser le marché et d'y agir pour maximiser le profit individuel de leur propriétaire. Ceci étant, compte tenu du fait que l'algorithme autonome apprend des interactions passées et du marché, il va s'y adapter instantanément. Or dans l'hypothèse où plusieurs intelligences artificielles sont programmées de la sorte sur le marché, au-delà même d'apprendre des interactions du marché, elles apprennent aussi les unes des autres et anticipent les comportements des concurrents sans pour autant perdre leur indépendance puisqu'elles ont été programmées dans une logique unilatérale non coopérative[45]. Dès lors, une telle situation pourrait conduire à un équilibre de maximisation du profit conjoint sans qu'il n'y ait pour autant ni accord entre concurrents ni intention coopérative. Il sera alors particulièrement complexe pour l'autorité de concurrence de déterminer s'il s'agit d'un parallélisme de comportements licite ou d'une collusion illicite résultant de l'intervention de l'intelligence artificielle.

Sous l'angle des **abus de position dominante**, la théorie des facilités essentielles peut être difficile à mobiliser lors d'un refus d'accès à des données, ce qui rend plus difficile de sanctionner un refus d'accès au caractère purement anticoncurrentiel. En effet, comme l'a rappelé la Commission européenne, dans le cadre du test des facilités essentielles, une entreprise qui occupe une position dominante dans la fourniture d'une installation, d'un produit ou d'un service indispensable pour concurrencer sur un marché en aval, abuse de sa position dominante lorsque, sans justification objective, elle refuse l'accès à cette installation, produit ou service, ce qui a pour effet d'éliminer toute concurrence effective sur un marché aval[46]. Or en matière de données, il faut reconnaître que celles-ci sont très hétérogènes et qu'elles peuvent être utilisées à des fins très diverses. Ainsi, contrairement aux demandes d'accès aux infrastructures (qui ont une finalité clairement identifiable et dont les conditions d'accès, bien qu'elles puissent être complexes, peuvent être normalisées), chaque demande d'accès aux données pourrait nécessiter une analyse séparée pour chaque objectif poursuivi, et donc la définition d'un marché pertinent différent, afin de déterminer si un refus d'accès constituerait un abus[47]. Cependant, une telle analyse au cas par cas, très coûteuse, ne peut être exigée de la part des entreprises détentrices des données pour prouver que ce refus est ou non justifié. De la même manière, l'évaluation d'un refus d'accès opposé de manière discriminatoire à une base de données doit reposer sur le caractère essentiel des données sur les marchés voisins. Or la Commission constate qu'il peut être difficile d'appliquer l'article 102 du TFUE à un refus d'accès aux données adressé à des demandeurs qui cherchent à y accéder à des fins étrangères au marché sur lequel leur titulaire est actif[48]. De même, l'abus ne saurait être retenu si l'application du simple

(44) F. Marty, préc., p. 100.
(45) F. Marty, préc., p. 99 et p. 93 et T. Titone, *Intelligence artificielle et droit de la concurrence : Rev. Lamy dr. aff.* 1er sept. 2019, n° 151, I-b).
(46) Commission européenne, Rapport Crémer, préc., p. 98-99.
(47) Commission européenne, Rapport Crémer, préc., p. 100.
(48) Commission européenne, Rapport Crémer, préc., p. 100.

droit à la portabilité des données, consacré à l'article 20 du RGPD, suffit à accéder à celles-ci[49].

En matière de **concentration**, il n'est par ailleurs pas toujours facile d'identifier le préjudice anticoncurrentiel que peut induire une opération et de le distinguer des effets pro-concurrentiels. En effet, au moment de la réalisation de la concentration, il se peut qu'il n'y ait pas encore de chevauchement substantiel entre le marché « principal » dominé par l'acquéreur et le marché distinct – mais généralement lié – sur lequel est présente l'entreprise cible[50]. En outre, si l'élimination de la concurrence potentielle peut suffire à soulever des problèmes de concurrence, il peut être difficile de prouver l'existence d'une concurrence potentielle future avec un degré suffisant de certitude. Face à des risques non encore avérés et à des dommages éventuels difficiles à mesurer, une intervention trop précoce pourrait entraver indûment le processus de concurrence, ceci d'autant plus lorsque l'intégration de produits ou d'activités complémentaires peut être considérée comme ayant des effets pro-concurrentiels[51].

Une autre difficulté qui se pose lors de l'application du droit de la concurrence est celle de **l'imputation de l'infraction anticoncurrentielle** lorsque l'intelligence artificielle est en jeu. À mesure que l'intelligence artificielle se développe, les liens entre l'algorithme et l'homme s'affaiblissent et la capacité des algorithmes à adapter de manière autonome leur comportement met en cause la responsabilité des entreprises qui en bénéficient. Cependant, pour engager la responsabilité de ces entreprises, encore faut-il démontrer que le comportement anticoncurrentiel aurait pu être anticipé ou prédéterminé. Pour ce faire, il faut analyser les instructions programmées de l'algorithme, les garanties disponibles, la structure de récompense, la portée des activités et s'attacher à examiner dans quelle mesure les hommes peuvent contrôler les activités des algorithmes[52]. Néanmoins, lorsque l'algorithme échappe totalement à son concepteur et adapte de manière autonome son comportement sur le marché, qui peut en être tenu pour responsable : son concepteur, l'entreprise qui en est propriétaire, celle qui en bénéficie ? Faut-il leur imputer une responsabilité automatique conjointe et solidaire ? Ces questions n'ont à ce jour pas de réponses claires, mais seront probablement soulevées devant les tribunaux à mesure qu'un plus grand nombre d'affaires impliquant des activités algorithmiques seront jugées.

Enfin, la place des algorithmes et de l'intelligence artificielle dans l'initiation de pratiques anticoncurrentielles pose des questions sur **l'aspect dissuasif des sanctions infligées**. Si l'algorithme ne fait souvent que remplacer l'humain, à l'inverse de ce dernier il ne connaît pas la crainte d'une sanction financière. Et quand bien même il serait *a priori* possible d'intégrer ce coût dans le calibrage initial de l'algorithme – dans la mesure où des logiciels reposant sur l'intelligence artificielle sont commercialisés pour l'analyse de la jurisprudence –, l'algorithme ne réagira pas

(49) L. Arcelin, préc., § 21 ; et Commission européenne, Rapport Crémer, préc., p. 102.
(50) Commission européenne, Rapport Crémer, préc., p. 112.
(51) F. Marty, préc., p. 86.
(52) OCDE, *Algorithms and Collusion : Competition Policy in the Digital Age*, p. 39-40.

comme une personne physique à ce risque[53]. Ainsi, la décision algorithmique joue défavorablement sur le volet dissuasif de la sanction, au détriment des autorités de concurrence.

Face à ces nombreuses problématiques juridiques, se pose alors la question de l'adéquation des politiques actuelles de concurrence au contexte numérique. Ces dernières sont-elles dotées des capacités adéquates pour caractériser et sanctionner de telles situations[54] ? La défense de l'ordre concurrentiel doit-elle passer par d'autres canaux[55] ? La complexité des algorithmes et de l'intelligence artificielle doit-elle conduire à passer d'une approche plus économique à une approche plus technique[56] ?

## § 2. – Quelles solutions pour maîtriser les risques concurrentiels ?

Afin de maîtriser les risques concurrentiels décrits *supra* et de faire face aux problématiques juridiques que rencontrent les autorités de concurrence pour faire appliquer le droit de la concurrence, des solutions peuvent être avancées, tant en ce qui concerne les pratiques anticoncurrentielles qu'en matière de concentration.

Dans le domaine des pratiques anticoncurrentielles, une première solution pourrait être celle d'une **régulation *ex ante* des algorithmes**[57]. Il s'agirait alors d'expérimenter les algorithmes avant leur mise en fonctionnement sur le marché, afin d'évaluer leur propension à induire des comportements anticoncurrentiels sur le marché et ainsi potentiellement les corriger au moyen d'engagements, de la même manière que les préoccupations de concurrence sont inhibées par des mesures correctives dans le cadre du contrôle des concentrations. En France, une première initiative en ce sens a pu être prise par l'Institut national de la recherche agronomique (en partenariat avec le Conseil national du numérique et l'Institut Mines Télécom) et résulte de la mise en œuvre d'une plateforme collaborative en ligne *TransAlgo*, visant à développer des outils logiciels et des méthodes de tests algorithmiques. Si cette solution permettrait à l'autorité de tester en amont les comportements des algorithmes dans certaines conditions les plus susceptibles de porter préjudice à la concurrence, il n'en demeure pas moins qu'elle resterait très coûteuse et qu'elle nécessiterait que les autorités de concurrence développent une véritable spécialisation dans ce domaine en se dotant d'experts afin d'être en mesure de détecter les risques potentiels. L'Autorité de la concurrence a d'ailleurs fait un pas en ce sens en se dotant dès janvier 2020 d'un service spécialisé dans l'économie numérique, ce dernier ayant pour mission de développer une expertise poussée sur l'ensemble des sujets numériques et de collaborer aux investigations sur les pratiques anticoncurrentielles dans l'économie numérique. En parallèle, il n'est pas

(53) F. Marty, préc., p. 94-95.
(54) F. Marty, préc., p. 86, § 2.
(55) *Ibid.*
(56) *Ibid.*
(57) F. Marty, préc., p. 102 et s.

improbable que les autorités se dotent elles-mêmes d'outils de détection des pratiques anticoncurrentielles en se penchant sur l'opportunité d'utiliser l'intelligence artificielle pour mettre en œuvre une régulation par les algorithmes. Par ailleurs, il serait également possible d'utiliser d'autres algorithmes comme contre-mesures pour altérer la transparence des marchés, en permettant par exemple aux consommateurs d'utiliser des algorithmes de comparaison de prix tout en réduisant la capacité des algorithmes des firmes à capturer instantanément cette information(58).

Une deuxième solution, moins coûteuse, peut consister à **introduire une règle de responsabilité sans faute** en faisant porter le contrôle sur le seul effet des pratiques. Toutefois, une telle règle serait très préjudiciable en termes d'efficience économique dans la mesure où elle inciterait les algorithmes, pourtant conçus pour être efficaces, à s'autoprogrammer pour être sous-efficients(59).

Enfin, une troisième solution, moins ambitieuse, plus facilement applicable mais certainement beaucoup moins efficace serait d'amener les autorités de concurrence à **rechercher une « preuve négative » d'un parallélisme de comportements**, en démontrant que dans une configuration de marché concurrentielle, seule une concertation tacite entre les entreprises *via* le déploiement et l'utilisation d'intelligences artificielles pourrait l'expliquer(60).

Dans un autre registre, maîtriser les risques concurrentiels pourrait passer par la **résolution de la problématique relative à l'imputabilité de l'infraction**. Il suffirait alors de s'appuyer sur des règles de responsabilité en se basant sur la réparation d'un éventuel dommage concurrentiel du fait de la mise en œuvre des algorithmes(61). Margrethe Vestager, commissaire chargée de la politique de concurrence au sein de l'Union européenne, est d'ailleurs venue conforter ces approches : « les responsables de l'application des règles de concurrence doivent se méfier de tous ceux qui utilisent un système automatisé pour fixer les prix. Les entreprises (…) doivent savoir que lorsqu'elles décident d'utiliser un système automatisé, elles seront tenues responsables de ce qu'il fait, elles ont donc intérêt à savoir comment ce système fonctionne »(62).

En matière de concentration, pour faire face aux risques de faux-négatifs, c'est-à-dire à l'autorisation d'opérations préjudiciables qui auraient dû être bloquées, se pose la question du **renforcement du contrôle des concentrations** dans le domaine du numérique. Une solution possible pour isoler les opérations motivées par l'acquisition des données d'un concurrent consisterait à **instaurer un seuil complémentaire de notification tenant compte de la valeur de la transaction de l'opération**. De tels seuils aideraient les autorités de concurrence à repérer les acquisitions préemptives destinées à évincer de potentiels futurs concurrents puisqu'ils témoigneraient du prix élevé que les acheteurs sont prêts à payer pour les actifs qu'ils acquièrent(63). Dans certains pays comme l'Allemagne

(58) F. Marty, préc., p. 103.
(59) F. Marty, préc., p. 104.
(60) T. Titone, préc., p. 3, I-B, al. 8.
(61) F. Marty, préc., p. 104 et s.
(62) M. Vestager, *Algorithms and Competition*, *Speech at the Bundeskartellamt 18th Conference on Competition*, Berlin, 16 mars 2017.
(63) OCDE, Données massives, préc., § 62.

ou l'Autriche, les seuils de contrôle ont déjà été révisés afin de permettre l'examen de telles acquisitions. Dans d'autres pays, à l'image du Royaume-Uni ou de l'Australie, des mesures prévoient d'imposer à certaines entreprises spécifiques d'informer les autorités de toutes les acquisitions qu'elles ont l'intention de réaliser(64). La Commission européenne estime de son côté qu'il est encore trop tôt pour modifier les seuils européens et attend les retombées des nouveaux seuils instaurés en Allemagne et en Autriche(65). Quant à la France, elle n'a pas opté pour l'introduction d'un seuil alternatif basé sur la valeur de la transaction, considérant cette notion comme difficile à appréhender(66), mais a pu examiner l'idée d'un contrôle *ex post* pour un nombre limité d'opérations susceptibles de poser des problèmes de concurrence, afin de vérifier les analyses prospectives réalisées en amont. Cette piste ne fait cependant pas l'unanimité, car elle serait une source d'insécurité juridique et pourrait entraîner une saturation du service de concentrations de l'autorité avec une augmentation inévitable des délais de réalisation des opérations(67). Cette option n'est toutefois plus à l'ordre du jour en raison de l'actualisation du renvoi à la Commission par le biais de l'article 22. En effet, la Commission européenne a franchi un pas décisif vers une forme de contrôle de ces acquisitions d'entreprises innovantes à haute valeur mais faible chiffre d'affaires en proposant une modification de l'interprétation de l'article 22 du règlement européen des concentrations de 2004(68). En vertu de cet article, une autorité nationale de concurrence peut renvoyer à la Commission pour examen une opération de concentration qui n'est pas de dimension européenne dès lors qu'elle affecte le commerce entre États membres. Ainsi, jusqu'à présent, la Commission n'acceptait un renvoi fondé sur cet article que dans l'hypothèse où l'opération franchissait les seuils de notification au niveau national d'au moins un État membre, laissant dès lors la possibilité à certaines opérations, portant sur des acteurs très innovants et qui commencent tout juste à valoriser leur innovation sur le marché, d'échapper au contrôle des concentrations, la cible ayant un chiffre d'affaires insuffisant pour que les seuils de notification s'appliquent. Or dans sa nouvelle approche, la Commission prévoit d'examiner dès la mi-2021 les renvois opérés par des autorités nationales de concurrence concernant des opérations de concentration qui méritent d'être examinées au niveau de l'Union européenne bien qu'elles ne soient pas de dimension européenne, y compris lorsque celles-ci ne franchissent pas les seuils de notification au niveau national. L'Autorité française de concurrence a dès lors annoncé que cette possibilité serait l'une de ses priorités pour l'année 2021(69). Elle a d'ailleurs annoncé entendre participer

(64) L. Arcelin, préc., § 43.
(65) Commission européenne, Rapport Crémer, préc., p. 113 à 115.
(66) L'Association française de l'étude de la concurrence (AFEC) a effectivement analysé cette question, mais a conclu qu'il n'était pas opportun de prévoir un tel seuil, la notion de transaction tout comme celle de numérique paraissant difficiles à appréhender.
(67) D. Théophile, *Non à un contrôle* a posteriori *des concentrations : Les Échos* 30 avr. 2019 (www.lesechos.fr/idees-debats/cercle/non-a-un-controle-a-posteriori-des-concentrations-1015031).
(68) Annonce de Margrethe Vestager, Commissaire chargée de la politique de concurrence, le 11 septembre 2020 lors du webinaire organisé à l'occasion de la 24e conférence concurrence de *International Bar Association* (IBA).
(69) Autorité de la concurrence, Communiqué de presse, *Après une activité très soutenue en 2020, l'Autorité de la concurrence annonce ses priorités pour 2021, qui seront centrées sur l'économie numérique*, 23 déc/ 2020.

activement à la définition d'orientations en la matière, et fera ainsi des propositions sur le cadre procédural qui pourrait être appliqué et sur les catégories d'opérations qui pourraient être concernées. Elle mettra par ailleurs en place une veille sur les marchés afin de détecter les opérations qui pourraient être soumises à renvoi à la Commission européenne. Une telle évolution constitue une avancée majeure et permettra ainsi de combler certaines lacunes du contrôle européen et national des concentrations par une meilleure appréhension du phénomène des acquisitions prédatrices ou consolidantes « sous les seuils », que l'on constate en particulier dans l'économie numérique, mais aussi dans le secteur pharmaceutique ou les biotechnologies. Par ailleurs, **sur le plan procédural**, une évolution pourrait apparaître puisque la Commission envisage que les parties notifiantes aient la charge de démontrer que les effets potentiellement négatifs sur la concurrence sont compensés par des gains d'efficacité (70).

## CONCLUSION GÉNÉRALE

L'intelligence artificielle et ses capacités à rebattre les cartes du jeu concurrentiel constituent l'un des facteurs majeurs de disruption dans notre économie numérique d'ores et déjà basée sur les algorithmes (71). Disruption à laquelle le droit de la concurrence n'échappe pas, dans la mesure où le recours à l'intelligence artificielle et les algorithmes pose des problèmes significatifs en matière de mise en œuvre des règles de concurrence.

Les enjeux pour les acteurs de la santé mettant en œuvre l'intelligence artificielle et les algorithmes sont alors liés à des questions de contrôle, de transparence et de redevabilité (72). Ils se doivent en effet, non seulement de maîtriser le processus de fonctionnement des algorithmes et de l'intelligence artificielle, mais également de faire preuve de transparence dans leur mise en œuvre, et ce sans oublier qu'ils auront des comptes à rendre quant aux effets sur le marché de leur utilisation. Partant de là, les acteurs de la santé qui y recourent se doivent de s'inscrire dans une logique d'auto-évaluation des impacts et de prévention des dommages, tant *ex ante* pour minimiser le risque de dommage qu'*ex post*. Il s'agit notamment de prévenir le risque que leur fonctionnement ait des effets anticoncurrentiels parfois même à l'insu de leurs développeurs et de leurs utilisateurs, en développant des algorithmes « responsables » (73).

(70) Commission européenne, Rapport Crémer, préc., p. 11.
(71) F. Marty, préc., p. 84 et 87.
(72) *Ibid.*, p. 107.
(73) *Ibid.*, p. 108.

CHAPITRE 9

# L'IMPACT DU NUMÉRIQUE SUR LA CONSOMMATION DES PRODUITS ET PRESTATIONS DE SANTÉ

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Seydou DIAKITE

L'impact du numérique sur la consommation des produits de santé soulève la question majeure de savoir quel est le statut de l'utilisateur des produits de santé et de bien-être connectés comprenant les robots dotés d'une intelligence artificielle, de l'utilisateur des services de santé connectés au travers de la télémédecine ou encore d'application numérique en santé. Le numérique en santé est devenu une priorité et est entré massivement dans les usages de la population, avec une force inédite pendant la phase pandémique de Covid-19. La situation de l'utilisateur des produits de e-santé et son encadrement juridique dépendent principalement de la qualification et de la classification juridique et réglementaire des produits, mais aussi du comportement de l'utilisateur des produits.

L'utilisateur du produit peut être une personne qui, en dehors de son champ professionnel, utilise un produit de e-santé de bien-être afin d'obtenir des informations et services de prévention en santé, il relève alors du droit de la consommation ; ce même utilisateur peut devenir un patient et utiliser le produit dans un sens de prévention et accompagnement dans le traitement de sa pathologie, toute la question est de savoir s'il reste un consommateur ou devient un patient, si le produit change de qualification par le fait qu'il est devenu un patient.

La situation peut aussi concerner un patient qui utilise un produit ou service de e-santé afin de suivre sa pathologie ; dans ce cas, ce produit dispose généralement du statut de dispositif médical soumis à une réglementation spécifique, et la relation entre dans le champ de la santé, mais le patient peut aussi être un consommateur de biens ou services de santé ou de bien-être qui visent à assurer une prévention et dans ce cas la question est de savoir si cette relation demeure dans le champ de la santé parce qu'elle touche un patient ou si elle entre dans le champ de la consommation.

Il serait aisé au plan théorique d'opérer dans chaque situation la distinction et de procéder à la qualification juridique permettant d'assurer l'application du dispositif normatif adapté au plan national ou européen. Toutefois, c'est sans compter sur la particularité des produits de e-santé qui sont souvent à la frontière et de plus en plus associés au traitement du patient, ou conduisant le consommateur dans un univers de santé préventive, prédictive.

Le droit de la santé et le droit de la consommation entretiennent des relations étroites et complexes, ce qui suppose d'identifier au préalable les caractéristiques du consommateur de produits et services numériques puis d'identifier les conséquences dans l'application du dispositif national et européen dans un contexte de constante innovation numérique en santé, qui nécessite de repenser les qualifications et les interactions normatives. L'impact est important concernant notamment les obligations des prestataires de services numériques, les obligations de protection des données collectées.

L'analyse de ces questions suppose de revenir sur la notion de consommateur afin d'en définir les contours au regard du droit de la santé. Les outils numériques ont été largement décrits tout au long de cet ouvrage, il n'est donc pas nécessaire de revenir sur les différents usages de la télémédecine, ou encore sur le déploiement de l'e-santé dans la vie des usagers.

En revanche, il est important de définir et distinguer en droit les notions de consommateur et de patient qui s'entrelacent tout au long de la vie d'une personne, et ce d'autant plus que la personne gagne en âge. En effet, toute personne au cours de son existence est constamment consommateur et patient, de la naissance à la fin de vie. Toutefois, c'est dans la population senior, la plus souvent polymédiquée et confrontée au système de santé, tout en restant consommateur de produits de e-santé à vocation préventive et de bien-être, que se pose la question de l'application croisée du droit de la santé et du droit de la consommation.

Si la relation de soins qu'entretient le patient avec le professionnel de santé, au travers de la télémédecine, entendue au sens large, entre dans le champ du droit de la santé et sort du champ du droit de la consommation, en revanche, la relation de bien-être ou de prévention qu'entretient le patient avec les acteurs du numérique, voire les professionnels de santé, pose la question de savoir si la relation relève toujours du droit de la consommation ou entre dans le champ du droit de la santé. Pour ce faire, il convient de préciser les règles de droit national et européen portant sur l'application spécifique du droit de la santé, excluant les règles de droit de la consommation, puis d'analyser les situations dans lesquelles le « patient-consommateur » utilise des outils numériques, prestations numériques, objets connectés ayant pour finalité de surveiller et accompagner la personne dans l'amélioration de sa qualité de vie. Ces produits et services sont à la frontière du droit de la santé, qui porte non seulement sur le traitement, mais aussi sur la prévention en santé, au sens de la définition donnée par l'OMS, selon laquelle 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, par l'Union européenne (TFUE, art. 3, 168 et 114) et le droit national. L'analyse de ces sources pose clairement comme critère l'exclusion de l'application du droit de la consommation dans la relation de santé,

c'est-à-dire dans la relation entre le professionnel de santé et le patient, ou encore dans la relation entre le patient et le système de santé, à savoir la prise en charge des soins par l'assurance maladie, laquelle n'entre pas dans le champ commercial et concurrentiel, car fondée sur le principe de solidarité.

Mais bien au-delà de cette relation *intuitu personae* entre le patient et le professionnel de santé, se pose aujourd'hui toute la question de l'intégration du numérique dans la relation de soin, entendue au sens large et par conséquent la nature des relations entre les opérateurs numériques, le professionnel de santé et le patient.

Cela conduit à définir la situation de la personne patient-consommateur connecté (Section 1), puis à définir les obligations et responsabilités des acteurs au regard du droit de la consommation ou de la santé (Section 2).

SECTION 1

# LA DÉFINITION DU PATIENT-CONSOMMATEUR CONNECTÉ

Aujourd'hui plus que jamais, du fait de la pandémie Covid-19, les outils numériques sont devenus un pilier central de la vie en société et du nouveau mode de consommation et de soins de chaque personne. Le recours aux applications mobiles en e-santé, en télémédecine est devenu une priorité dans la prise en charge du patient, mais aussi dans l'organisation des activités préventives développées par chacun. Ceci conduit à s'interroger sur la qualification du consommateur, dès lorsque chaque personne est tout à la fois un consommateur et un patient ou utilisateur du système de santé.

## § 1. – Le « patient-consommateur » dans sa relation avec le professionnel de santé

Si désormais chaque patient est en mesure de prendre en charge sa santé, au travers notamment d'applications de santé mobile ou grâce à des robots dotés d'une intelligence artificielle, la question de la relation du patient avec le professionnel de santé interroge dès lors que l'impact de ces outils numériques interfère dans le diagnostic médical et la prescription du professionnel de santé. La question se pose avec acuité de savoir si le patient le demeure, dès lors qu'il s'inscrit désormais dans sa relation avec le professionnel de santé dans une dynamique de bouleversement du rapport d'information existant entre les parties. En effet, il est devenu fréquent, voire systématique, que le patient vienne consulter le professionnel de santé après avoir identifié ou cru pouvoir identifier sa pathologie grâce à l'usage d'outils dotés d'intelligence artificielle, ou dès lors que le patient contrôle les prescriptions des professionnels de santé grâce à ces outils. Le patient devenu actif, acteur,

voire déterminant dans la relation de santé, change de rôle avec le développement des outils numériques. La question se pose alors de savoir s'il conserve un statut de patient protégé par les dispositions du Code de la santé publique, ce qui modifierait le droit d'information et la nature du consentement libre et éclairé tel qu'il est entendu en droit de la santé.

Il convient de rappeler que le patient dispose de droits prévus par le Code de la santé publique, et notamment dans le Code de déontologie des professionnels de santé (médecins, pharmaciens).

Au regard du droit européen, le TFUE prévoit dans ses articles 3 et 168 que les États membres disposent d'un pouvoir souverain dans l'organisation du système de santé et notamment dans l'organisation des monopoles en santé, portant sur les professionnels de santé. Les relations des professionnels de santé et patients entrent dans les champs spécifiques du droit de la santé et sont donc placées hors du droit de la consommation. En droit interne, le Code de la consommation exclut l'application des règles de la consommation en matière de santé ; nous avons l'exemple de l'article L. 224-105 sur les contrats de prestation de soins médicaux du Code de la consommation :

« Les règles relatives à l'information du patient par les professionnels de santé sont fixées par les dispositions du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique.

Les règles relatives à l'information du patient et au délai de réflexion en matière de chirurgie esthétique sont fixées par les dispositions du chapitre II du titre II du livre III de la sixième partie du code de la santé publique.

Les règles relatives à l'information du patient par un chirurgien-dentiste ou un médecin à l'occasion d'un acte faisant appel à un fournisseur ou un prestataire de services sont fixées par les dispositions du chapitre 2 du titre 6 du livre 1 du code de la sécurité sociale ».

Toutefois, il convient de rappeler qu'au plan historique, la jurisprudence a pu par le passé reconnaître l'application du droit de la consommation dans le cas particulier de la relation financière liant le patient et le professionnel de santé. Le principe de l'obligation d'information en matière de soins médicaux ou de frais liés aux soins médicaux doit être conforme aux dispositions du Code de la santé publique et non pas à celles du Code de la consommation. Cette décision impose donc aux professionnels de santé, dans leur relation avec le patient, le respect de l'application de l'article L. 1111-3 du Code de la santé publique.

Néanmoins, cette jurisprudence n'a plus cours. La question dans le secteur de la télémédecine se pose avec acuité, sachant que pendant de très nombreuses années le dispositif de télémédecine était opérationnel au plan technique et permettait une prise en charge du patient, mais pas une prise en charge financière par le régime de l'assurance maladie. Il a fallu attendre la récente loi sur l'e-santé numérique, puis la phase Covid-19 pour assister à une accélération de la prise en charge générale des consultations à distance des patients. La question se pose alors de savoir quel est le statut du patient dès lors que la prise en charge n'est pas assurée par l'assurance maladie et n'entre pas dans les actes cotés. S'agit-il d'actes contraires aux dispositions du Code de déontologie et donc de l'exercice illégal de la médecine, ou s'agit-il d'un exercice en secteur libéral non coté à la charge exclusive du patient restituant celui-ci dans le statut de consommateur de soins ?

Sur le plan de la médecine esthétique ou de la chirurgie plastique, non remboursée, les patients sont dans un rapport proche de la consommation, avec une obligation de résultat des professionnels de santé. Mais, dans le cadre d'une médecine classique, le praticien est tenu à une obligation de moyens et dont les actes sont pris en charge par l'assurance maladie, la relation est placée hors du champ de la consommation. Il en va de même lorsque l'acte est effectué à distance par le biais de la télémédecine.

Au sens du droit de la consommation, le consommateur est défini comme « toute personne physique qui régit à des fins qui n'entrent pas le dans le cadre de son activité commerciale, industrielle, artisanale ou libérale »[(1)]. Cette définition pose deux critères pour définir un consommateur : un critère subjectif et un critère objectif. Le consommateur est une personne physique qui agit à des fins qui n'entrent pas le dans le cadre de son activité professionnelle.

Il bénéficie d'un droit d'information et de protection, notamment en cas de fausses informations ou informations trompeuses.

Au sens du droit de la santé, le patient dispose également d'un droit d'information renforcé, assuré par le professionnel de santé, mais aussi par le fabricant du produit de santé. Cette information, qui vise à garantir sa sécurité et la protection de la santé publique, va bien au-delà des éléments exigés en droit de la consommation. Toutefois, il convient de noter une ambiguïté forte entre le statut de consommateur de soins et celui de patient. Cette difficulté de qualification avait déjà été relevée par la jurisprudence avant l'avènement de l'ère numérique, mais elle est renforcée avec l'utilisation des outils numériques.

En théorie, il y a une séparation entre le patient et le consommateur. Le premier est défini par le Code de la santé publique et le second par le Code de la consommation. La relation entre le patient et le professionnel de santé vise, d'une part, les prestations de soins, de diagnostic et prescription, qui sont régies par le Code de la santé publique et sont hors du champ du rapport de consommation et, d'autre part, la relation financière qui s'établit entre le professionnel de santé, visant la rémunération des soins pris en charge ou non par l'assurance maladie, au sujet desquelles la question de la relation de consommation peut se poser.

Par le passé, la jurisprudence a pu considérer le patient comme étant un consommateur dans le souci d'une bonne mise en œuvre de l'action en responsabilité médicale, ce qui apparaît notamment dans l'arrêt de la chambre criminelle de la Cour de cassation en date du 15 mai 1984[(2)]. Dans cet arrêt, il était mis en cause l'article L. 421-1 ancien du Code de la consommation devenu l'article L. 621.1, relatif à l'exercice de l'action civile par les associations de consommateurs agréées. La cour d'appel avait admis l'application de l'article 46 de la loi du 27 décembre 1973. Ce texte relatif à l'orientation du commerce et de l'artisanat permettait aux associations de consommateurs agréées à cette fin la mise en œuvre de l'exercice d'une action civile pouvant porter un préjudice direct ou indirect à l'intérêt collectif des consommateurs. La chambre criminelle de la Cour de cassation a conclu que

(1) L. n° 2014-344, 17 mars 2014, relative à la consommation, dite « loi Hamon », art. préliminaire.
(2) Cass. crim., 15 mai 1984, n° 84-90.252.

« l'article 46 de la loi du 27 décembre 1973 ne comporte pas de restriction de nature à exclure son application aux infractions qui seraient commises à l'occasion de services fournis, comme en l'espèce, dans l'accomplissement d'un contrat médical ; que les personnes avec lesquelles un médecin conclut un tel contrat doivent être considérées au sens de l'article 46 susvisé "comme consommateurs" desdits services ».

Dans une autre affaire tranchée par le Conseil d'État le 27 avril 1998[3], il était question de l'application de l'article L. 113-3 du Code de la consommation : « Tout vendeur de produit ou tout prestataire de service doit, par voie de marquage, d'étiquetage, d'affichage ou par tout autre procédé approprié, informer le consommateur sur le prix, les limitations éventuelles de la responsabilité contractuelle et les conditions particulières de la vente, selon les modalités fixées par arrêté du ministre chargé de l'économie, après consultation du Conseil national de la consommation ». L'application de cet article se heurtait à un principe du Code de déontologie médicale énuméré dans son article 55, repris dans l'article R. 4127 du Code de la santé publique qui dispose : « Le forfait pour l'efficacité d'un traitement et la demande d'une provision sont interdits en toute circonstance ». Le Conseil d'État, en application de l'article L. 113-3 du Code de commerce, considère que : « S'applique à toutes les activités entrant dans le champ d'application de l'ordonnance du 1er décembre 1986 relative à la liberté des prix et la concurrence, c'est-à-dire à toutes les activités de production, de distribution et de service, y compris celle qui sont le fait de personne publique, notamment dans le cadre de convention de délégation de service public ». Le Conseil d'État va encore plus loin dans sa décision en précisant que : « L'obligation d'information du consommateur instituée au premier alinéa de l'article L. 113-3 est mise à la charge de tous les prestataires de services, sans considération du caractère commercial ou libéral de leur activité et concerne notamment les prestations à caractère médical, que l'arrêt attaqué a donc été légalement pris sur le fondement de l'article L. 113-3 du code de la consommation ».

À l'époque, à défaut de disposition spécifique au droit de la santé, les juges avaient recours aux différentes notions du droit de la consommation pour sanctionner les manquements des professionnels de santé dans l'exécution du contrat médical, et notamment concernant l'information du patient sur le montant des honoraires. Le patient était donc dans une relation de « consommateur de soins » et, en face du professionnel de santé, considéré comme un « prestataire de service », au-delà du caractère libéral et médical de son activité. Le contrat entrait sous certaines conditions dans le champ de la consommation.

Cette position de la jurisprudence assimilant le patient à un consommateur a été durement critiquée par la doctrine considérant que : « La protection du patient devait passer nécessairement par une obligation d'information la plus complète possible, cela ne devait pas se faire au moyen d'une extension infinie de la notion de consommateur, mais *via* les dispositions du Code de la santé publique ».

(3) CE, 27 avr. 1998, n° 184473.

Cependant en 2013, une véritable distinction a été mise en lumière par un arrêt de la cour d'appel de Paris[4]. Dans cette affaire, la cour a écarté l'application des dispositions du Code de la consommation au patient d'un chirurgien-dentiste. Elle a refusé d'assimiler le patient à un consommateur, considérant que l'article L. 111-1 du Code de la consommation qui prévoit une obligation d'information du professionnel au consommateur n'a pas vocation à régir les relations entre un patient et le professionnel de santé organisées par des dispositions du Code de la santé publique. Le droit d'information, très fort en droit de la santé, est prévu par le Code de la santé publique dans son article L. 1111-3 : « Toute personne a droit à une information sur les frais auxquels elle pourrait être exposée à l'occasion d'activités de prévention, de diagnostic et de soins et, le cas échéant, sur les conditions de leur prise en charge et de dispense d'avance des frais. Cette information est gratuite ».

La relation médicale qui lie le patient au praticien ne peut pas être assimilée à un contrat de consommation en raison du caractère *intuitu personae* entre eux.

Après cette décision de la cour d'appel de Paris, on se demande si elle a pu mettre fin à l'extension de la notion de consommateur à l'absence de définition légale.

La réponse à cette question est négative. À défaut, de définition légale, il y a moult interprétations de la notion de consommateur dans le but souvent de protéger des personnes en situation de faiblesse. C'est pourquoi aujourd'hui nous assistons à l'évolution d'un nouveau type de consommateur en santé. Il s'agit du passage de consommateur de soins au patient-consommateur connecté.

Le Code de la santé publique ne fournit aucune définition spécifique des objets connectés. Le statut du patient a connu une grande évolution ; il est passé d'un sujet passif à un sujet actif. Il est aujourd'hui un acteur dans la prise en charge de sa santé et la reconnaissance de ses droits.

L'ubérisation (ce nouveau modèle de commerce) permet au patient de sa propre initiative pour sa propre santé, le droit de pouvoir choisir les soins et les produits qui lui paraissent adaptés sur le marché.

En effet, le patient connecté est un non-professionnel. C'est-à-dire, une personne qui manque sérieusement d'informations, contrairement au professionnel du soin ou des produits de santé. Il doit être informé, formé, voire accompagné dans sa démarche avec la plus grande vigilance et prudence sur le recueil de son consentement tout ayant une information éclairée sur sa santé.

Le patient connecté en tant qu'acteur actif doit avoir connaissance de ses droits et obligations. Cette information incombe au professionnel de santé et aussi sur l'intermédiaire qui fournit l'objet connecté qui va ensuite collecter les données personnelles de santé. Quand bien même le patient va se comporter comme un consommateur connecté, il reste et demeure un patient.

L'article R. 4127 du Code de la santé publique exige des professionnels de santé qu'ils procèdent à la recherche du consentement de la personne examinée ou soignée dans tous les cas. Lorsque le patient est dans l'impossibilité de donner son consentement, le professionnel de santé doit procéder à la recherche

(4) CA Paris, 21 mars 2013, n° 12/01892.

du consentement auprès d'un tiers de confiance dans le cas où le patient n'avait pas pu donner son consentement dans une directive anticipée.

Dans l'utilisation d'un objet connecté, le consentement éclairé doit apparaître dans une norme de protection intégrée au moment de la conception de l'objet connecté qui va engendrer peut-être de nouvelles conventions codifiables par le droit destinées à encadrer l'exploitation économique des données du patient connecté.

Les objets connectés jouent un rôle important dans notre société ; grâce aux applications mobiles et aux plateformes en ligne, ces objets connectés vont effectuer une transmission plus régulière des données aux praticiens. Par ailleurs le Comité consultatif national d'éthique (CCNE), dans un avis rendu public en date du 29 mai 2019, a mis en exergue les différents risques d'égalité d'accès aux soins entre les patients connectés et non connectés. Ce risque pourrait s'aggraver avec l'influence de plusieurs facteurs, dont le vieillissement de la population face à une jeunesse ultraconnectée et la désertification des régions face aux villes connectées.

Le statut juridique de l'objet connecté ayant une revendication de santé est réglementé par les règles générales de la protection des données[5], à savoir la loi Informatique et Libertés du 6 janvier 1978, modifiée par la loi n° 2018-493 du juin 2018 auxquels s'ajoutent les nombreux textes relatifs à la télémédecine.

La sécurité du patient connecté lors de l'utilisation des objets connectés sera assurée par les mesures relatives à la protection des données et par le règlement portant sur les dispositifs médicaux. Dans certains cas, le patient souffrant de certaines pathologies sera prévenu ou suivi grâce à un objet, qui peut être doté d'une intelligence artificielle. Ces types d'objets peuvent revêtir la qualification de dispositifs médicaux quand ils sont destinés à être utilisés à des fins « de diagnostic, prévention, contrôle, traitement ou atténuation d'une maladie ; de diagnostic, contrôle, traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap ; d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique ; de nature de la conception » (C. santé publ., art. R. 511-1).

Il convient de préciser que les autorités de contrôle disposent d'un pouvoir de coopération. Notamment, il est à noter une relation forte entre la DGCCRF et l'ANSM dans le signalement des effets indésirables et publicités trompeuses pouvant porter atteinte au « patient-consommateur ». La DGCCRF est une entité nationale, son rôle est primordial au sens du droit de la consommation, elle veille à la régulation et au bon fonctionnement des marchés. Elle a été dotée depuis la loi Hamon d'un pouvoir d'inspection pour vérifier qu'aucune infraction n'a été commise ; elle peut prononcer des amendes administratives. Elle a un pouvoir de transaction (négociation d'une peine), un pouvoir de saisir les autorités civiles ou administratives en cas de clause abusive et demander le retrait de cette clause. Ce pouvoir s'applique sur les biens de consommation ordinaires et également sur les produits cosmétiques et les compléments alimentaires.

En conséquence, si dans sa relation avec le professionnel de santé, la question de l'utilisation du numérique est sans effet sur la nature des relations liant les parties

(5) RGPD, 27 avr. 2016 ; Loi pour une République numérique, 7 oct. 2016.

et donc sur les conséquences concernant l'application de droit de la santé, il n'en demeure pas moins que le statut du patient devient de plus en plus complexe, engagé dans une démarche de recherche de consumériste de soins, le plaçant dans une situation de clientélisme par rapport au professionnel de santé. Pour l'instant, les juridictions n'ont pas cédé à la qualification de la relation entre le professionnel de santé et les patients comme relevant du droit de la consommation, mais la frontière devient de plus en plus ténue, notamment du fait de l'utilisation du numérique et de l'intervention des prestataires de services numériques que sont les grands acteurs du numérique, organisateurs des prises de rendez-vous, de la gestion du carnet de santé du patient ou encore de la gestion de la prise de rendez-vous pour la vaccination Covid-19. De ce fait, la relation se trouble ; les acteurs commerciaux entrent dans le champ du droit de la santé, alors que le patient se dirige vers une relation de consommation avec ces acteurs.

## § 2. – Le « patient-consommateur » dans sa relation avec les opérateurs numériques

Il va sans dire que la relation du patient avec les acteurs du numérique, et notamment des créateurs de plateformes de santé ou robots dotés d'une intelligence artificielle, s'inscrit dans le cadre d'une relation commerciale et place le patient dans une situation de consommateur. La relation est soumise en principe aux dispositions du Code de la consommation. En conséquence, l'ensemble de la relation commerciale engendre des droits pour le patient de bénéficier d'une information protégée par le droit de la consommation. Sont visés l'ensemble des applications et outils numériques de bien-être, voire de prévention en santé.

Dans cette hypothèse, la relation directe est établie entre le prestataire numérique et le consommateur, bien que le contenu de la prestation permette de mettre en lien le professionnel de santé et le patient. Nombreuses sont les plateformes et *startups* agissant dans ce secteur, dopé par la phase de pandémie. Cette relation est placée dans le secteur du droit de la consommation au titre des articles L. 111-7 à L. 111-8 du Code de la consommation.

L'article L. 111-7 dudit code dispose :

« I. – Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur :

1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ;

2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service ».

Toutefois, la question se pose de savoir quelle est la nature de la relation du patient avec cette plateforme lorsque celle-ci est investie d'un pouvoir accordé par les pouvoirs publics, notamment dans l'organisation de la prise de rendez-vous et la répartition des patients dans le cadre de la vaccination Covid-19. La mission confiée à Doctolib par les pouvoirs publics influe-t-elle sur la relation de consommation avec les utilisateurs,

dès lorsque la prise de rendez-vous est automatiquement dirigée vers et par la plateforme ? La question de la responsabilité des acteurs numériques, comme acteurs dans l'organisation du système de santé, se pose au-delà du droit de la consommation.

Les droits du patient à l'accès aux soins, et à l'information en santé sont en cause, car désormais soumis au contrôle par les plateformes. L'évolution du droit dans ce domaine nécessitera de déterminer quelles sont les responsabilités des acteurs du numérique et des professionnels de santé dans le suivi du patient-consommateur de soins et services de santé.

SECTION 2

## OBLIGATIONS ET RESPONSABILITÉS DES ACTEURS AU REGARD DU DROIT DE LA CONSOMMATION ET DE LA SANTÉ

L'évolution du numérique en santé conduit à repositionner la relation des acteurs et donc leurs responsabilités sur le fondement du droit de la consommation ou de la santé. L'intermédiation des prestataires de services numériques dans la relation de soins modifie l'approche juridique des responsabilités, notamment lorsque les outils numériques sont dotés d'une intelligence artificielle auto-apprenante, capable d'analyse autonome sur laquelle peuvent se baser les professionnels de santé dans leurs actes de diagnostic ou de prescription. La question est alors de savoir si la décision relève toujours du droit de la santé ou si elle relève de la responsabilité autonome de l'IA dans sa relation de consommation avec le patient utilisateur. Dans l'attente d'un règlement européen sur l'IA, qui devrait intervenir au cours de l'année 2021, il convient de poser plusieurs hypothèses de réflexion sur la responsabilité des acteurs numériques et professionnels de santé.

### § 1. – Responsabilité des professionnels de santé et acteurs de santé

Il ne fait aucun doute que les professionnels de santé voient leur relation placée sous l'angle du droit de la santé et du Code de déontologie qui les obligent à l'égard du patient, y compris lorsqu'ils utilisent des outils numériques dans l'organisation de leurs relations avec le patient. Toutefois, il convient de préciser que l'utilisation du numérique doit être maniée avec prudence. En effet, les professionnels de santé doivent assurer une information complète. Le recours à la télémédecine, et notamment aux outils de téléconsultation, n'est pas indiqué dans certaines circonstances où la visite physique du patient est imposée, ce qui peut être le cas notamment pour les médecins orthopédistes qui doivent avoir une visite physique avant une intervention et non pas une visite virtuelle. Les outils numériques ne sont donc pas automatiques et obligatoires dans la relation de soins y compris dans une période

d'urgence sanitaire, exigeant de mettre en place le plus possible une visite virtuelle du patient.

Depuis juin 2011, les médecins utilisant le recours à la télémédecine ont vu leurs obligations s'étendre à travers un nouveau programme de téléconsultation mis en place par l'autorité publique dans le but d'améliorer l'accès aux soins dans plusieurs domaines prioritaires comme l'accès à l'imagerie médicale pendant la permanence des soins, l'accès à la thrombolyse, l'accès à des téléconsultations spécialisées dans les établissements pénitentiaires, dans les structures médico-sociales (EHPAD)…

En conséquence, la relation, utilisant le numérique, demeure placée dans le domaine du droit de la santé et implique donc un respect du droit d'information du patient, du libre choix du professionnel de santé, du consentement du patient. Le professionnel de santé engage donc sa responsabilité civile, pénale, et déontologique dès lors qu'il ne respecte pas les dispositions du Code de la santé publique.

Le patient ne peut invoquer son statut de consommateur que dans l'hypothèse où la plateforme numérique qu'il utilise pour contacter le professionnel de santé porte atteinte à ses droits, notamment en ne respectant pas la protection des données de santé et la confidentialité des échanges avec le professionnel de santé, ou encore en ne respectant pas ses obligations de mise en relation dans les délais prévus. Dans ces cas, les personnes chargées de la gestion des plateformes numériques s'exposeront à des sanctions qui peuvent être administratives et/ou pénales pour non-respect de la loi encadrant le traitement des données de santé. Mais dès lors qu'il s'agit d'une relation entrant dans le champ de la santé, seront applicables les articles L. 1111-8, L. 1115-1 du Code de la santé publique et les articles 222-18, 226-18 à 226-24 du Code pénal.

Lorsque la responsabilité médicale d'un agent de service public (praticien hospitalier) ou d'un médecin de l'établissement privé ayant fait le recours aux outils numériques (téléconsultation, télésurveillance, télé-expertise…) est engagée, elle sera analysée sous l'angle de la responsabilité contractuelle et délictuelle qui caractérise la relation du médecin avec le patient.

Suite à la loi n° 2002-303 du 4 mars 2002, le fondement de la responsabilité médicale est devenu délictuel selon l'article L. 1142-1 du Code de la santé publique :

« I. – Hors le cas où leur responsabilité est encourue en raison d'un défaut d'un produit de santé, les professionnels de santé mentionnés à la quatrième partie du présent code, ainsi que tout établissement, service ou organisme dans lesquels sont réalisés des actes individuels de prévention, de diagnostic ou de soins ne sont responsables des conséquences dommageables d'actes de prévention, de diagnostic ou de soins qu'en cas de faute… ».

Cet article renvoie à la faute délictuelle.

Par ailleurs, la question peut se poser de la qualification juridique des applications utilisées dans la relation entre professionnels de santé et patients et assurant un service d'aide à la décision ou d'aide à la prescription.

Selon une décision de la Cour de justice de l'Union européenne du 21 décembre 2011[6] et un arrêt rendu par la Cour de cassation le 9 novembre 1999[7] : « Le contrat

(6) CJUE, 21 déc. 2011, n° C-495/10.
(7) Cass. 1re civ., 9 nov. 1999, n° 98-10.010.

formé entre le patient et son médecin met à la charge de ce dernier une obligation de sécurité de résultat en ce qui concerne les matériels qu'il utilise pour l'exécution d'un acte médical d'investigation ou de soins ». Il appartient au patient la charge de prouver que ce sont bien ces matériels qui sont à l'origine de son dommage.

Lorsqu'est en cause une défectuosité du matériel, la responsabilité du fournisseur sera engagée dans le cadre d'une obligation de sécurité de résultat. Il appartient à ce dernier d'exercer une action récursoire contre le producteur. Ces recours sont gérés par le biais des assureurs responsabilité civile. Le régime, lié à la qualité du matériel, permet d'engager la responsabilité personnelle de toutes les personnes intervenant dans la chaîne des outils informatiques et des technologies. Le professionnel de santé doit aussi s'assurer d'une maîtrise de l'outil qu'il manœuvre, et il doit pouvoir disposer de contacts permettant de joindre des informations professionnelles en cas de défaillance. Enfin il doit, dans le cadre des soins effectués, s'assurer de la compétence et de la disponibilité des professionnels techniques.

La perte de chance que peut invoquer le patient-consommateur connecté implique de s'interroger sur l'opportunité pour le professionnel de recourir aux outils numériques (à l'IA), et sur les risques de mise en cause de sa responsabilité en cas de non-utilisation. Le Code de déontologie médicale, à travers l'article R. 4127-32 du Code de la santé publique, établit la possibilité de recourir à l'aide d'un tiers compétent. Lorsque le médecin s'engage à assurer personnellement au patient des soins fondés sur les données acquises de la science, et cela à partir du moment où il accepte de répondre à une demande, il peut être tenu de recourir à un tiers compétent ou à une technologie extérieure intelligente (IA). De plus, l'article R. 4127-33 du Code de la santé publique va plus loin en obligeant le médecin à toujours élaborer son diagnostic avec le plus grand soin, et en s'aidant dans toute la mesure du possible des méthodes scientifiques les mieux adaptées. La décision de la première chambre civile de la Cour de cassation du 27 novembre 2008[8] est une illustration parfaite de la prise en considération de ces dispositions du Code de déontologie médicale et leur violation est de nature à constituer une faute civile. La chambre civile de la Cour de cassation a admis, en cas de doute sur le diagnostic médical, sur le fondement des articles R. 4127-32 et suivant du Code de la santé publique, que le praticien doive recourir à l'aide de tiers compétents ou de concours appropriés.

Lorsque le professionnel médical dispose du moyen de la télémédecine, il doit s'en servir pour pratiquer une téléconsultation pour les patients se trouvant dans l'incapacité ou l'impossibilité d'effectuer un déplacement, ou par mesure de précaution en vue de ralentir la circulation du virus, comme on a vu pendant la pandémie de la Covid-19.

Dans le cadre d'un suivi à distance, le recueil de consentement peut se faire de manière suivante : soit par le patient lui-même, peut-être de manière automatique par des capteurs personnels non intrusifs, soit par un professionnel paramédical. Mais cette tâche spécifique devrait faire l'objet d'une reconnaissance économique. L'analyse des méthodes de recueillement du consentement et de son expression doit être précisée étant entendu la distance virtuelle entre le professionnel de santé

(8) Cass. 1re civ., 27 nov. 2008, n° 07-15.963.

et le patient. En conséquence, il est tout particulièrement important, dans l'hypothèse d'une utilisation d'un objet connecté, doté d'une IA, de préciser clairement les conditions dans lesquelles le consentement est donné, par le patient acteur, et ce tout au long de la relation.

La question peut se poser de la qualification juridique des applications utilisées dans la relation entre professionnels de santé et patients et assurant un service d'aide à la décision ou d'aide à la prescription.

La Haute Autorité de santé a émis de nombreuses recommandations sur la qualification juridique de ces applications et sur les conséquences concernant la prise en charge de ces services par l'assurance maladie. Il convient de préciser que les outils d'aide à la décision ou à la prescription sont considérés comme des dispositifs médicaux, contenant un logiciel apte à orienter la décision du professionnel de santé dans le diagnostic ou la prescription.

Dans ce cas précis, les outils numériques qualifiés comme des dispositifs médicaux impliquent pour le prestataire de services une responsabilité au titre du nouveau règlement sur les dispositifs médicaux. De ce fait, ces produits, et les prestations qui y sont attachées, sortent du champ du droit de la consommation et entrent dans le champ sectoriel de la responsabilité des fabricants de dispositifs médicaux, qui doivent assurer la traçabilité, la surveillance et la sécurité des DM, avec un système de pharmacovigilance, sous le contrôle de l'ANSM.

## § 2. – Responsabilité des prestataires de services numériques

La question de la responsabilité des prestataires de services numériques dépend alors fortement de la qualification du produit numérique qui est proposé à l'utilisateur. De cette qualification dépendra le statut de DM ou de produit de consommation classique pour les applications de bien-être et de prévention en santé.

Toutefois, il convient de préciser que cette qualification est très ambiguë dans la mesure où les actions de prévention en santé peuvent aussi bien relever de pratique de bien-être que de pratique de prévention en santé, prochainement prise en charge par l'assurance maladie, à l'instar du sport ou de l'exercice physique programmé par un professionnel de santé. Certaines applications de santé préventives ont notamment été considérées, hors UE, en Inde notamment, comme des techniques de prévention de santé prises en charge par le système de santé. Une dynamique internationale est en cours sur la prise en charge de la santé préventive. En France, la prise en charge est encore balbutiante. Dans cette attente, les plateformes et outils numériques en santé organisant la prévention sont des outils de consommation entraînant la responsabilité des acteurs envers les consommateurs.

De ce fait, la DGCCRF doit contrôler ces plateformes afin de vérifier si les informations sont trompeuses ou non, si les droits du consommateur sont respectés.

Les prestataires de services numériques, en l'état actuel du droit positif, sont soumis aux règles du droit de la consommation.

Les sanctions civiles et pénales encourues par les prestataires à l'égard du patient porteront donc principalement sur deux catégories principales d'infractions : le respect de la protection des données et des conditions générales du site, et la sincérité de l'information donnée par la plateforme conditionnant le consentement du patient.

La plateforme doit supporter garantir le résultat dans la mise en relation avec les professionnels de santé.

Elle doit assurer la confidentialité des données, le respect du RGPD, mais aussi la traçabilité des opérations suivies sur la plateforme.

Aussi, le concepteur de la plateforme devra porter une attention toute particulière aux risques de développement du produit, et notamment à l'usage qui sera fait, ainsi qu'aux risques de cyberattaques visant à la captation des données de santé. Ce phénomène s'est démultiplié depuis le début de la phase Covid-19, et implique une vigilance toute particulière de la part des acteurs intervenant dans le secteur du numérique en santé.

Les fuites accidentelles ou les attaques sont de plus en plus récurrentes, qui sont souvent dues non pas à une malveillance, mais plutôt à une insuffisance de mise en œuvre des règles de sécurité.

Il convient de préciser que la plupart des activités des plateformes sont gratuites pour l'utilisateur. Toutefois, il est important de préciser que le service rendu est donné en contrepartie de l'utilisation des données du patient collectées par les plateformes. Dès lors ces dernières auront la possibilité de mettre en place des services de traitement des données collectées afin de les revendre à des opérateurs économiques tels que les laboratoires pharmaceutiques ou pourront les mettre à disposition des établissements de santé afin d'assurer la recherche et développement dans les projets innovants d'études des produits de santé. Les plateformes ont une obligation d'anonymisation des données afin que le patient ne puisse être identifié.

La question qui peut se poser est celle de savoir si le droit de la consommation est plus ou moins favorable, ce qui pourrait entraîner des comportements de *forum shopping* de la part des prestataires de services numériques, afin de se placer sous le régime le plus favorable.

L'Union européenne a présenté le 15 décembre 2020 deux projets de règlements portant sur de nouvelles règles visant à réguler les géants du numérique : le premier (*Digital Market Act*), sur la modération des contenus publiés sur les plateformes, et le second (*Digital Service Act*) relatif à la concurrence.

Ces nouvelles mesures toucheront sans doute à tous les secteurs, elles visent à introduire sur le territoire de l'UE de nouvelles obligations harmonisées pour les services numériques. Ces nouvelles règles seront adaptées aux circonstances, c'est-à-dire à la taille et à l'impact des services numériques comme « des règles en vue de la suppression de biens, services ou contenus illicites en ligne ; des garanties pour les utilisateurs dont un contenu a été supprimé par erreur par une plateforme ; de nouvelles obligations, pour les très grandes plateformes, de prendre des mesures fondées sur les risques afin d'empêcher une utilisation abusive de leurs systèmes ; des mesures de transparence, notamment en ce qui concerne la publicité en ligne

et les algorithmes utilisés pour recommander des contenus aux utilisateurs ; de nouvelles compétences pour examiner le fonctionnement des plateformes, notamment en facilitant l'accès des chercheurs aux données des plateformes clés ; de nouvelles règles sur la traçabilité des utilisateurs professionnels sur les places de marché en ligne, pour retrouver plus facilement les vendeurs de biens ou services illégaux ».

De même, ces nouvelles mesures s'attaqueront aux comportements néfastes des plateformes dites « contrôleurs d'accès » sur le marché numérique. Elles visent à définir et ensuite interdire les pratiques déloyales de la part des plateformes dites « contrôleurs d'accès », tout en mettant en place un mécanisme de contrôle du respect des règles sur des enquêtes de marché.

Un système de mise à jour des obligations afin de s'assurer de l'évolution constante de la réalité numérique est aussi prévu par ce projet de règlement.

Ces nouvelles mesures permettront à la Commission européenne de sanctionner directement les très grandes plateformes en vue de réguler les marchés numériques.

La nouvelle législation vise concrètement à réguler le marché numérique dans le respect des règles de la concurrence notamment : la mise en place des critères objectifs pour les services de plateforme essentiels les plus exposés aux pratiques déloyales en vue d'être désignés comme contrôleurs d'accès ; la définition des seuils pour déterminer les contrôleurs d'accès, permettre à la Commission après une enquête sur le marché de désigner des sociétés pour assurer la mission de contrôleur d'accès ; l'interdiction des pratiques manifestement déloyales ; l'instauration des sanctions en cas de non-respect des dispositions, des amendes pouvant aller jusqu'à 10 % du chiffre d'affaires mondial du contrôleur d'accès, afin de garantir l'effet utile des nouvelles règles. En cas de récidive, des mesures structurelles seront envisagées, pouvant aller jusqu'à la cession de certaines activités[9]...

Le 20 mai 2021, le Parlement européen a adopté une résolution sur le thème : « Façonner l'avenir du numérique de l'Europe ».

Deux points ont été abordés par cette résolution : supprimer les obstacles au bon fonctionnement du marché unique numérique et améliorer l'utilisation de l'IA pour les consommateurs européens.

D'abord pour les obstacles : il a été abordé la nécessité de créer une politique numérique en vue de soutenir les principaux fondements pour que les secteurs publics et privés soient des chefs de file mondiaux d'une innovation numérique fiable et centrée sur l'humain. Le Parlement considère que la crise de la Covid-19 a offert la possibilité d'accélérer la transition numérique et que la transformation numérique doit servir l'intérêt public dans son ensemble.

Le Parlement considère que la stratégie de l'Union en matière de transition numérique doit être conforme aux droits fondamentaux.

Le Parlement estime la nécessité d'éliminer les pratiques compromettant les droits des consommateurs, la protection des données et les droits des travailleurs.

Le Parlement est fortement convaincu que l'IA peut améliorer et offrir dans beaucoup de domaines comme dans les soins de santé des avantages et une

(9) Comm. CE, *Une Europe adaptée à l'ère du numérique : la Commission propose de nouvelles règles pour les plateformes numériques*, 15 déc. 2020 (https://ec.europa.eu/france/news/20201215/digital_services_act_fr).

valeur considérable lorsque le développement de l'IA est conforme à la législation applicable.

Pour améliorer l'utilisation de l'IA, il a été souligné la nécessité d'une collaboration efficace entre les différents acteurs au profit de l'IA, à savoir les États membres, la Commission, le secteur privé, la société civile et la communauté scientifique afin de créer un écosystème.

Il faut rassurer les consommateurs à travers la mise en place d'un cadre juridique clair et prévisible en cas de dysfonctionnement d'un produit.

## CONCLUSION

En somme, la crise du Covid-19 a prouvé que le numérique est devenu un outil indispensable à la consommation des produits et prestations de santé. Le numérique en santé permet la limitation des déserts médicaux, il contribue dans tous les territoires à favoriser l'accès aux soins et aux prises en charge médico-sociales. Le numérique dans la consommation des produits et prestations de santé n'est pas un phénomène *ex nihilo*. Le droit de l'UE et le droit français disposent d'un énorme arsenal juridique qui encadre le numérique en santé et la consommation des produits de santé, dont la violation de ces règles juridiques est assortie de sanction de diverses natures.

Aujourd'hui, les bénéfices qu'apporte le numérique au patient-consommateur sont prometteurs. Ces bénéfices sont sans doute supérieurs aux risques encourus lorsque son utilisation raisonnable s'appuie sur les données acquises dans la science médicale.

CHAPITRE 10

# IMPACT DU NUMÉRIQUE SUR LE MODE DE CONSOMMATION DU « PATIENT-CONSOMMATEUR » DES PRODUITS DE SANTÉ CONNECTÉS

Béatrice ESPESSON-VERGEAT

L'explosion du secteur numérique et des objets connectés, dotés d'une intelligence artificielle, révolutionne le secteur de la santé. De l'auto-évaluation de la personne à la prise en charge et l'assistance dans la prévention, le suivi et le traitement du patient, la protection de la santé personnelle et de la santé publique est désormais intrinsèquement liée à celle du numérique et au développement des objets connectés. La santé est un bien à protéger et le patient un consommateur, qui se forme et s'informe à l'exploitation des données des produits connectés pour améliorer sa situation, en naviguant dans un univers à l'échelle planétaire. Le regard sur les relations juridiques entre les acteurs change et transforme les professionnels de santé et patients en partenaires engagés ensemble dans la prévention et le soin. Les relations évoluent en fonction du statut des produits connectés oscillant entre produits de bien-être, dispositifs médicaux, voire médicaments connectés. Tout indique, face aux perspectives de croissance de ce marché, que cette complexification ne fera que croître, et nécessitera une classification et une normalisation de ce secteur afin de clarifier les responsabilités et garantir la protection des données personnelles et données de santé dans un contexte marqué par les cyberattaques et cybercriminalité.

## INTRODUCTION

Il n'est pas un jour où un torrent d'informations ne se déverse sur l'évolution du marché des objets connectés dans le secteur de la santé entendu au sens large, à savoir les secteurs de la prévention, du traitement et du suivi de populations saines ou malades. L'Internet des objets de santé (*Internet of Things*), est un marché engagé

dans une fascinante expansion. Les *wearables*, ou technologies portables, et autres accessoires de santé sont les premiers à être mis en avant : bracelets, montres, balances et autres *trackers* d'activité. Mais l'univers des objets connectés va bien au-delà et envahit toute la sphère de la santé au centre de laquelle se trouve le patient devenu un sujet actif, voire hyperactif au risque d'atteinte à ses données personnelles et données de santé[1]. La définition de ce secteur est confuse, recourant à des formulations telles que e-santé, m-santé[2], numérique, objets de santé connectés, application mobile, santé mobile[3], télémédecine[4]. D'une manière très générale, le terme e-santé recouvre un vaste domaine d'application des technologies de l'information et de la télécommunication au service de la santé et permet de cibler l'ensemble des produits ou services que le « patient-consommateur » a à sa disposition dans une nouvelle approche de la santé connectée[5].

Ce déferlement du numérique dans la vie du « consommateur-patient » est porté par l'engagement de l'OMS, où un département dédié au numérique a été créé en mars 2019 en réponse à une résolution adoptée en 2018 afin que l'OMS mette en place une stratégie mondiale sur l'évaluation des technologies numériques dans un objectif d'utilisation sûre et éthique. Elle recommande notamment aux États de légiférer sur l'utilisation des données et sur l'encadrement des objets connectés de santé. Le numérique est soutenu par l'action de l'Union européenne et des autorités nationales engagées vers la santé globale avec et grâce à la santé connectée autour du patient acteur, actif et moteur dans la gestion de sa santé[6]. Le chantier du développement de l'e-santé dans l'Union européenne est axé sur des objectifs d'interopérabilité entre pays membres, dans l'intérêt des patients, des professionnels et des systèmes de santé, tout en favorisant le développement d'un marché pour les industriels européens. En France, le numérique est un axe majeur du plan « Ma santé 2022 » présenté en septembre 2018 par le gouvernement[7], et son volet opérationnel, visant l'exploitation des données de santé au service du bien commun, envisage la préfiguration d'un *Health Data Hub*[8].

C'est un changement total de paradigme dans la santé qui trouve son origine dans les années 2000 avec le concept d'e-santé et concomitamment l'apparition d'un nouveau patient, consommateur de services et de produits de santé. Cette révolution se caractérise par une prolifération de *startups* et d'innovation en e-santé et m-santé, dans un univers global encore inadapté au plan juridique.

(1) D. Gruson, *Le numérique et l'intelligence artificielle en santé : surveillance généralisée ou avancée majeure ? : Les Tribunes de la santé* 2019, vol. 60, n° 2, p. 23-29.
(2) « mHealth » pour *Mobile Health*.
(3) OMS, *Santé mobile : utilisation des technologies mobiles sans fil pour la santé publique*, 27 mai 2016, EB139. – OMS, *Utilisation des technologies numériques appropriées pour la santé publique*, 27 nov. 2017, EB142/20.
(4) L'article 78 de la loi n° 2009-879 du 21 juillet 2009 dite « HPST » (hôpital, patients, santé et territoires) définit pour la première fois la télémédecine (C. santé publ., art. L. 6316-1).
(5) HAS, Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (*Mobile Health* ou *mHealth*), oct. 2016.
(6) CESE, Avis sur la « Promotion d'un marché unique européen associant génie biomédical et industrie des services médicaux et de soins » (2015/C 291/07).
(7) D. Pon et A. Coury, *Stratégie de transformation du système de santé : Accélérer le virage numérique*, Rapport final, Paris, Ministère chargé de la santé, 2018.
(8) Rapport de C. Villani, *Donner un sens à l'intelligence artificielle*, 28 mars 2018, mise à jour 28 nov. 2018.(www.enseignementsup-recherche.gouv.fr/cid128577/rapport-decedric-villani-donner-un-sens-a-l-intelligence-artificielle-ia.html).

Cette croissance fulgurante de la santé numérique n'en est qu'à son début. Elle laisse entrevoir de profonds bouleversements sociétaux dans l'approche de la santé et dans les modes d'exercice des pratiques professionnelles liées à la santé et aux soins, ce qui est pointé dans une multitude d'études économiques prospectives[9]. Les récentes études démontrent une rapidité d'adaptation aux nouveaux outils et techniques de la part des professionnels de santé[10] et une croissance exponentielle, voire inquiétante, du secteur dont la valeur du marché mondial de la santé numérique atteindrait 234,5 milliards de dollars d'ici 2023, soit une hausse de près de 160 % par rapport à 2019. Le nombre d'objets connectés serait d'environ 80 milliards en 2020 avec environ trente objets connectés par foyer, ce qui est considérable et qui ne va cesser d'augmenter en générant des risques majeurs concernant la protection des données personnelles et de santé.

En l'état actuel, les utilisateurs, professionnels de santé et personnes physiques, sont confrontés à une démultiplication des produits dont la qualification juridique implique de faire la distinction entre les objets connectés de santé, les dispositifs médicaux connectés, et les objets connectés de bien-être créant un besoin d'encadrement juridique et de régulation, ce qui est pointé par la Haute Autorité de santé (HAS) dans un référentiel d'octobre 2019 sur l'utilisation de ces outils où elle annonce 101 règles de bonnes pratiques[11].

Une orientation vers une forme d'accompagnement juridique agile, flexible portant sur ces outils est préconisée.

L'un des objectifs de l'e-santé est de mieux suivre les patients, notamment ceux atteints de maladies chroniques. Grâce aux objets connectés, aux applications mobiles et aux plateformes en ligne, ils transmettent plus régulièrement leurs données aux praticiens.

Cette prolifération s'accompagne d'une multitude de nouveaux termes, dont le contenu est variable d'un pays à un autre, qui visent à définir de nouveaux secteurs d'activités, produits, ou pratiques professionnelles[12] (« e-santé, m-santé, domotique, télémédecine, *self quantified*, *etc.*). Le recours à ces terminologies, qui caractérise une révolution dans la prise en charge du patient, dans les rapports entre professionnels de santé et patients et dans l'organisation du soin avec la télémédecine[13], génère et entretient aussi la confusion entre la description des caractéristiques du produit, son usage, sa fonction, son utilisation, sa revendication et sa finalité. Le règlement général sur la protection des données du 27 avril 2016, la loi pour une République numérique du 7 octobre 2016, ajoutés à la loi Informatique et Libertés du 6 janvier 1978 modifiée par la loi n° 2018-493 du 20 juin 2018

(9) LEEM, Santé 2025, *Un monde d'innovations*.

(10) H. Chaput et M. Monziols (DREES), B. Ventelou et A. Zaytseva (AMSE), L. Fressard et P. Verger (ORS Paca), M.-C. Bournot, J.-F. Buyck et A. Jolivet (ORS Pays de la Loire), F. Zemour (URPS-ML Provence-Alpes-Côte d'Azur), T. Hérault (URML Pays de Loire), *E-santé : les principaux outils numériques sont utilisés par 80 % des médecins généralistes de moins de 50 ans : Études et Résultats* janv. 2020, n° 1139, DREES.

(11) HAS, *La e-santé & la m-santé, Des avantages concrets pour vos patients*, oct. 2019, (www.has-sante.fr/upload/docs/application/pdf/2019-10/e_sante_essentiel_en_4_pages.pdf).

(12) ASIP, Étude pour l'accompagnement au déploiement de la télémédecine, Étude comparative sur le développement de la télémédecine à l'international, juill. 2019.

(13) M. Dubreuil, *E-santé : décryptage des pratiques et des enjeux*, Observatoire régional de santé Île-de-France. 2019. – IRDES, *La e-santé Télésanté, santé numérique ou santé connectée*, Bibliographie thématique, juill. 2019.

et aux nombreux textes relatifs à la télémédecine, constituent la base légale au développement de la e-santé. En conséquence, dans l'analyse de la qualification du produit et de son statut, l'ensemble de ces critères devra être pris en considération afin d'identifier la réglementation applicable et, en conséquence, les obligations et responsabilités des fabricants et utilisateurs, qu'il s'agisse des professionnels de santé ou du patient lui-même.

Les modes d'utilisation révèlent une confusion des statuts entre le patient devenu consommateur de produits et services de santé « patient-consommateur » ou le consommateur devenu, ou qui va devenir, patient « consommateur-patient ».

Ce mélange des genres entre les produits toujours plus performants avec une accélération de l'innovation technologique, couplé au caractère évolutif de la situation de santé de la personne au cours de son existence, perturbe l'analyse de la relation de l'objet connecté avec le « patient-consommateur » connecté, et suppose une approche avec un double regard (Section 1) sous l'angle de l'objet connecté et de sa revendication par le fabricant et sous l'angle des comportements de l'utilisateur final, ce qui va conduire à lui conférer un statut de « patient-consommateur » ou « consommateur-patient », sachant que chacun entrera tour à tour au cours de son existence dans une situation ou l'autre. Cela ne devrait pas affecter la qualification initiale du produit ; pourtant, la question pourra se poser de savoir si le statut de la personne utilisatrice, et l'action attendue du produit peuvent conduire à reconsidérer la fonction initiale auquel le fabricant a destiné le produit, mais dont l'évolution a dépassé sa prévision.

Dans ce contexte extrêmement mouvant et évolutif, une distinction claire est indispensable permettant de reconnaître ceux qui ont une revendication en termes de santé de ceux qui entrent dans le champ du bien-être (Section 2).

Si l'analyse de la relation entre le consommateur et les objets connectés de bien-être présente un intérêt majeur, largement documenté par d'importantes études, l'intérêt réside ici plus spécifiquement dans l'analyse de la relation entre le produit connecté de santé, *a priori* dispositif médical (DM), par une personne dont le statut est évolutif, passant d'une relation de consommation à une relation de soin avec le produit connecté.

SECTION 1

## LA RELATION ENTRE L'OBJET CONNECTÉ ET L'UTILISATEUR DANS SON OBJECTIF DE SANTÉ

La formulation « patient-consommateur » ou « consommateur-patient » peut, au plan juridique, porter à confusion et soulever des contestations.

La définition juridique du consommateur[14] est donnée par le Code de la consommation, lequel retient qu'est considérée comme consommateur « toute

(14) Pour la première fois, le législateur, *via* la loi n° 2014-344 du 17 mars 2014 relative à la consommation, dite « loi Hamon », a fourni une définition générale du consommateur.

personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole » (C. consom., art. liminaire). Il s'agit d'une définition « relative », en ce sens qu'elle ne vaut qu'au sens du Code de la consommation. À côté du consommateur, ledit code a institué la catégorie du non-professionnel, c'est-à-dire toute personne (y compris une personne morale) qui agit en dehors de sa profession.

La formulation choisie ne vise donc pas à créer une nouvelle catégorie de consommateur, mais à marquer le statut hybride du consommateur qui, au cours de son existence, cumulera les statuts de patient et de consommateur, ou donnera une dimension consumériste à la prise en charge de sa santé.

Dans le secteur de la santé, l'analyse du comportement du patient dans sa dimension consumériste avec les produits de santé a conduit, au plan réglementaire et sur le terrain économique et sociologique, à s'intéresser au passage du statut de patient passif à celui d'acteur dynamique et décisionnaire.

L'entrée du numérique dans la vie de la Cité et dans tous ses aspects publics et privés contraint à une adaptation rapide, immédiate, incontournable à l'utilisation des objets et applications connectés dans la vie quotidienne et dans la prise en charge de la santé[15]. Ce passage modifie la posture du patient et la dissymétrie d'information entre le sachant, représenté par le professionnel de santé, et le sujet patient[16]. Il ouvre un espace d'information, de connaissance et d'autonomie de décision au patient qui modifie son statut. Toute la question est alors d'identifier l'impact de ces évolutions comportementales sur l'analyse juridique du statut du produit connecté, le plus souvent autonome et doté d'une intelligence artificielle.

## § 1. – Le passage du patient au « patient-consommateur » connecté

L'interrogation sur la protection du « patient-consommateur » a débuté dès l'utilisation d'Internet dans la santé[17]. Le patient est devenu au fil du temps un consommateur de soins, de produits et de services de santé[18]. La naissance du terme « patient-consommateur » remonte aux travaux portant sur l'autonomisation du patient dans la prise en charge de sa santé et la reconnaissance de ses droits[19]. Cette terminologie a donné lieu à de très nombreuses études en santé publique et sociologie, mais peu sur le terrain du droit. Les approches centrées sur

(15) M. Al Dahdah, *mHealth : l'information de santé ubique ? : Le Temps des médias* 2014, vol. 23, n° 2, p. 52-65.

(16) C. Le Pen, *« Patient » ou « personne malade » ? Les nouvelles figures du consommateur de soins : Rev. éco.* 2009, vol. 60, n° 2, p. 257-271. – A. Sarradon-Eck, *Le patient contemporain : Cancer(s) et psy(s)* 2019, vol. 4, n° 1, p. 51-60.

(17) M. Hardey, *Internet et société : reconfigurations du patient et de la médecine ?*, in *Sciences sociales et santé* 2004, vol. 22, n° 1, in Dossier ss dir. M. Akrich, C. Méadel, J. Pierret et V. Rabeharisoa, « Les technologies de l'information à l'épreuve des pratiques », p. 21-43.

(18) C. Le Pen, *« Patient » ou « personne malade » ? Les nouvelles figures du consommateur de soins : Rev. éco.* 2009, vol. 60, n° 2, p. 257-271.

(19) J.-P. Pierron, *Une nouvelle figure du patient ? Les transformations contemporaines de la relation de soins : Sciences sociales et santé* 2007/2, vol. 25, p. 43-66. – P. Batifoulier, J.-P. Domin et M. Gadreau. *Mutation du patient et construction d'un marché de la santé. L'expérience française : RF Socio-Économie* 2008, vol. 1, n° 1, p. 27-46. – P. Batifoulier, *Le marché de la santé et la reconstruction de l'interaction patient-médecin : RF Socio-Économie* 2012, vol 10, n° 2, p. 155-174.

la personne (*patient-centred* ou *client-oriented*, voire *family* ou *community-centred*) ont imprégné la loi Hôpital, Patient, Santé, Territoires (HPST, 2009) en France, et intègrent deux dimensions : le patient et l'intervenant. Cette vision conduit à une approche intégrative de tous les acteurs qui interviennent dans son protocole de soins et sa trajectoire de vie afin que la prise en charge, notamment des pathologies chroniques, soit optimale d'un point de vue clinique et organisationnel[20]. C'est dans ce contexte qu'apparaît l'impact du numérique comme support à la mise en œuvre de cette politique de santé, et ce tout particulièrement dans la stratégie « Ma santé 2022 »[21]. Cette loi poursuit la politique de santé engagée vers la reconnaissance des droits (et devoirs) du patient dans la prise en charge de santé, dont le pilier est le consentement éclairé[22]. Pour rappel, la notion de droit des patients est évoquée pour la première fois, dans l'histoire du droit français, dans l'arrêt *Teyssier* du 28 janvier 1942[23]. Une jurisprudence suivie par le législateur, en 1946, dans le préambule de la Constitution qui reconnaît le droit à la protection de la santé[24], puis, en 1988 avec la loi Huriet qui formalise le droit au consentement[25], la loi Kouchner du 4 mars 2002, relative aux droits des malades et à la qualité du système de santé[26], la loi Leonetti de 2005 qui a complété les droits du patient avec des dispositions concernant notamment les droits des malades en fin de vie[27], puis la loi du 26 janvier 2016 de modernisation du système de santé qui renforce les droits et la sécurité des patients[28], pour arriver à la loi Buzin, consacrant le numérique en santé dans une approche globale[29] et intégrant les mesures de la stratégie nationale de santé, « Ma santé 2022 », dans laquelle le profil du patient est désormais connecté.

Le « patient-consommateur » est qualifié comme tel par le fait qu'il conçoit la santé comme un droit et se saisit de son pouvoir (*empowerment*)[30] pour choisir les soins et les produits, sur un marché de la santé révolutionné par l'ubérisation[31]. Il devient un partenaire dans l'organisation de son parcours de soins et modifie sa relation aux professionnels de santé en intégrant la dimension numérique et l'interface des plateformes numériques, permettant notamment aux GAFAM de se positionner fortement et de collecter largement ses données personnelles et de santé. Le colloque singulier entre le patient et le professionnel de santé intègre désormais l'usage de la technologie, faisant pénétrer dans cette sphère privée les acteurs économiques et une forme marquée de consumérisme en santé.

(20) Sebai Jihane et Fatima Yatim, *Approche centrée sur le patient et nouvelle gestion publique : confluence et paradoxe : Santé publique* 2018, vol. 30, n° 4, p. 517-526.
(21) Dossier d'information « Ma santé 2022 » – Un engagement collectif (https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/ma-sante-2022-un-engagement-collectif).
(22) V. Siranyan et O. Toucas, *L'évolution des normes face au développement des objets de santé connectés : Médecine et Droit* oct. 2019, Issue 158, p. 130-136.
(23) Cass. civ., 28 janv. 1942, *Teyssier : D.* 1942, jurispr. p. 63 ; *Gaz. Pal.* 1942, 1, jurispr. p. 177.
(24) Const. 27 oct. 1946, Préambule, art. 11.
(25) Loi Huriet n° 88-1138, 20 déc. 1988.
(26) Loi Kouchner n° 2002-303, 4 mars 2002, relative aux droits des malades et à la qualité du système de santé.
(27) Loi Leonetti n° 2005-370, 22 avr. 2005, relative aux droits des malades et à la fin de vie.
(28) L. n° 2016-41, 26 janv. 2016, de modernisation de notre système de santé. – Ministère des Affaires sociales, de la Santé et des Droits des femmes, Dossier de presse, 28 janv. 2016.
(29) L. n° 2019-774, 24 juill. 2019, relative à l'organisation et à la transformation du système de santé.
(30) A.-S. Cases, *L'e-santé : l'empowerment du patient connecté : Journal de gestion et d'économie médicales* 2017, vol. 35, n° 4, p. 137-158.
(31) D. Bazin-Beust, *La santé et les droits du consommateur : RGDM* 2010, n° 14, p. 129-152.

Si le professionnel de santé doit être formé sur de nouvelles bases à la relation avec le patient dans un contexte numérique, le « patient-consommateur » doit lui aussi être formé, informé, accompagné dans un consentement éclairé, avec la plus grande vigilance et prudence. Et notamment l'utilisation des outils d'aide à l'automédication, complétés par des applications donnant la possibilité d'achat en ligne des produits de santé, sur des plateformes commerciales gérées par les GAFAM pose, au niveau national, et européen, la question de la sécurité des comportements d'automédication et celle de la nécessité du contrôle médical et pharmaceutique, rendant encore plus prégnante la protection des monopoles pharmaceutique et médical.

Cela étant, l'e-santé et les objets connectés sont considérés par le législateur, dans la loi du 24 juillet 2019 sur l'organisation et la transformation du système de santé, comme un moyen d'assurer la prévention, la gestion des addictions, l'accélération de l'accès aux professionnels de santé, aux services et aux produits de santé, et notamment dans les déserts médicaux, grâce à l'implantation de cabines connectées de consultation, ou encore celle de la pénurie des médecins généralistes ou spécialistes par la consultation à distance, et comme un atout majeur en termes de recherche clinique ou épidémiologique. À cela s'ajoute le DMP : un dossier médical partagé sera automatiquement ouvert à toute personne née à compter du 1er juillet 2021 et, au plus tard le 1er janvier 2022, tous les patients auront accès à un espace numérique de santé accessible en ligne (ce qui suppose un accès Internet pour tous).

La réactivité du « patient-consommateur » se traduit notamment par la prise de décision en dehors du circuit médical organisé et du parcours de soins, et par le recours à la télémédecine qui lui permet de compléter le circuit classique de consultation chez son généraliste puis spécialiste, pour avoir une téléconsultation à tout moment, dont le remboursement est organisé. L'avenant n° 6 à la Convention nationale, approuvé par un arrêté du 1er août 2018, fixe les tarifs des actes de téléconsultation et de télé-expertise et en prévoit le cadre de mise en œuvre(32). Au-delà de son bienfait simplificateur dans l'accès aux soins, l'organisation de ces pratiques basée sur l'e-santé, entendue dans un sens large, comporte un biais en ce qu'elle peut conduire, d'une part, à une aggravation des inégalités entre les citoyens qui ont ou non accès au numérique et, d'autre part à la surconsommation de produits de santé ou de soins, voire à la recherche d'une source d'enrichissement par la valorisation de ses données de santé. Cette difficulté, pointée par le Conseil national de la consommation(33) et par la Haute Autorité de santé (HAS), devrait dans la politique numérique lancée par les pouvoirs publics se réduire avec l'adoption des mesures visant à l'augmentation de la couverture numérique et l'accès pour tous(34).

(32) Collège de la HAS, déc. n° 2018.0057/DC/SA3P, 4 avr. 2018, portant adoption de la fiche mémo intitulée « Qualité et sécurité des actes de téléconsultation et de télé expertise ».

(33) S. Bernheim-Desvaux, *L'objet connecté sous l'angle du droit des contrats et de la consommation : Contrats, conc. consom.* janv. 2017, n° 1.

(34) Le Plan France Très Haut Débit vise à couvrir l'intégralité du territoire en très haut débit d'ici 2022. En 2017, le Président de la République a ajouté un objectif de cohésion visant à garantir un accès au bon haut débit pour tous d'ici 2020.

Au fil du temps, le patient passif est donc devenu actif, puis acteur[35], consommateur[36], moteur, décideur et désormais un « patient connecté » influenceur[37], voire lanceur d'alerte[38], avec une élasticité dans la période de vie liée au vieillissement de la population. Les personnes âgées de soixante ans et plus seront près de 24 millions en 2060 et auront un besoin croissant d'équipements domestiques en objets connectés, de bien-être, de confort, de soins, de prévention, de traitement ou de surveillance, objets qui collectent en permanence les données personnelles, de vie privée et professionnelle, données de santé et médicales qui posent la question de leur protection sachant qu'une donnée personnelle qui n'est pas une donnée de santé par nature peut le devenir du fait de son croisement avec d'autres données. Le « patient-consommateur » constamment connecté accepte de transmettre l'ensemble de ses données en contrepartie d'un service au travers de l'objet connecté. Il permet ainsi l'exploitation et la valorisation de ses données par lui-même et par l'ensemble des acteurs directs ou indirects, intermédiaires qui captent les informations, ce qui constitue l'enjeu économique majeur bouleversant le système de santé, laissant se profiler la question de la monétisation des données de santé[39] et celle de la nature juridique des données, attachées à la personne ou de biens ayant un statut de valeurs incorporelles. Ce sujet brûlant d'actualité aux USA, portant sur l'infraction des GAFAM (et notamment Google)[40] au *Health Insurance Portability and Accountability Act* (HIPAA) dans leur comportement de captation des données des établissements de santé et dans leur mode de rémunération des patients transférant leurs données de santé ne manquera pas de trouver un écho au sein des États membres.

Certes, au niveau européen, la protection des données est assurée par le règlement général de la protection des données (RPGD)[41], transposé en France dans la loi sur la protection des données personnelles[42]. Selon le considérant 35 du RPGD :

> « Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil au bénéfice de cette personne physique ».

(35) M. Girer, *Les droits des patients : les enjeux d'une autonomie affirmée. Commentaire : Sciences sociales et santé* 2014, vol. 32, n° 1, p. 29-37.

(36) C. Le Pen, *« Patient » ou « personne malade » ? Les nouvelles figures du consommateur de soins : Rev. éco.* 2009, vol. 60, n° 2, p. 257-271.

(37) « Un influenceur (ou blogueur, vlogueur…) est un individu exprimant un point de vue ou donnant des conseils (par écrit, audio et/ou visuel) dans un domaine spécifique et selon un style ou un traitement qui lui sont propres et que son audience identifie. »

(38) L. n° 2016-1691, 9 déc. 2016, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique. La loi Sapin 2 définit le lanceur d'alerte comme toute personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un fait dont il a eu personnellement connaissance et qui constitue notamment un crime ou un délit, une menace ou un préjudice grave pour l'intérêt général ou une violation grave et manifeste d'un engagement international.

(39) D. Desbois, *Le Marché unique numérique des données et la santé à l'heure du RGPD : les spécificités de la santé publique en Europe*, in *I2D – Information, données & documents* 2019, n° 1, p. 29-33.

(40) E. Wery, *Nightingale, le nouveau scandale « made in Google » : Droit et Technologies* nov. 2019.

(41) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 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) et son rectificatif : *JOUE* n° L 1272, 23 mai 2018.

(42) L. n° 2018-493, 20 juin 2018, relative à la protection des données personnelles.

Depuis une recommandation du 27 mars 2019, les données de santé appartiennent à une catégorie particulière qui bénéficie d'un niveau de protection plus élevé en raison du risque de discrimination pouvant résulter du traitement de ces données. L'article L. 1110-8 du Code de la santé publique organise le dépôt et la conservation des données de santé à caractère personnel afin de garantir leur confidentialité et leur sécurité.

Par ailleurs, au niveau national, le patient dispose d'un droit à la protection absolue des données médicales (C. santé publ., art. L. 1110-4) et du secret médical. Les données de santé sont donc distinctes des données médicales, mais elles sont aussi protégées. Mais concrètement, la sécurisation complète des données dans le secteur de la santé est très loin d'être résolue(43).

Pour preuve, la lutte contre la cybercriminalité, notamment dans les établissements de santé publics et privés, détenteurs des données de santé et de vie du patient, est un sujet brûlant qui suscite la mobilisation des États et de l'Union européenne, sachant que le risque peut être généré par le « patient-consommateur » connecté lui-même. Les mesures de précaution à l'attention des établissements de santé, responsables de traitement et professionnels de santé se multiplient dans un contexte d'interopérabilité des systèmes d'information qui oblige à ouvrir les réseaux tout en renforçant leur sécurité conformément aux exigences du RGPD (art. 32 notamment).

Désormais, ce renforcement de l'intervention du patient se caractérise par la mise à disposition d'informations médicales sur sa maladie et ses traitements, rendue plus effective par le dossier médical partagé (DMP) qui continue de soulever de nombreux questionnements pour la protection des données au sein du nouveau *Health Data Hub*.

Mais l'action du « patient-consommateur » se manifeste également à travers son témoignage auprès d'autres patients ou de leur entourage. Cette évolution historique transforme la dissymétrie d'information entre le professionnel de santé et le patient, lequel est désormais informé par diverses sources officielles, scientifiques ou non(44), et devient un évaluateur, blogueur, influenceur, avec toutes les conséquences encore inconnues sur l'organisation et la sécurité du système de santé(45). Notamment apparaissent des problématiques nouvelles liées au traitement des fausses informations ou *fake news* pouvant entraîner des postures à risque dans la population. Ces comportements à risque expliquent la recherche d'une voie permettant de renforcer ou repenser l'encadrement juridique(46) de l'information par une norme contraignante ou par une régulation souple(47). La décision individuelle du patient connecté, qu'il prend sur le fondement d'un traitement algorithmique

(43) S. de Silguy, *E-santé et protection de la vie privée : à la recherche d'un équilibre : Rev. Lamy dr. civ.* 1er déc. 2016, n° 143.
(44) H. Nabarette, *L'Internet médical et la consommation d'information par les patients : Réseaux* 2002, vol. 114, n° 4, p. 249-286.
(45) M. del Río Carral, A. Schweizer, A. Papon et M. Santiago-Delefosse, *Les objets connectés et applications de santé : étude exploratoire des perceptions, usages (ou non) et contextes d'usage : Pratiques psychologiques* mars 2019, vol. 25, Issue 1, p. 1-16.
(46) M. Griguer, *Quel cadre légal pour l'e-santé ? : CDE* sept. 2016, n° 5.
(47) P. Besse, C. Castets-Renard et A. Garivier, *Loyauté des décisions algorithmiques : contribution au débat public initié par la CNIL*, Éthique et numérique, 2017.

de l'objet connecté et qu'il retransmet à la communauté de patients, implique de s'assurer et d'encadrer la confiance et la loyauté. Dans ce contexte, les notions de précision, transparence ou explicabilité des décisions, et biais des algorithmes, sont centrales pour aborder la « loyauté » de ces derniers et les questions éthiques envers le « patient-consommateur ».

En conséquence, le « patient-consommateur connecté », bien qu'il demeure avant tout un patient protégé au regard du droit de la santé, doit avoir connaissance de ses droits mais aussi désormais de ses obligations en tant qu'acteur actif, consommateur de services[48].

L'analyse de son consentement doit s'effectuer à un double niveau, envers le professionnel de santé, mais aussi face à l'intermédiaire qui fournit l'objet connecté et va collecter les données personnelles et de santé.

À l'égard du patient, le principe est toujours celui du libre choix du professionnel de santé, qui doit donc être assuré par l'objet connecté ou la plateforme utilisée (C. santé publ., art. L. 1110-8 ; CSS, art. L. 162-2). Il s'agit d'un principe fondamental et incontournable protégé par l'article 34 de Constitution. L'article 36 du Code de déontologie médicale (C. santé publ., art. R. 4127-36) et ses commentaires définissent précisément les modalités de recueil du consentement du patient. La recherche du consentement éclairé du patient préside toujours dans la relation de santé. Le consentement, clé de voûte dans le secteur de la santé, ne répond pas aux canons obligationnels du droit des contrats imposés par la Cour de cassation. La vulnérabilité du patient, à laquelle s'ajoute le risque d'incompréhension de l'information, fait de la relation de santé une situation spécifique. Si le numérique permet d'accéder à une information plus rapide, il ne garantit pas sa fiabilité, et encore moins la compréhension du système de gestion de l'information par l'objet connecté ou l'application interfacés avec les professionnels de santé. Cela implique donc pour les acteurs de santé et prestataires, de s'assurer d'une communication claire, transparente et compréhensible sur la sécurisation des modes de transmission, la qualification des hébergeurs de données, l'évaluation de la vulnérabilité de l'objet, le parcours des données permettant d'informer les patients, les professionnels de santé, et garantir une sécurisation suffisante. Cette obligation est clairement prévue par l'article R. 6316-2 du Code de la santé publique, lequel stipule que les actes de télémédecine sont réalisés avec le consentement libre et éclairé de la personne, en application notamment des dispositions des articles L. 1111-2 et L. 1111-4 du Code de la santé publique, et par l'article R. 6316-10 du même code concernant les obligations des organismes et professionnels de santé utilisateurs des technologies de l'information et de la communication.

Dans le cadre de l'utilisation d'un objet connecté, plutôt que de consentement éclairé de la part du « patient-consommateur », qui ne sait pas par qui, comment, et dans quel but ses données peuvent être utilisées, intentionnellement ou non, directement ou indirectement, il conviendrait donc de parler de comportement éclairé de la part du consommateur, dans une pratique de *privacy by using*. Dans

(48) J. Lucas, *Le partage des données personnelles de santé dans les usages du numérique en santé à l'épreuve du consentement exprès de la personne*, in *Ethics, Medicine and Public Health* janv.-mars 2017, vol. 3, Issue 1, p. 10-18.

cette vision, il serait moins demandé aux personnes de donner leur consentement initial à une opération que d'apprendre et d'être en situation d'apprendre quelles sont les conséquences de la divulgation de leurs informations lors de l'utilisation de l'objet connecté. Avec cette notion de comportements éclairés, devrait apparaître une nouvelle norme de protection intégrée dès la conception de l'objet connecté, avec pour conséquence de nouvelles conventions, éventuellement codifiables par le droit, destinées à encadrer l'exploitation commerciale des données du « patient-consommateur » par les courtiers de données.

Le sujet est d'autant plus épineux lorsqu'il s'agit d'un « patient-consommateur » dont la capacité de raisonnement peut décroître avec l'âge ou la pathologie, et qui devra donc avoir l'assistance des professionnels de santé, d'une personne de confiance, d'un aidant ou de la famille. Tout le problème est de réduire l'asymétrie informationnelle et la méconnaissance des conséquences des comportements de divulgation, sans faire porter une charge cognitive trop élevée sur les individus, d'où la nécessité d'un processus adaptatif fondé sur l'apprentissage du « patient-consommateur » et du professionnel de santé. Cet apprentissage est assuré par le fabricant du produit et fournisseur du service avec la nécessité d'encadrer la relation et de distinguer entre formation, information et publicité effectuée par le fabricant.

Au cas par cas, il convient donc de clarifier la situation juridique du « patient-consommateur », utilisateur d'un produit connecté intelligent qui peut interférer dans la décision médicale.

Cela suppose alors d'identifier ce qu'il faut entendre par objet connecté dans le secteur de la santé en distinguant les dispositifs médicaux des objets connectés autres, de bien-être, qui apportent une information préventive en santé.

## § 2. – De l'objet connecté à l'objet connecté de santé, il n'y a qu'un pas

Les objets connectés ou l'Internet des Objets (IdO)/ *Internet of Things* (IoT) sont parmi les locutions les plus rémanentes du moment.

Dans le secteur de la santé, aucune définition juridique n'a été identifiée spécifiquement pour les objets connectés. Ils sont présentés par la Haute Autorité de santé (HAS) comme « des dispositifs connectés à l'Internet pouvant collecter, stocker, traiter et diffuser des données ou pouvant accomplir des actions spécifiques en fonction des informations reçues »[(49)].

S'agissant des applications mobiles, l'Organisation mondiale de la santé (OMS) les définit en 2011 comme des « pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs de surveillance des patients, les PDA (*Personal Digital Assistant*) et autres appareils sans fil »[(50)].

(49) HAS, Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (*Mobile Health* ou *mHealth*), oct. 2016.

(50) Autorité de régulation des communications électroniques et des postes (Arcep), Conseil général de l'économie (CGE), Agence du Numérique-CREDOC, Baromètre du numérique 2017.

L'objet connecté est par essence un produit disposant d'une connexion à Internet et permettant de communiquer une information, relier des personnes entre elles afin d'établir à travers l'objet la transmission d'une information, ou encore un objet connecté qui a la capacité d'apprendre et contient une intelligence dite « artificielle ».

La définition de l'Internet des Objets (IdO)[51] est vaste. Les usages sont multiples et vont de l'équipement de la maison en domotique aux nanorobots en médecine. La santé est l'un des secteurs phares permettant l'association de grands opérateurs des GAFAM avec l'industrie pharmaceutique et des produits de santé, dans la perspective d'une médecine préventive, prédictive, personnalisée, participative[52] utilisant une intelligence artificielle « petite » ou « grande ». L'invasion de ces nouveaux objets dans le quotidien du « patient-consommateur » provoque une circulation de toutes les données personnelles, de santé et médicales, ce y compris celles de son entourage connecté aux mêmes produits. Cette pratique numérique expose les utilisateurs et les patients aux failles de sécurité et à la cybercriminalité dont les effets sont dramatiques en santé publique, ce qui justifie l'élaboration d'une réglementation très protectrice au sein des États, au niveau européen, voire international. Au-delà de la captation des données, c'est toute la sécurité du patient qui est en cause dans la mesure où le détournement de la fonction d'un dispositif médical implantable sur un organe vital peut avoir un effet létal pour le patient.

La toute première difficulté réside dans la qualification et la classification de cet objet connecté qui permet une multitude d'usages, et dont les frontières sont extrêmement floues, non seulement parce que le produit a intrinsèquement une fonction évolutive qui implique une approche juridique agile, mais aussi parce qu'en raison d'une politique de santé ouverte sur la reconnaissance des pratiques préventives telles que le sport, l'objet connecté devient un outil d'évaluation de la vie en bonne santé. Cette assistance dans la prise en charge de la prévention afin de vivre et vieillir en bonne santé est une conséquence de l'application des recommandations de l'OMS[53], de la Commission européenne et enfin de la politique nationale avec la stratégie globale « Vieillir en bonne santé 2020-2022 » lancée le 16 janvier 2020[54].

Nombreux sont les commissions et les rapports dans le cadre des politiques de santé successives qui se sont penchés sur la question du numérique dans la vie du patient connecté, pointant le risque de rupture d'égalité entre les patients connectés ou non[55] et la nécessité de prendre des mesures visant à faciliter l'accès à Internet[56].

Cette frontière entre les différentes catégories de patients connectés ou non dans le périmètre de la santé vient croiser la classification des patients considérés

(51) Le concept d'*Internet of Things* est né en 1999 au centre Auto-ID du MIT. L'idée était d'associer un tag RFID (identification par radiofréquence) à chaque objet du monde réel pour pouvoir à tout instant et à distance : l'identifier, l'inventorier et tracer ses déplacements.

(52) L'industrie du futur, enjeux et perspectives pour la filière industries et technologies de santé, Ministère de l'Économie et des Finances, juin 2019.

(53) OMS, *Vieillir en bonne santé : politiques et interventions prioritaires*, 2012, Stratégie et plan d'action pour vieillir en bonne santé en Europe, 2012-2020.

(54) https://solidarites-sante.gouv.fr/IMG/pdf/200116-cp_vieillir_en_bonne_sante.pdf.

(55) CNS-IFOP, *Les Français et les objets connectés*. Ifop pour la Dicom du ministère des Solidarités et de la Santé, juill. 2017. – M.-J. Moquet, *Inégalités sociales de santé : des déterminants multiples*, La Santé de l'Homme, INPES, sept.-oct. 2008, p. 17-19.

(56) GT28, *Créer les conditions d'un développement vertueux des objets connectés et des applications mobiles en santé*, 16 janv. 2017. – CNS, *Faire en sorte que les applications et objets connectés en santé bénéficient à tous*, avis adopté en assemblée plénière, 8 févr. 2018.

comme des consommateurs de soins, voire des hyper ou superconsommateurs de soins et de produits de consommation courante.

Trois situations radicalement différentes doivent être distinguées afin de parvenir à la qualification et à la classification du produit au regard notamment de la réglementation sur les dispositifs médicaux (Règl. [UE] n° 2017/745), sachant qu'il y a une porosité entre les catégories, générée ou accentuée par le comportement du patient-consommateur.

• La situation dans laquelle le « patient-consommateur » utilise un objet connecté dans le cadre du suivi médical et d'un protocole de soins remboursé ou non. Dans ce cas, la relation est entièrement placée dans le périmètre du droit de la santé, avec le risque d'une utilisation excessive ou d'un usage détourné. Le produit a clairement une revendication médicale et dispose d'un marquage CE conformément à l'article L. 5211-1 du Code de la santé publique définissant les dispositifs médicaux dont font partie les logiciels en application de la directive 93/42/CEE, et désormais du nouveau règlement « DM », sachant que la définition de dispositif médical évolue avec ce nouveau règlement (UE) n° 2017/745.

Dans ce contexte médical, pour les objets connectés utilisés qui répondent à une stricte finalité au sens « santé médicale », c'est-à-dire de diagnostic, de prévention, de contrôle, de traitement ou d'atténuation d'une pathologie, leurs fabricants doivent répondre à la réglementation des « dispositifs médicaux » (DM), évalués pour ce faire selon quatre niveaux de risque (I, IIA, IIB, III) et soumis aux exigences de la réglementation européenne (Dir. 90/385/CEE et 93/42/CEE et Règl. [UE] n° 2017/745) qui valident ces dispositifs médicaux et imposent un marquage CE. Cette démarche présente l'avantage de la protection et de la transparence entre les acteurs. Au sens de l'article L. 5211-1 du Code de la santé publique, constitue également un dispositif médical (DM) le logiciel destiné par le fabricant de l'objet à être utilisé à des fins diagnostiques ou thérapeutiques. En conséquence, les fabricants de DM doivent respecter une série d'obligations, notamment : le marquage CE au sens de la réglementation précitée, la déclaration auprès de l'Agence nationale de sécurité du médicament et des produits de santé (ANSM), les obligations de matériovigilance (remontée à l'ANSM des effets indésirables graves). Ces produits font l'objet d'une surveillance de la part de la DGCCRF et de l'ANSM, renforcée avec l'arrivée du nouveau règlement « DM ».

• La situation dans laquelle le patient a recours à des produits connectés de bien-être pour prévenir ou contrôler ses besoins de santé réels ou supposés, en dehors de son parcours de soins et hors de tout contrôle médical, dans le cadre de sa propre pratique d'automédication. Le produit, soumis au droit commun, est alors détourné de sa fonction initiale de bien-être et exploité dans un objectif autre de transmission d'une information de santé. Or, la conception même de son logiciel, bien qu'utilisant des données de santé, ne devrait pas conduire à une capacité de diagnostic et de prescription de comportements médicaux à adopter pour le patient. La situation est celle d'une extension d'utilisation du produit, d'un mésusage ou détournement de l'usage normal du produit avec pour conséquence d'engager en principe la seule responsabilité de son utilisateur, c'est-à-dire le « patient-consommateur ». Mais la situation n'est pas aussi simple, et la question se posera de la responsabilité du concepteur de l'objet connecté.

• La situation dans laquelle le « patient-consommateur » utilise un objet connecté à usage courant, afin de lui fournir dans un but récréatif des données sur le bon maintien de son état de santé (chronomètre de course, compteur de pas, *coach* sportif connecté). Cet objet, qui ne présente pas d'enjeu ni de revendication de santé, entre clairement dans le périmètre du droit de la consommation. Ces objets connectés répondent à une finalité de type « santé bien-être » ; ce sont alors des dispositifs non médicaux (non DM), c'est-à-dire des produits ou services de consommation courante, soumis en France, notamment, aux règles du Code de la consommation. Les objets connectés en santé « non DM » ne peuvent en aucun cas se prévaloir du statut de DM ni du marquage CE propre à ces produits. Mais ils sont soumis à la réglementation générale des produits et aux réglementations spécifiques (RED, RoHS[57]...) en rapport avec leur fonctionnement : notamment les règles du Code de la consommation, comme pour tous les biens de consommation loyaux et marchands. À cet égard, le traitement des problèmes de fabrication ou de distribution éventuels de ces objets connectés « non DM » est de la responsabilité du fabricant et/ou du metteur en marché (cas d'atteinte à la sécurité, la santé ou la vie privée des personnes qui les utilisent). Leur surveillance relève de la compétence de la DGCCRF. Mais il est évident que le contrôle de la sécurité de ces produits *a priori* avant leur mise sur le marché est impossible en France. C'est pourquoi le positionnement sur le terrain des DM peut offrir un avantage concurrentiel fort en présentant le produit sécurisé au « patient-consommateur ».

Il convient en effet de rappeler et d'affirmer clairement que les objets connectés ne pourront devenir des dispositifs médicaux que si le fabricant le revendique, sauf à procéder à une requalification en démontrant la pratique frauduleuse du concepteur visant à se positionner sur un marché plus favorable au plan réglementaire, sans remplir les critères de qualification.

Dans la pratique, cette distinction théorique n'est pas aussi claire ni aisée à caractériser.

La difficulté survient lorsque ce « patient-consommateur » de solutions de santé transmet des données de santé, au-delà de ses seules données personnelles, dans un usage de l'objet connecté intelligent, qui serait normal pour un consommateur lambda, mais qui devient problématique lorsqu'il s'immisce dans le secteur de la santé, ce qui a été remarqué par le Conseil national de la consommation[58].

En conséquence, peu importe que l'utilisateur soit une personne entrant dans la catégorie des patients ou professionnels de santé pour que ce produit soit reconnu comme un produit de santé ; encore faut-il qu'il présente les critères de qualification d'un dispositif médical, ayant une revendication santé, ce qui pourra lui permettre d'obtenir un marquage CE et éventuellement un remboursement par l'assurance maladie. Mais rares sont les produits parmi la multitude d'objets connectés qui pourront prétendre à ce statut.

(57) PE et Cons. UE, dir. 2011/65/UE, 8 juin 2011, relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques (Texte présentant de l'intérêt pour l'EEE).
(58) CNC, Rapport sur les objets connectés en santé, 7 juill. 2017.

L'enjeu du marquage CE et de la qualification de l'objet connecté comme dispositif médical est fondamental en ce qu'il offre une garantie de sécurité à l'utilisateur, mais suppose une mise en conformité et des procédures qui peuvent être jugées contraignantes et onéreuses dans le secteur mouvant du numérique. Il va sans dire que la question de la qualification et de la classification ne se pose véritablement que pour les objets connectés de santé frontière ou *borderline*. Pour ces produits, qui sont à la frontière mais qui néanmoins collectent des données de santé et ont un impact fort dans la vie du « patient-consommateur », par l'information de santé qu'ils transmettent, la HAS a émis des recommandations à l'attention des concepteurs notamment d'application de santé. Les objets connectés en santé sont définis par la HAS comme « des dispositifs connectés à l'Internet pouvant collecter, stocker, traiter et diffuser des données ou pouvant accomplir des actions spécifiques en fonction des informations reçues »(59). Le marché est considérable. Près de 100 000 applications santé sont actuellement disponibles et de nouvelles apparaissent chaque jour. Certaines proposent des conseils individualisés, recueillent des données personnelles (poids, tension, fréquence cardiaque…), ou délivrent des informations médicales. Leur développement se fait sans cadre prédéfini, ce qui soulève de nombreuses questions sur leur fiabilité médicale, la réutilisation des données collectées ou le respect de la confidentialité. Un référentiel de bonnes pratiques, élaboré par la HAS, vise à améliorer la fiabilité et la sécurité de ces applications et objets connectés afin que les utilisateurs, particuliers comme professionnels, puissent les utiliser en toute confiance. Ce référentiel porte sur les outils connectés sans finalité médicale déclarée. Il s'agit essentiellement des applications liées à la prévention, au bien-être. Les dispositifs médicaux sont exclus du périmètre de ce référentiel. De son côté, le Conseil national de la consommation (CNC), dans un avis du 8 février 2018, privilégie l'accessibilité pour tous des objets de santé connectés et recommande l'élaboration d'un référentiel socle de qualité, avec un processus de certification volontaire afin d'encadrer les risques(60). Toutefois le CCNE pointe le risque de rupture d'égalité d'accès aux soins entre les patients connectés et non connectés, risque qui pourrait s'aggraver sous l'influence de deux facteurs : d'une part, le vieillissement de la population face à une jeunesse ultraconnectée et, d'autre part, la désertification des régions face aux villes connectées.

Si théoriquement la qualification du produit est revendiquée par le fabricant et ne saurait varier en fonction de l'usage qu'en retire le patient, la question peut toutefois se poser de la responsabilité du fabricant ou concepteur qui n'aurait pas envisagé, limité et encadré le détournement de son produit connecté et notamment doté d'une intelligence artificielle. Se pose avec une acuité particulière la question de l'algorithme intelligent auto-apprenant, et la protection des droits de la personne algorithmée. En la matière, il apparaît clairement au plan juridique une complexité dans la mise en œuvre de la norme selon la classification du produit et les interactions entre la norme visant à la protection des données (RGPD) et la réglementation sur les dispositifs médicaux (règlement « DM »).

(59) HAS, Référentiel de bonnes pratiques sur les applications et les objets connectés en santé, oct. 2016.
(60) CNC, *Faire en sorte que les applications et objets connectés en santé bénéficient à tous*, avis, 8 févr. 2018.

Plus largement, cette confusion des genres entre les produits qui surfent sur la vague du bien-être et de la prévention en santé invite le juriste à s'interroger sur les sujets relatifs à la qualification du produit au regard du droit des biens, à la sécurité sous l'angle du droit de la responsabilité, à la capacité à contracter au regard du droit des contrats, ou encore à la protection du patient-consommateur au regard du droit de la consommation, et enfin sur la question des pratiques au regard du droit de la concurrence. C'est pourquoi, dans cet imbroglio, la qualification de DM connecté peut paraître plus efficace et protectrice tant pour le fabricant concepteur que pour l'utilisateur et patient-consommateur, voire donner des avantages concurrentiels.

La mouvance de ce secteur a laissé surgir un torrent de *soft law* au travers d'avis, recommandations, chartes, guides de bonnes pratiques, référentiels visant à favoriser l'analyse et l'encadrement des produits, et émanant des différentes autorités impliquées dans l'évaluation du produit (CNIL, HAS, ARS notamment). Cette prolifération de sources juridiques de droit dur et souple dont l'objectif est de poser un cadrage, souple, flexible, et en mouvement, adapté à la vitesse de prolifération des produits, traduit toute la complexité de saisir par le droit la situation de ces produits innovants connectés.

SECTION 2

## L'UTILISATION PAR LE « PATIENT-CONSOMMATEUR » D'UN DM CONNECTÉ

Les objets connectés dans le secteur des DM visent une catégorie très large de produits. La première difficulté réside donc dans la qualification juridique du dispositif connecté, de laquelle va découler l'ensemble du *corpus* juridique et réglementaire applicable. Cette qualification va conditionner la protection de l'utilisateur final « patient-consommateur ».

La deuxième difficulté réside dans la question de savoir comment s'articulent les dispositions spécifiques relevant du droit de la santé et celles plus générales relevant notamment du droit de la consommation ou droit du numérique, avec pour conséquence l'analyse du consentement, libre et éclairé, ainsi que celle de la protection, de l'exploitation et de la valorisation des données dont il convient de définir si ce sont des données non personnelles, personnelles, données de santé, données mixtes.

Enfin la question se pose de la responsabilité du fournisseur, du distributeur, de l'objet connecté lui-même (robot) dès lors qu'il est pourvu d'une intelligence artificielle, qui permet de prendre la décision de santé ou médicale. Le recours à l'objet connecté dans le secteur de la santé modifie donc la cartographie des responsabilités entre les acteurs, sans qu'il y ait encore un consensus fort sur la responsabilité de cet objet.

## § 1. – Le DM connecté et l'enjeu de sa qualification pour le « patient-consommateur » de soins

L'hypothèse est celle d'un « patient-consommateur » dont la pathologie est prévenue ou suivie grâce à un objet connecté, qui peut être doté d'une intelligence artificielle. La qualification d'objet connecté, intelligent, comme dispositif médical a pour conséquence une protection renforcée du patient.

La diversité de ces objets connectés et applications pouvant avoir le statut de dispositif médical impose de les classer en plusieurs catégories selon le type de revendication. Il peut s'agir d'objets ayant préalablement intrinsèquement le statut de DM, auxquels vient s'ajouter un logiciel doté d'un algorithme permettant d'assister le patient. Ce peut être le cas d'une canne connectée, d'une prothèse connectée. Il peut aussi s'agir d'un objet connecté implantable qui va remplacer ou assister la fonction d'un organe et qui suppose une intervention chirurgicale. Enfin, il peut s'agir d'une application qui remplit la fonction d'une aide à la décision d'automédication, ou de suivi de traitement, de prévention. La fonction logicielle est alors incorporée dans un produit qui dispose ou non en lui-même du statut de DM. Il est important de distinguer la relation de la fonction principale et accessoire que joue le logiciel avec celle de l'objet physique.

Le statut de DM et la classification du produit vont dépendre de sa dangerosité et donc du risque qu'il représente pour le « patient-consommateur », et les utilisateurs du produit.

**Pour rappel**, la définition du dispositif médical, telle que prévue par le Code de la santé publique, dans son article L. 5211-1[(61)], incorpore le logiciel et concerne certains objets connectés dès lors qu'ils remplissent les critères :

« Tout instrument, appareil, équipement, logiciel, matière ou autre article, utilisé seul ou en association, y compris le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostique et/ou thérapeutique, et nécessaire au bon fonctionnement de celui-ci.

Le dispositif médical est destiné par le fabricant à être utilisé chez l'homme à des fins de :

– diagnostic, prévention, contrôle, traitement ou d'atténuation d'une maladie ;

– diagnostic, contrôle, traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap ;

– d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique ;

– maîtrise de la conception ;

et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens ».

Pour entrer ou rester dans cette catégorie de DM ou DMDIV, l'objet connecté doit être conforme au règlement « DM »[(62)].

(61) Article 1, 2° de la directive 93/42/CEE transposée par le Code de la santé publique à l'article L. 5211-1 dudit code ; application du règlement « DM » à compter du 20 mai 2020. C. santé publ., art. L. 5211-1 et R. 5211-1.

(62) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux et PE et Cons. UE, règl. (UE) n° 2017/746, 5 avr. 2017, relatif aux dispositifs médicaux de diagnostic *in vitro*. Le premier règlement abroge et remplace les directives 90/385/CEE et 93/42/CE à compter du 26 mai 2020, tandis que le second abroge et remplace la directive 98/79/CE à compter du 26 mai 2022.

Les critères de qualification des applications mobiles et des objets connectés sont complexes. Ils doivent répondre à plusieurs critères :

– fournir une information médicale nouvelle contribuant par exemple au diagnostic ou au traitement du patient ;

– donner un résultat propre à un patient sur la base de données individuelles ;

– effectuer une action sur les données entrantes, telle qu'une analyse afin de fournir une information médicale nouvelle.

L'ANSM(63) donne une ligne d'interprétation de ces critères et précise qu'une application d'analyses de données de signaux physiologiques propres à un patient et dotée de fonctions d'alerte à finalité médicale sera qualifiée de DM. Une distinction est à faire selon la dangerosité et la fonction du DM ou du DMDIV qui est essentiellement utilisé dans le secteur des laboratoires de biologie médicale par les professionnels de santé. Selon la nouvelle classification, les DMDIV sont répartis en classe A, classe B, classe C et classe D en fonction de la destination des dispositifs et des risques qui leur sont inhérents. Pour les trois dernières classes, l'intervention d'un organisme notifié est obligatoire.

Un DMDIV connecté entre aussi dans cette catégorie. Un DMDIV connecté est un produit ou instrument connecté destiné par son fabricant à être utilisé *in vitro* dans l'examen d'échantillons provenant du corps humain. Leur but étant de fournir une information, notamment, sur l'état physiologique ou pathologique d'une personne ou sur une anomalie congénitale. Les produits dénommés « réactifs » appartiennent notamment à cette catégorie. Ainsi revêt la qualification de logiciel permettant d'évaluer le niveau de fibrose hépatique d'un patient, un logiciel de prédiction du risque de mélanome, logiciel type « calculette/réglette électronique » destiné à calculer le débit de perfusion d'un médicament.

La relation du « patient-consommateur » au produit connecté concerne donc essentiellement les DM simples et outils d'aide à la décision. La clarification portant sur la qualification d'un logiciel d'aide à la prescription médicale qui ne se borne pas au stockage de données, mais qui les utilise, les exploite, et les interprète, est apportée par la Cour de justice de l'Union européenne(64) qui conclut : « Un logiciel dont l'une des fonctionnalités permet l'exploitation de données propres à un patient, aux fins notamment de détecter les contre-indications, les interactions médicamenteuses et les posologies excessives, constitue, pour ce qui est de cette fonctionnalité, un dispositif médical, au sens de l'article 1er, paragraphe 2, sous a), de la directive 93/42, et ce **même si un tel logiciel n'agit pas directement dans ou sur le corps humain** ».

La Cour de justice indique donc clairement que la finalité médicale s'apprécie au regard de la définition du DM, et que la notion de modules dans un logiciel peut être retenue. Elle précise que chacun d'entre eux doit être individuellement qualifié, au regard de sa finalité ; à cet égard, seuls les modules/fonctionnalités ayant une finalité médicale sont qualifiés de DM et devront à ce titre être marqués CE.

(63) ANSM, *Mise sur le marché des dispositifs médicaux et des dispositifs médicaux de diagnostic* in vitro, 2020 (www.ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Logiciels-et-applications-mobiles-en-sante/(offset)/2).

(64) CJUE, 7 déc. 2017, aff. C-329/16, *SNITEM* c/ *Min. Affaires sociales et Santé*.

Ces précisions apportées par la Cour et par le règlement permettent d'avoir une approche plus précise, mais la complexité et l'intrication de différentes fonctions des objets connectés nécessitent une analyse au cas par cas très précise et détaillée des fonctionnalités de l'objet.

Une fois qualifiés de DM, ces logiciels d'aide à la prescription (LAP) et à la décision doivent être classifiés en classe I, IIa, IIb ou III, en fonction des risques inhérents à leur utilisation(65). En tant que DM, les logiciels doivent donc désormais respecter les obligations qui s'imposent à ce type de produits, telles que répondre aux exigences essentielles applicables et être dotés du marquage CE, qui atteste de leur conformité à ces exigences.

Dans le cadre de la directive, ces logiciels relèvent de la classe I, et donc une procédure d'auto-certification visée à l'annexe VII de la directive s'applique. En fonction de la classe, le fabricant doit suivre une ou des procédures définies par la réglementation, permettant de démontrer la conformité de ses produits aux exigences essentielles. Mais, en application du règlement « DM »(66), ils relèveront des trois autres classes en fonction du risque potentiel lié à leur utilisation, soit de la classe IIa, IIb ou III. La modification de la classification du DM est donc à anticiper pour les fabricants, avec toutes les conséquences en termes d'organisation de la gestion des risques sur le produit. En tant que DM, les logiciels doivent donc désormais respecter les obligations qui s'imposent à ce type de produits, telles que répondre aux exigences essentielles applicables et être dotés du marquage CE, qui atteste de leur conformité à ces exigences(67).

De nombreuses *startups* qui s'étaient lancées sur ce secteur en visant la qualification « DM de classe I » avec une autocertification doivent donc, pour pouvoir percer le marché, se mettre en conformité avec le règlement « DM », visant au renforcement de la protection des droits des patients et utilisateurs. L'objectif de protection de la sécurité des patients utilisateurs est renforcé dans cette nouvelle classification, ce qui peut pousser les créateurs de logiciels et applications à rechercher un marquage CE, afin de renforcer l'image de sécurité du produit sur le marché confus des objets connectés. L'enjeu de la qualification est donc déterminant dans la vie du produit sur son marché, de son remboursement éventuel par l'assurance maladie, et donc de son accessibilité par le patient dans le cadre de sa politique de soins.

Pour qu'un appareil connecté soit pris en charge par l'assurance maladie, il faut qu'il soit prescrit par un médecin bien sûr, et qu'il soit inscrit sur la liste des produits et prestations remboursables (LPPR) au titre de dispositif médical à usage individuel. Le Code de la santé publique définit le dispositif médical comme « tout instrument, appareil, produit (…) destiné à être utilisé chez l'homme à des fins médicales et dont l'action principale n'est pas obtenue par des moyens pharmacologiques » (C. santé publ., art. L. 5211-1). Seuls certains objets connectés médicaux et

(65) En application des règles de classification établies par la dir. 93/42/CEE, les LAP relèvent de la classe I (règle 12 de l'annexe IX : « Tous les autres dispositifs actifs font partie de la classe I »).

(66) PE et Cons. UE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, actuellement en vigueur et dont l'application sera obligatoire le 26 mai 2020.

(67) C. santé publ., art. R. 5211-12 tel qu'issu de la transposition de la directive 93/42/CEE.

marqués CE (attestant de leur conformité à la réglementation) sont pris en charge par la Sécurité sociale[68]. Mais leur nombre va nécessairement augmenter avec le développement exponentiel de ce secteur, dans un contexte de vieillissement de la population dont les besoins s'accroissent[69]. Cette croissance est aussi dynamisée par la politique de santé publique, notamment avec le fameux article 51 de la loi de financement de la sécurité sociale, portant sur les dérogations en faveur des projets innovants et notamment basés sur le déploiement du numérique et des objets connectés. Le ministère des Solidarités et de la Santé s'est également doté en 2018 d'un dispositif permettant d'expérimenter des organisations innovantes reposant sur de nouveaux modes de financement grâce à l'article 51 de la loi de financement de la sécurité sociale pour 2018 (dispositif reconduit en 2019)[70]. Cet article permet de déroger à certaines dispositions du droit commun afin d'améliorer la prise en charge et le parcours des patients, l'efficience du système de santé et l'accès aux soins. L'utilisation de dispositifs numériques de coordination des professionnels de santé agissant dans la prise en charge ou d'outils de télésuivi permettant d'assurer la continuité des soins, après une hospitalisation, entre dans le cadre de ces expérimentations dérogatoires[71].

Afin d'éclaircir le paysage et de faciliter la qualification pour le fabricant et le parcours de la demande de remboursement du produit, une note de cadrage a été transmise par le ministère des Solidarités et de la Santé, car s'il convient de doper l'innovation dans le secteur du numérique en santé, il ne s'agit pas d'assurer la prise en charge et le remboursement de tous les produits et objets connectés, ce qui exige donc de mettre en place des critères d'évaluation des projets[72] déposés dans le cadre du dispositif expérimental et dérogatoire porté par l'article L. 162-31-1 du Code de la sécurité sociale. Un guide méthodologique a été élaboré par l'assurance maladie en 2019[73]. L'ANSM a donné une liste d'exemples de qualification à partir de cas soumis[74], dont la lecture permet de tirer une ligne directrice. La HAS[75] a élaboré des documents permettant de poser les critères d'évaluation qui sont retenus par la CNEDiMTS afin de permettre un accès rapide des produits les plus innovants et utiles pour le patient.

(68) Lecteurs de glycémie, d'électrodes, de bandelettes et de capteurs, de stylos injecteurs, d'appareils de mesure de la coagulation, d'appareillages de ventilation à pression positive continue (PPC) et de débitmètres de pointe.

(69) M. Dubreuil, *E-santé : décryptage des pratiques et des enjeux*, Observatoire régional de santé Île-de-France, 2019.

(70) Le décret du 21 février 2018 précise les modalités de mise en œuvre expérimentale du dispositif, dont les grandes orientations sont définies par le Conseil stratégique de l'innovation en santé, D. n° 2018-125, 21 févr. 2018, relatif au cadre d'expérimentations pour l'innovation dans le système de santé prévu à l'article L. 162-31-1 du Code de la sécurité sociale. La circulaire n° SG/2018/106 du 13 avril 2018, relative au cadre d'expérimentation pour les innovations organisationnelles prévu par l'article 51 de la LFSS pour 2018 précise les modalités de mise en œuvre du dispositif de l'article 51 par les agences régionales de santé.

(71) 8 % des lettres d'intention reçues en 2018 concernaient le numérique (art. 51, Innovation en santé, 2018).

(72) Note sur le cadre d'évaluation des expérimentations dans le cadre du dispositif d'innovation en santé (LFSS 2018, art. 51).

(73) *Guide méthodologique de l'évaluation des projets*, LFSS 2018, art. 51 : Accompagnement pour la mise en œuvre de l'évaluation de projets dans le cadre de l'innovation en santé.

(74) ANSM, *Mise sur le marché des dispositifs médicaux et des dispositifs médicaux de diagnostic in vitro*, 2020 (www.ansm.sante.fr/Activites/Mise-sur-le-marche-des-dispositifs-medicaux-et-dispositifs-medicaux-de-diagnostic-in-vitro-DM-DMIA-DMDIV/Logiciels-et-applications-mobiles-en-sante).

(75) HAS, *Évaluer les dispositifs médicaux connectés, y compris ceux faisant appel à l'intelligence artificielle*, févr. 2019. Rapport méthodologique d'évaluation clinique d'un dispositif médical connecté. *Guide sur les spécificités d'évaluation clinique d'un DMC en vue de son accès au remboursement*.

Elle a publié un guide[76] concernant les procédures à anticiper par le fabricant ou l'exploitant afin d'obtenir l'évaluation par la CNEDiMTS.

La situation est plus complexe pour les objets connectés ou applications mobiles qui se trouvent à la frontière et disposent de plusieurs fonctionnalités. La question à se poser au cas par cas est celle de savoir si la qualification principale s'applique aux accessoires, et ce qu'il faut entendre par accessoire de la fonction principale, en application de la décision de la Cour de justice de l'Union européenne.

Si la procédure de marquage CE permet d'assurer une protection du patient, l'application de ces réglementations spécifiques dans le secteur de la santé doit être confrontée à l'application des dispositions de droit commun en matière de consommation concernant les droits du « patient-consommateur », et disposition relevant du règlement général sur la protection des données dès lors qu'il s'agit d'un « produit connecté frontière ».

**L'utilisation détournée d'un « DM connecté frontière » utilisé par le « patient-consommateur ».**

L'hypothèse de départ est celle d'un objet connecté utilisé dans le contexte de la santé, mais qui n'a pas de revendication médicale par le fabricant, et n'est donc pas un DM au sens du règlement[77].

Sont visés les objets connectés grand public, de bien-être, objets connectés intelligents à usage courant, destinés à être utilisés par un consommateur lambda, mais qui dans l'hypothèse sont utilisés ou détournés de leur usage par un « patient-consommateur » dans un objectif de contrôle de sa santé. Il peut s'agir aussi de la multitude de produits utiles pour suivre l'état de santé du patient, mais qui n'ont pas d'allégation thérapeutique.

Sur le principe, ces objets connectés frontières sont soumis au droit commun et au contrôle de leur statut par la DGCCRF. Celle-ci vérifie notamment les infractions à la loi pour la confiance dans l'économie numérique[78], à la réglementation sur la vente à distance[79] et à la réglementation sur la langue française[80], aux pratiques commerciales trompeuses[81]. Leur requalification ne peut être encourue que s'ils présentent une revendication médicale et des allégations thérapeutiques. La tromperie dans la qualification du produit, positionné sur le périmètre des produits de bien-être alors qu'il se présente dans la réalité comme un dispositif médical créant une confusion dans l'esprit du public, peut entraîner une sanction lourde et l'interdiction de continuer l'exploitation du produit.

(76) HAS, *Guide sur les spécificités d'évaluation clinique d'un dispositif médical connecté (DMC) en vue de son accès au remboursement*, 1er janv. 2019

(77) CNC, Avis sur les objets connectés en santé, 7 juill. 2017.

(78) L. n° 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique, dite « LCEN ».

(79) L. n° 2017-203, 21 févr. 2017, ratifiant les ordonnances n° 2016-301 du 14 mars 2016 relative à la partie législative du Code de la consommation et L. n° 2016-351, 25 mars 2016 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage d'habitation et simplifiant le dispositif de mise en œuvre des obligations en matière de conformité et de sécurité des produits et services.

(80) L. n° 94-665, 4 août 1994, relative à l'emploi de la langue française, plus connue sous le nom de « loi Toubon ».

(81) C. consom., art. L. 121-1 ; la directive UE n° 2005-29 du 11 mai 2005, relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs en donne la définition suivante : « toute action, omission, conduite, démarche ou communication commerciale, y compris la publicité et le marketing, de la part d'un professionnel, en relation directe avec la promotion, la vente ou la fourniture d'un produit au consommateur ».

Toutefois, dans la situation où l'objet connecté est systématiquement détourné de son usage par le « patient-consommateur », qui l'utilise à visée médicale, toute la question est de savoir si la qualification du produit provient encore de la fonction assignée par le fournisseur, ou de celle du statut de l'utilisateur qui pourrait influer sur la fonction assignée et l'étendre ou la détourner. Sur le principe, une telle requalification ne devrait pas être envisageable, dès lors que le fabricant a clairement communiqué sur la fonction bien-être de l'objet connecté, et exclu clairement toute autre utilisation. En conséquence, l'extension ou le détournement des fonctions de l'objet connecté par le « patient-consommateur » ne devrait pas conduire à une modification du statut du produit, dès lors que l'information donnée par le fournisseur est explicite sur les fonctions du produit. La qualité de l'information est alors cruciale dans un secteur complexe et souvent confus pour l'utilisateur. Seul le « patient-consommateur » clairement informé peut être tenu responsable des conséquences du mésusage.

Les risques liés à l'utilisation détournée du produit par le « patient-consommateur » sont importants et portent sur la nature et le traitement des données de santé collectées, et sur la sécurité du produit notamment dans l'information donnée et le service rendu au consommateur.

La question est encore plus complexe dans l'hypothèse d'un produit connecté doté d'une intelligence artificielle, dont la décision autonome pourra produire des effets négatifs sur la santé du patient. Dans ce cas, la question se posera de savoir quel encadrement de la responsabilité de l'utilisateur du produit peut être mobilisé.

L'analyse de la responsabilité du fabricant et du concepteur donne lieu à de nombreuses études sur la mobilisation du régime de responsabilité avec ou sans faute, responsabilité du fait des produits défectueux, responsabilité de l'IA qui aurait une personnalité autonome. Mais l'on peut s'interroger aussi sur la délimitation du périmètre de responsabilité de l'utilisateur « patient-consommateur », notamment dans la prévision du risque par les assurances.

La situation est tout autre si le produit, qui présente une revendication médicale, a volontairement été placé par le fournisseur dans la catégorie « bien-être » afin de faciliter la pénétration du marché, tout en évitant la procédure d'obtention d'un marquage CE. Dans cette situation, le risque de tromperie du consommateur est patent[(82)].

L'encadrement de la protection du « patient-consommateur » dans l'utilisation d'un objet connecté à visée de santé est conditionné par le statut attribué au produit[(83)].

(82) DGCCRF, *Objets connectés santé et bien-être : sont-ils fiables ?*, 2018.
(83) CNC, Rapport et avis sur les objets connectés en santé, 7 juill. 2017.

## § 2. – Le renforcement de la protection des droits du « patient-consommateur » utilisateur de DM connecté

La protection du patient dans le règlement « DM » vise essentiellement à assurer la sécurité du produit contre les défaillances qui pourraient nuire au patient, et à assurer la protection des données du patient, qui sont des données de santé.

### I. – La protection des données

La complexité des produits exige de procéder dans chaque situation à une confrontation des règles applicables au titre du règlement « DM » et du RGPD, et d'analyser les notions de données de santé, données personnelles, essais et évaluations, intérêt de santé publique.

Le règlement général sur la protection des données (RGPD), d'étendue européenne, et la loi française sur la protection des données personnelles, promulguée en juin 2018, adaptant la loi Informatique et Libertés, constituent désormais le socle de la nouvelle réglementation sur la protection de toutes les données personnelles et celles qui concernent la santé notamment. Le RGPD définit les données personnelles comme « toute information se rapportant à une personne physique identifiée ou identifiable »(84). La CNIL a édicté un guide permettant l'analyse des conditions de collecte des données dans le secteur de la santé et des conditions d'information du patient(85). Le RGPD confirme le principe antérieur de l'interdiction du traitement de données « sensibles » concernant la santé. Par exception, les textes autorisent le traitement de telles données lorsque la personne concernée, « le patient », a donné son consentement explicite (RGPD, art. 9.1). Pour le DM, le traitement des données de santé est dispensé de formalités auprès de la CNIL dans la mesure où le patient a donné son consentement, ce qui ne sera pas le cas si le produit n'a pas le statut de DM.

Dans tous les cas, le patient, utilisateur de l'objet connecté, doit donner son consentement au professionnel de santé et à l'intermédiaire qui fournit la plateforme pour la collecte et le traitement des données. Il peut à tout moment retirer son consentement et a le droit de s'opposer à l'utilisation par un organisme de télémédecine ou de santé connectée de ses données de santé à caractère personnel.

Il peut en effet craindre à tout moment le risque de valorisation des données auprès des assureurs sans son consentement, et les conséquences néfastes qui pourraient en résulter.

La protection et la valorisation des données du patient sont des sujets brûlants et portent sur la possibilité pour les différents intermédiaires de valoriser les données récoltées, mais aussi pour le patient de monétiser les données de santé qu'il transmet.

(84) Le décret n° 2018-687 du 1er août 2018 est entré en application le 4 août 2018. Ce décret vient compléter la loi « Informatique et Libertés » de janvier 1978, qui avait elle-même été modifiée par la loi n° 2018-493 du 20 juin 2018. Le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est venu apporter la touche finale à l'alignement du droit français par rapport au règlement général sur la protection des données à caractère personnel n° 2016/679/UE, ou « RGPD » en abrégé.

(85) CNIL, *Traitement de données de santé : comment informer les personnes concernées ?*, 2018.

## II. – La sécurité de l'objet connecté et la protection du patient-consommateur

Tous les produits connectés DM ou produit connecté frontière peuvent présenter une faille de sécurité[86]. Les exemples de cybercriminalité se multiplient au niveau international, avec un risque de santé publique majeur. La situation est d'autant plus grave lorsqu'il s'agit d'un DM connecté implantable. Les risques de cyberattaques concernent principalement l'échange de données, le pilotage du dispositif, le suivi du patient à distance ou la maintenance des produits.

Face à ce risque, il est indispensable de préciser quel est l'encadrement juridique qui permet de protéger la sécurité des DM connectés. Ces appareils sont soumis à un corps de règles qui nécessite pour l'entreprise la mise en œuvre de textes complexes et enchevêtrés. La question pour le fabricant de DM est de mettre en œuvre le dispositif le plus sécurisant pour éviter toute attaque malveillante.

Le DM connecté est en effet soumis à la fois au règlement « DM » et au RGPD. Ces textes visent à assurer la confidentialité, l'intégrité et la disponibilité des informations contenues ou issues d'un DM connecté ou d'un logiciel. Ils visent à assurer la protection contre les attaques intentionnelles et malveillantes. Mais il conviendrait d'ajouter à ces textes la notion de manipulation non intentionnelle, de mésusage ou d'erreur d'utilisation, *a fortiori* lorsque ces DM sont utilisés ou « mis à disposition » de personnes fragiles, de personnes âgées, dépendantes, malades, ou encore présentant des altérations de leurs facultés de discernement.

Le règlement « DM » ne règle pas toutes les questions : il ne couvre pas toutes les problématiques transversales, et les fabricants ne disposent que d'un guide de référence sans valeur contraignante qui ne saurait les dédouaner de leur responsabilité.

Au plan national, une sanction pénale pourra être prononcée notamment pour tentative d'escroquerie (C. pén., art. 313-3), et atteinte à la vie privée (C. pén., art. 226-1), voire mise en danger de la vie d'autrui (C. pén., art. 223-1). Mais encore faut-il pouvoir identifier l'auteur de l'infraction.

Les risques peuvent aussi provenir de la fiabilité du produit. Les produits peuvent être utilisés au-delà de leur revendication, caractérisant un mésusage par le patient ; le produit peut présenter une défaillance en transmettant des informations fausses ; ou encore et surtout, le produit connecté intelligent peut donner un résultat d'analyse effectué par son algorithme inadapté à la situation de santé du patient.

Enfin, le risque peut provenir des modalités de vente ; la vente à distance engendre un risque pour le patient-consommateur de contrefaçon, falsification du produit.

Le Code de la consommation a prévu (art. L. 221-1 et s.) des dispositions particulières pour la vente à distance de dispositifs médicaux, faisant une distinction entre la vente par les professionnels de santé et les autres. Concernant les professionnels de santé, le régime juridique des contrats conclus à distance ne s'applique pas, ils n'ont pas à proposer le droit de rétractation légal de quatorze jours.

(86) FDA, Alerte sur la sécurité de certains défibrillateurs connectés de Medtronic, 26 mars 2019 (www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home).

Le niveau de protection du « patient-consommateur » varie donc considérablement selon le statut du produit.

Le règlement « DM » prévoit les conditions et modalités de mise en cause de la responsabilité du fabricant et du fournisseur de logiciel ayant le statut de DM. Le règlement permet de traiter l'ensemble de ces situations au plan réglementaire, ce qui n'exclut pas l'action en responsabilité contre le fabricant sur les fondements de droit commun. Cette procédure administrative est placée sous le contrôle des autorités de santé. L'ANSM dispose d'un pouvoir de police sanitaire. Les procédures de matériovigilance qui doivent être assurées par les fabricants, fournisseurs, professionnels de santé, établissements de santé, utilisateurs, permettent de garantir le risque.

L'objet connecté de bien-être est quant à lui soumis au dispositif de contrôle assuré par la DGCCRF et repose sur l'application des règles de droit commun de la consommation, et notamment les pratiques commerciales trompeuses. La responsabilité du fabricant pourra être engagée en cas de défaillance du produit, au plan civil voire pénal.

Les diverses études et enquêtes, notamment de la DGCCRF, démontrent que l'origine du risque provient souvent du comportement imprudent ou inadapté de l'utilisateur, qu'il s'agisse d'un professionnel de santé ou du patient-consommateur lui-même.

Enfin, la responsabilité du professionnel de santé qui prescrit l'utilisation d'un objet connecté pourrait en théorie être mobilisée et conduire à une condamnation pour avoir prescrit un produit n'étant pas marqué CE en cas d'aggravation de l'état de santé du patient, ou de surveillance d'un effet indésirable lié au mésusage du produit, sans compter une éventuelle responsabilité en cas de fuite des données de santé.

Néanmoins, il convient de marquer les limites du droit à traiter un ensemble de risques provoqués par l'objet connecté intelligent, qui décide en dehors de toute intervention humaine (robot intelligent en santé). Le sujet porte sur la responsabilité d'un objet connecté. La responsabilité du gardien de la chose (C. civ., art. 1243) pourra toujours être mobilisée, mais comment démontrer cette responsabilité lorsque la décision de l'objet connecté est autonome et hors du contrôle du gardien de la chose ? Sur le fondement de la défectuosité du produit (C. civ., art. 1245), la difficulté est du même ordre. Il sera difficile d'invoquer la responsabilité du fabricant ou du fournisseur dès lors que le dommage commis provient d'un apprentissage autonome de l'objet intelligent survenu après la mise sur le marché du produit. Le « défaut » peut donc être l'effet d'un apprentissage que l'état des connaissances scientifiques au moment où l'objet a été vendu ne permettait pas d'anticiper, ce qui permet au fabricant ou fournisseur du produit connecté de s'exonérer de sa responsabilité (C. civ., art. 1245-10). Un rapport de la cour d'appel de Paris sur la responsabilité des robots intelligents[87], rendu public le 25 juin 2019, met l'accent sur ces questionnements et la nécessité de réguler au niveau européen, en pointant

(87) Groupe de travail de la CA de Paris, Rapport sur « la réforme du droit français de la responsabilité civile et les relations économiques », 25 juin 2019.

du doigt le fait que la Commission européenne ne s'interroge que dans le cadre de la directive sur la responsabilité du fait des produits défectueux[88]. Allant dans le même sens que le Sénat[89], ce rapport écarte l'idée d'une responsabilité du robot par la reconnaissance d'une personnalité morale autonome.

La protection du patient-consommateur utilisateur d'un objet connecté intelligent doté d'un algorithme qui permet d'analyser l'ensemble des données de vie et de santé du patient, au travers notamment de sa compatibilité avec d'autres objets et réseaux, semble illusoire.

La CNIL met l'accent sur plusieurs principes de fond sur lesquels s'appuyer pour assurer une protection du patient-consommateur dans une perspective de numérisation complète de la société, et ce tout particulièrement avec la plateforme santé nationale (Hub santé). Ces principes sont fondés sur l'indépendance du patient utilisateur à l'objet, la confiance, et la loyauté.

Ces principes sont les bases sur lesquelles sont assises les techniques de *blockchain* en santé, qui offrent une solution pratique à un questionnement juridique de fond sur la protection de la vie privée et de la sécurité du patient-consommateur.

Cette technique permet d'encadrer et d'assurer une amélioration de la protection du patient tant par les fabricants de dispositifs médicaux, que par les fournisseurs de produits de bien-être connectés, captant des données de santé. La *blockchain* est un système de base de données distribuée qui permet de rendre infalsifiable l'historique des transactions. Avec un système décentralisé, le livre de comptes est détenu par l'ensemble des utilisateurs, ce qui le rend impossible à falsifier, et qui permet de se passer d'un tiers en charge de la validation et de l'historique des transactions. La *blockchain* permet d'organiser une communication entre les objets connectés intelligents avec, en amont, un contrôle et l'organisation des barrières et capacités des objets à prendre les décisions[90]. Cette technique permet de sécuriser les données du patient face à la cybercriminalité. Il conviendra d'identifier dans un *smart contract* les données du patient qu'il est nécessaire de protéger et dont il faut suivre la progression. Les usages sont multiples et vont jusqu'à permettre une certaine forme de valorisation des données au bénéfice du patient avec l'arrivée de *startups* visant à redonner aux patients le contrôle sur leurs données grâce à la *blockchain*. La *blockchain* ouvre des perspectives à l'exploitation des objets connectés intelligents dans le secteur de la santé, en redonnant au patient-consommateur le pouvoir sur l'ensemble des données qu'il transfère[91] dans un encadrement juridique fondé sur une norme volontaire évolutive[92].

(88) Comm. UE, 9 avr. 2019.
(89) Rapp. Sénat n° 279, 2018-2019, *Stratégie européenne pour l'intelligence artificielle*, 31 janv. 2019, p. 30.
(90) I. Poirot-Mazères, *Santé, numérique et droit-s*, PU Toulouse 1 Capitole, 2019.
(91) O. Peyrat, *Quel est l'apport d'une norme volontaire dans le domaine du numérique ? Pourquoi les acteurs s'y intéressent-ils ? : Enjeux numériques* mars 2019, n° 5, p. 6.
(92) M. Della Chiesa, F. Hiault et C. Téqui, Blockchain *: Vers de nouvelles chaînes de valeur*, Eyrolles, 2019.

# CONCLUSION

La société, dans le secteur de la santé, est entrée dans une ère de numérisation[93] généralisée qui implique la multiplication des objets et applications connectés, dans une population très variée, allant de la prévention au traitement tout au long de la vie. La confiance, le consentement et l'information sont les sujets majeurs à traiter au plan juridique par la loi, mais aussi par la voie conventionnelle (guides, chartes, engagements). L'engouement pour la création et l'innovation numériques nécessite une adaptation juridique permanente. L'encadrement suppose une agilité juridique permettant une capacité d'adaptation au progrès et à l'innovation. C'est de la Commission européenne que les solutions sont attendues afin d'apporter une solution qui dépasse largement la question nationale.

(93) Une étude du Pôle interministériel de prospective et d'anticipation des mutations économiques (Pipame), en date du 19 juin 2019, analyse les opportunités offertes par le numérique pour moderniser les industries de santé, appelant à « faire de la numérisation un sujet stratégique » et une « priorité » dont le pilotage doit être renforcé au niveau du Comité stratégique de filière (CSF) santé.

CHAPITRE 11

# IMPACT DU NUMÉRIQUE DANS LE DOMAINE DE L'ENVIRONNEMENT

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Aleyna CAPRAZ
Élisa LEMAIRE
Anaïs PELLETIER

## INTRODUCTION

Antoine de Saint-Exupéry écrivait : « Nous n'héritons pas de la terre de nos parents, nous l'empruntons à nos enfants ». La protection du milieu naturel participe à la sauvegarde des êtres humains. Pourtant, l'importance de sa protection n'a émergé que récemment et avec elle les moyens de sa mise en œuvre et de sa protection. Le numérique, autre aspect de cette étude, a lui aussi connu ces dernières décennies un essor considérable et son impact sur les mœurs n'est plus à démontrer. Il s'agit là de deux sujets incontournables du XXIe siècle. Ils soulèvent de multiples interrogations, notamment concernant leurs risques et avantages respectifs et les moyens dont il faut et dont il est possible de se munir afin de se protéger et/ou de tirer le meilleur bénéfice possible. Il semble pertinent de définir ici les deux termes d'environnement et d'écologie, quoique cette réflexion porte aussi bien sur l'un que sur l'autre, l'un étant à l'autre ce que l'espèce est au genre, mais souvent confondus. Selon le dictionnaire Larousse, l'environnement est « l'ensemble des éléments (biotique ou abiotique) qui entourent un individu ou une espèce et dont certains contribuent directement à subvenir à ses besoins » ; en d'autres termes, l'environnement est le cadre dans lequel vit l'Homme et dans lequel il évolue. L'environnement est un système en soi, général, constitué par la planète sur laquelle vit l'être humain. L'écologie quant à elle se définit comme « la science ayant pour objet les relations des êtres vivants avec leur environnement, ainsi qu'avec les

autres êtres vivants », la « science de l'habitat » ou encore, la « science de l'environnement ». Plus récemment, avec l'émergence des considérations environnementales, l'écologie a pris le sens de l'analyse de l'impact de la vie humaine sur « son » environnement et les moyens de lutter contre ses aspects négatifs. Ainsi, l'environnement est tout ce qui entoure l'Homme et l'écologie la science qui sert à protéger cela. L'un ne pouvant finalement exister sans l'autre. Quant au numérique, il constitue un vaste ensemble d'informations présentées sous forme binaire (0 et 1), plusieurs fois présenté sous la forme d'outils informatiques dont il prend souvent la forme, mais auquel il ne se limite pas. Cet ouvrage contribue à évaluer son rôle dans le secteur de la santé. Ainsi dans ce chapitre, une première partie traitera de la conciliation de l'environnement et du numérique, au regard notamment du principe de précaution (Section 1), une deuxième partie de l'évolution de la politique territoriale et de la dynamisation des territoires par le biais du numérique (Section 2) et enfin, dans une troisième et dernière partie, sera présenté, plus concrètement, l'impact écologique du numérique (Section 3).

SECTION 1

# LE PRINCIPE DE PRÉCAUTION FACE À L'ENVIRONNEMENT ET LE NUMÉRIQUE

Le principe de précaution met notre société au défi d'agir de manière moins risquée et propice à la sauvegarde d'un environnement sain (§ 1). Ce principe juridique constitutionnel tend à s'appliquer aux révolutions en cours, la révolution environnementale certes, mais aussi la révolution numérique (§ 2).

## § 1. – Le principe de précaution : pilier du droit à un environnement sain

Dans le classement des droits, le droit à un environnement sain fait partie de la catégorie des droits nouveaux communément appelés « droits de solidarité », dont la plupart regroupent les grands défis à relever pour les générations futures. Avec la fin de l'Holocène et l'entrée dans l'Anthropocène, une ère où l'Homme est la principale force de changement de la Terre, s'est parallèlement développée l'idée d'une protection du milieu naturel (I) se retrouvant notamment dans le principe de précaution (II).

### I. – Naissance et évolution d'un droit fondamental à un environnement sain

Avec la considération nouvelle que la pérennisation du genre humain passera nécessairement par la conservation d'un cadre de vie qualitatif, sont apparus le droit à un environnement sain (A) et le principe de précaution (B).

## A. – Le droit à un environnement sain : la volonté de préserver notre système pour les générations présentes et futures

Le droit à un environnement sain est apparu lors de la Conférence tenue par les Nations unies à Stockholm, à laquelle a participé la France, en 1972. À l'occasion de cette conférence, les Nations adoptent trois séries de textes et, dès lors, placent les questions écologiques sur la scène internationale. Parmi les textes adoptés, la Déclaration de Stockholm énonce vingt-six principes dont le premier consacre le droit fondamental de l'Homme « à la liberté, à l'égalité, et à des conditions de vie satisfaisantes, dans un environnement dont la qualité lui permette de vivre dans la dignité et le bien-être »[(1)]. La Conférence aboutit également à l'adoption d'un plan d'action contenant pas moins de 109 recommandations à l'attention des gouvernements nationaux pour la mise en place de mesures d'évaluation et de gestion de l'environnement. À un niveau international plus restreint ensuite, la Cour européenne des droits de l'homme (CEDH) reconnaissait aussi le droit à un environnement sain, bien que de manière ambiguë et indirecte[(2)]. Cette difficulté de la Cour européenne à consacrer pleinement et explicitement le droit à vivre dans un environnement sain peut s'expliquer notamment par le fait qu'il a été construit d'une manière souvent qualifiée d'anthropocentrique. Suivant cette vision, l'environnement n'aurait de valeur que relativement à ce que lui attribue l'être humain : « C'est l'idée selon laquelle l'homme est la mesure de toutes choses, les composantes non humaines de la nature ne pouvant se voir reconnaître de valeur qu'en relation aux intérêts des êtres humains et aux buts qu'ils assignent ». Il s'agit de sauvegarder les systèmes naturels seulement pour ce qu'ils apportent aux Hommes, pour l'usage qu'ils en font (éthique parfois qualifiée d'utilitariste)[(3)]. Ainsi, la Cour européenne des droits de l'homme a-t-elle pu juger utile d'agir prudemment au regard des enjeux complexes du sujet. En France, c'est en 2004 – date de l'adoption de la Charte de l'environnement[(4)] que la notion de « droit à un environnement sain » est consacrée en droit positif. L'article 1er de la Charte dispose ainsi que : « Chacun a le droit de vivre dans un environnement équilibré et respectueux de la santé ».

## B. – La consécration du principe de précaution

Au niveau international c'est en 1992, à l'issue de la deuxième Conférence des Nations unies, que le principe de précaution est adopté dans la Déclaration de Rio. L'article 15 de la déclaration stipule que : « Pour protéger l'environnement, des mesures de précaution doivent être largement appliquées par les États selon leurs capacités » et fonde le principe selon lequel : « En cas de risque de dommages

(1) Rapport de la conférence des Nations unies sur l'environnement, Stockholm, 5-16 juin 1972, A/CONF.48/14/Rev.l.

(2) Plusieurs arrêts de la CEDH protègent le droit de vivre dans un environnement sain en le rattachant à des droits subjectifs, au droit à la vie privée et familiale : Conv. EDH, art. 8 (dans l'arrêt *Lopez Ostra* c/ *Espagne*, 9 déc. 1994, n° 16798/90) et au droit à la vie : Conv. EDH, art. 2 (dans les arrêts *Öneryildiz* c/ *Turquie*, 30 nov. 2004, n° 48939/99 et *Boudaïeva et a.* c/ *Turquie*, 29 sept. 2009, n° 15339/02).

(3) H.-S. Afeissa, *Éthique de l'environnement : Nature, valeur, respect*, Paris, Vrin, coll. « Textes clés », 2007, 384 p. – D. Birnbacher, *Éthique utilitariste et éthique environnementale, une mésalliance ?*, in *Rev. philosophique de Louvain* 1998, 4e série, t. 96, n° 3, p. 427-448. – E. Lambert, *Environnement et droits de l'homme*, 2019-2020.

(4) Charte de l'environnement de 2004.

graves ou irréversibles, l'absence de certitude scientifique absolue ne doit pas servir de prétexte pour remettre à plus tard l'adoption de mesures effectives visant à prévenir la dégradation de l'environnement »[5]. En France, ce principe avait déjà été repris par une loi de 1995[6] – et par l'article L. 110-2 du Code de l'environnement[7] – avant d'être consacré dans la Charte de l'environnement de 2004.

Inspiré des normes internationales, ce principe rend nécessaire et préalable à toute action publique, en théorie, la réalisation d'une étude des risques existants ou potentiels et d'une balance avec les bénéfices attendus de cette action permettant de mesurer l'impact éventuel de cette action sur l'environnement et, selon les résultats, de prendre toute mesure nécessaire à limiter la réalisation des risques encourus. Ce principe ne doit pas être confondu avec celui de prévention qui consiste, dès lors qu'il existe un risque, à ne pas réaliser l'action envisagée. Plus qu'un principe juridique, le principe de précaution est un principe philosophique avec une portée anticipatrice très symbolique et peut être considéré comme le pilier du droit à un environnement sain. Introduit par l'article 5 de la Charte en droit français, il est formulé ainsi :

> « Lorsque la réalisation d'un dommage, bien qu'incertaine en l'état des connaissances scientifiques, pourrait affecter de manière grave et irréversible l'environnement, les autorités publiques veillent, par application du principe de précaution et dans leurs domaines d'attributions, à la mise en œuvre de procédures d'évaluation des risques et à l'adoption de mesures provisoires et proportionnées afin de parer à la réalisation du dommage ».

À compter de son apparition dans le droit positif, la Charte et les droits qu'elle consacre ont connu une évolution rapide. Intégré au bloc de constitutionnalité en 2005 par une loi constitutionnelle modifiant l'article 34 de la Constitution[8], le principe de précaution est érigé trois ans plus tard comme un droit fondamental à valeur constitutionnelle par le Conseil constitutionnel[9]. Plus récemment, le droit à un environnement sain a quant à lui été qualifié d'« objectif de valeur constitutionnel »[10] et – de façon plus symbolique encore – de « protecteur du patrimoine commun des êtres humains »[11]. Plus récemment encore, le Conseil d'État

(5) Déclaration de Rio sur l'environnement et le développement, 12 août 1992, A/CONF.151/26 (vol. I).

(6) L. n° 95-101, 2 févr. 1995, dite « loi Barnier », relative au renforcement de la protection de l'environnement : « l'absence de certitudes, compte tenu des connaissances scientifiques et techniques du moment, ne doit pas retarder l'adoption de mesures effectives et proportionnées visant à prévenir un risque de dommages graves et irréversibles à l'environnement à un coût économiquement acceptable ».

(7) C. env., art. L. 110-2 : « Les lois et règlements organisent le droit de chacun à un environnement sain ».

(8) L. const. n° 2005-205, 1er mars 2005, relative à la Charte de l'environnement.

(9) Cons. const., 19 juin 2008, n° 2008-564 DC, *Loi relative aux organismes génétiquement modifiés*. Le Conseil affirme que cette loi « qui organise un régime d'autorisation préalable des OGM et qui soumet leur culture à des procédures d'évaluation, de surveillance et de contrôle ne méconnaît pas le principe de précaution lorsqu'elle organise la coexistence des cultures OGM et non OGM ».

(10) Cons. const., 31 janv. 2020, n° 2019-823 QPC. Le Conseil ne considère pas inconstitutionnelle la norme en cause relative à l'interdiction de produire, de stocker et de faire circuler des produits comportant des substances nocives pour la santé humaine et animale non approuvées. Le Conseil affirme que « le législateur a assuré une conciliation qui n'est pas manifestement déséquilibrée entre la liberté d'entreprendre et les objectifs de valeur constitutionnelle de protection de l'environnement et de la santé ».

(11) *Ibid.* « Aux termes du préambule de la Charte de l'environnement : "l'avenir et l'existence même de l'humanité sont indissociables de son milieu naturel (…) l'environnement est le patrimoine commun des êtres humains (…) la préservation de l'environnement doit être recherchée au même titre que les autres intérêts fondamentaux de la Nation (…) afin d'assurer un développement durable, les choix destinés à répondre aux besoins du présent ne doivent pas compromettre la capacité des générations futures et des autres peuples à satisfaire leurs propres besoins". Il en découle que la protection de l'environnement, patrimoine commun des êtres humains, constitue un objectif de valeur constitutionnelle. »

a été saisi pour avis d'un projet de loi constitutionnelle complétant l'article 1er de la Constitution et relatif à la protection de l'environnement. Dans son avis du 14 janvier 2021, le Conseil d'État met toutefois en garde le gouvernement sur les termes employés par le projet, notamment ceux visant à la « garantie » d'un environnement sain, lesquels feraient peser sur ce dernier une lourde « obligation d'agir »[(12)].

Au regard de ces éléments et de la mise en lumière récente de l'intérêt de la protection de l'environnement, au travers d'un prisme sanitaire notamment, la question se pose de la conciliation de cette problématique avec celle de la croissance numérique. Le numérique représente un certain risque pour l'environnement, et donc indirectement pour la santé. Mais, le numérique est à la fois une solution à l'amélioration de la santé et du cadre de vie de l'Homme. Il est donc important de s'intéresser à la nécessité de trouver un équilibre entre la protection de l'environnement et la liberté d'entreprendre.

## II. – Les risques de la révolution numérique en application du principe de précaution

Partout dans le monde, le numérique a très vite imposé sa présence. Cette nouvelle composante de l'environnement présente ses risques et ses avantages (A), et questionne sur la façon de sa mise en œuvre, notamment du point de vue du principe juridique de précaution (B).

### A. – Les risques et avantages de la révolution numérique

Le numérique présente de nombreux avantages : nouveaux moyens de communication, plus rapides et efficaces, nouvelles technologies de soins, nouveaux modes de distribution, participation à l'amélioration de la santé des populations, lutte contre la désertification. Certains de ces points seront abordés plus loin dans ce chapitre, mais la liste des avantages est longue et ne peut en l'espèce être exhaustive. Le numérique a aussi ses inconvénients, notamment en matière d'environnement, et les exemples sont également nombreux : augmentation de l'émission d'ondes électromagnétiques, production de déchets électriques et électroniques, gaz à effet de serre, consommation énergétique, création de déserts numériques ; ces effets seront présentés plus avant dans ce chapitre. Il reste à propos ici de dresser une liste des avantages et des inconvénients du numérique afin d'expliquer pourquoi il est pertinent, pour l'aborder, de faire référence au principe de précaution. En effet, les effets négatifs suscités font peser un risque sur l'environnement et par conséquent sur la santé humaine. Toutefois ni leur nature pour certains ni leur ampleur pour d'autres ne sont encore connues ou démontrées scientifiquement. Et pourtant, il semble encore aujourd'hui que les politiques sont orientées vers une augmentation, une amélioration et une consécration du numérique. Les décisions en la matière étant seulement saupoudrées de considérations environnementales.

(12) CE, avis, 21 janv. 2021, n° 401868, sur un projet de loi constitutionnelle complétant l'article 1er de la Constitution et relatif à la préservation de l'environnement.

En effet, peu nombreuses sont les mesures de précaution mises en œuvre permettant de réduire les effets néfastes du numérique sur l'environnement et sur la santé, de même que les études d'impact[13].

## B. – Le numérique face au principe de précaution

Il est possible en faisant référence au numérique de se rapporter à la théorie dite de l'« effet rebond » ou « Paradoxe de Jevons » émise en 1865 par William Stanley Jevons, un économiste anglais[14]. Cette théorie énonce l'idée selon laquelle le progrès qui serait apporté par une technologie serait souvent annihilé par le changement de comportement induit par ce dernier. En d'autres termes, l'introduction de nouvelles technologies plus efficaces, permettant à la théorie de réaliser des économies d'énergie et de ressources, augmenterait paradoxalement la consommation finale de ces énergies du fait de l'augmentation inévitable de l'utilisation des technologies en question. Cet effet, appliqué au numérique, se matérialiserait ainsi par une annulation des effets positifs due à l'induction de multiples inconvénients. En 1999, dans un rapport de l'Académie de médecine, a été posée la question de savoir si « le principe de précaution, faisant du "sécuritaire" une priorité absolue, [ne] risque-t-il [pas] d'entraîner un frein à toute entreprise, une inhibition du progrès thérapeutique, une paralysie de l'innovation, une abstention décisionnelle regrettable, bref un immobilisme dommageable, dans tous les domaines » ?

Ce questionnement, appliqué au domaine du médicament étant précisé qu'en matière pharmaceutique « sont mis en place des dispositifs de pharmacovigilance (…) et que personne n'ignore que le rapport bénéfice/risque n'est jamais définitif »[15], est-il transposable à celui du numérique notamment au regard de la théorie de Jevons ? Autrement dit, peut-on appliquer de la même manière le principe de précaution en matière environnementale, sanitaire ou numérique ? Le principe de précaution, qui invite à réfléchir en amont aux conséquences des actions prises dans un domaine particulier, est un principe qui se veut tout de même, sans être tout à fait préventif, à tout le moins prospectif. Comme énoncé plus haut, ce principe ne semble pas pour l'instant couvrir complètement le secteur du numérique compte tenu de la faiblesse des moyens mis en œuvre pour la surveillance et le contrôle des risques et outils mis en œuvre pour anticiper et prévenir leur survenance. Toutefois, compte tenu de son essor, il faut donc bien reconnaître la nécessité de mettre en place des mesures d'évaluation et de réduction des risques liés au numérique, lesquels ne sont pas, ou peu, réversibles.

(13) Sur le sujet, V. not. le rapport de l'OMS sur les champs électromagnétiques ainsi que le projet international CEM dont l'objectif est d'évaluer les effets sur la santé et sur l'environnement de l'exposition aux champs électriques et magnétiques.

(14) W.S. Jevons, *The Coal Question ; An Inquiry Concerning the Progress of the Nation and the Probable Exhaustion of Our Coal Mines*, Londres, Macmillan, 2e éd. 1866.

(15) Rapport adopté lors de la session du CNOM en avril 1999 sous la direction du docteur J. Pouillard (cité *in* D. Grison, *Du principe de précaution à la Philosophie de la précaution : Philosophie*, Université Nancy 2, 2006, Français. ffNNT : 2006NAN21015f).

## § 2. – La mise en œuvre de la révolution numérique au service de l'environnement

Jusqu'à présent, les questions environnementales et numériques étaient déconnectées ; la nature duale matérielle et immatérielle du numérique combinée à une seule approche bénéfices/risques explique en partie la difficulté de quantifier l'impact environnemental du numérique, mais aussi la réalité des bénéfices attendus de son développement. Toutefois, la mise en œuvre de la révolution numérique au service de la révolution environnementale a permis de reposer le débat et d'ouvrir de nouvelles voies (I), tout particulièrement dans le secteur de la santé, et cette nouvelle considération permettra en théorie de tirer le meilleur de chacune des révolutions. Ainsi émerge, depuis quelques années, un environnement juridique au croisement de ces notions (II).

### I. – Une convergence des révolutions

Si la mise en œuvre des révolutions numérique et écologique la plus rationnelle et effective se trouve dans la mise de l'une au service de l'autre, l'environnement numérique n'est pas encore totalement maîtrisé (A). Mais il reste d'ores et déjà possible d'entrevoir que l'ère digitale ne pourra être mise en place autrement qu'au travers de considérations sanitaires et environnementales (B).

#### A. – La difficulté de mettre le numérique au service de l'environnement

Les législations portant sur le numérique et sur l'environnement découlent principalement de la réglementation européenne. Malgré l'émergence de projets de régulation du numérique tels que les projets européens pour certains, il reste que les législations actuelles, fondées sur les principes de « développement durable », « énergies renouvelables », « croissance verte » ou qui prônent la mise en place d'une « économie circulaire », sont vouées à l'échec. Les détracteurs de ces législations emploient des termes tels que « mythe » ou « utopie »[16]. Certains, rappelant la théorie émise par Jevons, ont l'impression de « déjà vu » d'une fiscalité verte qui, selon eux, bien qu'elle présente certains avantages, ne suffit pas à satisfaire les intérêts environnementaux et sanitaires à long terme[17]. En l'espèce, leur position est celle du Conseil constitutionnel qui en 2009 avait déclaré inconstitutionnelles les dispositions législatives relatives à l'instauration d'une taxe carbone, exonérant 93 % des émetteurs industriels[18]. Mais la définition du plan de relance pour 2020 par la Commission européenne est l'occasion d'observer que la stratégie européenne reste

(16) Reporterre, *La « croissance verte » est une mystification absolue, Entretien avec P. Bihouix* (ingénieur et auteur de *L'Âge des low tech : vers une civilisation techniquement soutenable*), 16 juin 2015. Reprenant la définition d'« économie circulaire » de l'ADEME, P. Bihouix affirme qu'« il s'agit de "faire plus avec moins". C'est beau, mais utopique, car on ne sait pas découpler de manière absolue croissance du PIB et décroissance de la consommation matérielle et pollution ».

(17) A. Missemer et W. Stanley Jevons, *Un pionnier des réflexions sur la fiscalité écologique*, L'Économie politique, Scop-Alternatives économiques, 2013, 60, p. 78-90.f.

(18) Dans sa décision, le Conseil constitutionnel énonce que « l'importance des exemptions totales de contribution carbone étaient contraires à l'objectif de lutte contre le réchauffement climatique et créaient une rupture d'égalité devant les

celle-ci, la stratégie de l'Union européenne est ambitieuse. L'UE prévoit de réformer l'espace numérique pour permettre à terme de parvenir à la mise en place d'un numérique neutre[19]. Portant haut ses ambitions, l'Union a ainsi proposé de mettre en place de nouvelles ressources propres, lesquelles contribueraient largement au remboursement de la dette soulevée afin de faire face à l'épidémie de Covid-19 et dans le cadre du budget européen à long terme pour 2021-2027. Ces nouvelles ressources consistent à instaurer de nouvelles taxes, respectivement plastique, numérique et carbone. Une des réactions face à ce discours est de se demander si les bénéfices de ces mesures contribueront effectivement à la protection environnementale et non dans leur totalité à la seule relance économique européenne.

Mais, la proposition de loi européenne sur le climat de 2018[20] montre bien la volonté du Conseil européen de faire de la construction d'une Europe neutre pour le climat, verte, équitable et sociale, l'une des quatre grandes priorités de son programme stratégique pour la période 2019-2024. Compte tenu des récentes données scientifiques disponibles et de la nécessité de renforcer l'action climatique menée à l'échelle mondiale, le Conseil s'est ainsi fixé l'objectif d'une Union neutre pour le climat d'ici 2050, dans ses conclusions du 12 décembre 2019[21], conformément aux objectifs de l'Accord de Paris[22]. Et ainsi que l'affirme le Pacte vert pour l'Europe, selon lequel toutes les actions et politiques de l'Union devraient concourir à lui permettre de réussir une transition juste vers la neutralité climatique et un avenir durable[23]. Aussi, la Commission européenne a annoncé le 24 février 2021, l'adoption d'une nouvelle stratégie relative à l'adaptation au changement climatique, permettant de construire un avenir résilient face au changement climatique.

En 2019, le Conseil européen a reconnu la nécessité de mettre en place un cadre facilitateur et admis que la transition exigerait d'importants investissements publics et privés. Et conclut que toutes les législations et politiques pertinentes devaient être compatibles avec la réalisation de l'objectif de neutralité climatique et y contribuer. Et l'Union d'affirmer, à l'occasion de la mise en place de la nouvelle stratégie, que « l'objectif des propositions présentées aujourd'hui est de se concentrer davantage sur l'élaboration de solutions plutôt que sur la compréhension du problème, et de passer de la planification à la mise en œuvre ».

Paradoxalement, c'est donc dans d'autres législations, telles que celles relatives au numérique, que se retrouvent des mesures prônant un développement plus respectueux de l'environnement. En effet, pour parvenir à mettre en œuvre la révolution numérique, l'Union européenne prévoit de passer par la construction d'une stratégie de capacité digitale, se traduisant par l'augmentation de l'investissement dans le domaine de l'environnement et de l'utilisation des technologies numériques

charges publiques ». Par voie de conséquence il a censuré l'ensemble du régime relatif à cette contribution (art. 7, 9 et 10) (Cons. const., 29 déc. 2009, n° 2009-599 DC, Communiqué de presse, *Loi de finances pour 2010*, non-conformité partielle).

(19) Digital Europe, *Draft orientations for the preparation of the work programme(s) 2021-2022* : « Digital for a clean planet » ou « le digital pour une planète propre ».

(20) PE et Cons. UE, Prop. de règlement établissant le cadre requis pour parvenir à la neutralité climatique et modifiant le règlement (UE) n° 2018/1999 (loi européenne sur le climat).

(21) Conclusions du Conseil européen, 12 déc. 2019.

(22) L'Accord de Paris a été signé par l'UE le 5 octobre 2016 et est entré en vigueur le 4 novembre 2016.

(23) Communication de la Commission au PE, au CE, au CESCE et au CdR, *Le pacte vert pour l'Europe*, 11 déc. 2019 : Doc. COM (2019), 640 final.

dans les secteurs publics et privés et par le renforcement du réseau des pôles d'innovation numériques européens, garantissant une large utilisation de ces technologies numériques dans toute l'Europe. Le développement du numérique consiste à répondre aux enjeux complexes de santé de demain (modélisation moléculaire, outils de diagnostic et de traitement des nouvelles maladies) et ceux liés à l'environnement (prévisions météorologiques)[24].

L'analyse croisée des réglementations portant sur le numérique et sur l'environnement dernière montre que ces deux préoccupations sont encore largement déconnectées. Mais, considérant ce qui précède, alors qu'il s'agissait de combler un certain vide juridique en la matière, il est encourageant de voir qu'il est possible que les mesures se précisent. Celles-ci posent les bases de la mise en œuvre de la révolution numérique au service de l'environnement par le biais notamment de nouvelles technologies, lesquelles seront déployées pour mettre en œuvre les mécaniques environnementales et sanitaires de demain. Mais une question persiste, celle de savoir si cette approche est la « meilleure ». Il ne faut pas oublier les impacts environnementaux du numérique et la difficulté de les prévoir, de les connaître, et plus encore de les réparer. Ces considérations posées, l'analyse de l'encadrement juridique se pose alors, permettant d'identifier en termes de risques, et donc de prévention, réparation, indemnisation, ce que l'homme peut mettre en place pour organiser une réponse à la désorganisation environnementale par l'effet positif du numérique.

## B. – La santé, point de convergence numérico-environnemental

Après toute cette exposition de l'impact du numérique sur l'environnement, il est possible de voir que les législations numériques et environnementales sont encore déconnectées, bien qu'un rapprochement s'opère par le fait de la considération commune. La législation récente relative au numérique emprunte des caractéristiques des législations environnementales et sanitaires avec une approche que l'on pourrait à nouveau qualifier d'anthropocentrée, se concentrant sur le bien-être de l'Homme. Les caractéristiques du numérique, de l'environnement et de la santé les font se rapprocher et devraient logiquement les soumettre à des principes similaires tels que le principe de précaution, permettant dès lors d'adopter des mesures adéquates et suffisantes pour réduire drastiquement les risques encourus. À ce titre, a récemment émergé un principe de *sustainability by design*[25], qui n'est pas sans rappeler les principes modernes de *privacy by design* et de responsabilisation issus des normes européennes relatives à la protection des données[26]. Le ton est donné, il faut que le défi soit relevé de mettre en place une réglementation adaptée aux temps présents et futurs permettant aux sociétés de s'adapter rapidement, et idéalement en mesure de perdurer dans le temps. Pourtant, certaines incertitudes subsistent et freinent la mise en place de cette législation. En effet, ce

(24) Comm. UE, brochure, *Digital Europe for a more competitive, autonomous and sustainable Europe*, 20 janv. 2021.
(25) « Durable par conception » (ARCEP, *Le rapport pour un numérique soutenable*, déc. 2020).
(26) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 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.

principe de précaution n'a en réalité à ce jour jamais été admis en droit de la santé par le Conseil constitutionnel.

Dans une décision du 27 juin 2001, le Conseil constitutionnel jugeait : « contrairement à ce qu'affirment les requérants, le principe de précaution ne constitue pas un objectif de valeur constitutionnelle ». Pourtant, force est de constater que ce principe est devenu une référence constante dans les discours relatifs à la santé[27]. Et opportun de voir que le domaine possède en effet ses propres techniques de vigilance et de surveillance, d'une part, et de réparation des conséquences des risques sanitaires, d'autre part, qui ont pu et pourraient encore inspirer le droit de l'environnement[28]. Le droit de l'environnement a développé des règles nouvelles, mais parfois de signification de portée ambiguë, telles que la notion de patrimoine commun, de développement durable, de principe pollueur-payeur et de précaution, dont il convient de se demander dans quelle mesure elles pourraient être étendues au droit de la santé.

Ainsi, le droit à un environnement sain a été récemment promu par le Conseil constitutionnel au rang d'objectif à valeur constitutionnelle. À l'appui d'une question prioritaire de constitutionnalité (QPC), il été soutenu que la loi interdisant la production et l'exportation de certains produits phytopharmaceutiques dangereux en raison de leurs effets sur la santé humaine et l'environnement était contraire à la liberté d'entreprendre protégée par l'article 4 de la Déclaration des droits de l'homme et du citoyen (DDHC). Mais la disposition contestée atteste de plusieurs motifs d'intérêt général légitimant son existence. D'une part, la préservation de la santé humaine. À cet égard, le Conseil constitutionnel considère depuis longtemps que la préservation de la santé, telle que garantie par la Constitution de 1946, permet de justifier une atteinte à une liberté que la Constitution garantit, telle que la liberté d'entreprendre[29]. D'autre part, la préservation de l'environnement. Pour la première fois, le Conseil constitutionnel considère la protection de l'environnement comme permettant au législateur de restreindre la liberté d'entreprise et l'érige en objectif de valeur constitutionnelle. Toutefois, bien qu'elle ait son importance, cette décision emporte une réserve puisqu'un objectif même à valeur constitutionnelle n'est pas un droit ou une liberté et ne peut pas être invoqué devant le juge ni par un particulier, ni par une entreprise ou une association dans le but de contester une disposition législative. Il en va de même, pour le moment, des droits et devoirs consacrés par la Charte comme le principe de précaution. La décision n'en révèle pas moins l'attachement du Conseil constitutionnel aux préoccupations environnementales qui irriguent désormais la société. Finalement, à ce propos, Sandrine Maljean-Dubois, directrice de recherche au CNRS, rappelle que le droit de l'environnement trouve son origine dans la santé humaine, dans les premières législations sur la pollution

(27) D. Truchet, *Aspects juridiques*, *in* Document d'orientation scientifique, 31 mars et 1er avril 2005 organisé par le ministère délégué à la recherche, le CEA, le CEE, le CNRS, la CPU, l'INED, l'INRA, l'INSERM, l'Institut Pasteur, l'IRD, dans le cadre du Plan national santé environnement et du Plan santé travail en liaison avec le ministère des Solidarités, de la Santé et de la Famille, le ministère de l'Écologie et du Développement durable, le ministère de l'Emploi, du Travail et de la Cohésion sociale.

(28) *Ibid*.

(29) V. Cons. const., 13 août 1993, n° 93-325 DC, § 16.

et les nuisances sonores[30]. L'environnement et la santé ont été par suite séparés quelques temps ; l'environnement s'intéressant à la nature et à la biodiversité, alors que la santé est liée à la protection humaine ou animale, ce n'était que pour mieux se retrouver, ces domaines étant fondamentalement liés. C'est donc naturellement que le principe de précaution s'est retrouvé à être considéré comme principe commun, vision magnifiée dans le concept multidimensionnel et pluridisciplinaire *One Health*[31], une seule santé, fondement de la stratégie législative européenne.

Ainsi, les deux domaines se confondent, se complètent et transcendent les concepts classiques juridiques. « Émergence d'une humanité non plus seulement interconnectée, hypermobile faisant de l'accès une valeur capitale, mais désormais hybridée à des systèmes qui orientent et décident de comportements collectifs et individuels, sous des modalités encore discrètes mais déjà prégnantes, appelées à être étendues à de nombreux champs de la société »[32], le numérique est empreint des législations sanitaires et environnementales.

## II. – L'émergence d'une réglementation croisée

Considérant que les notions de numérique, environnement et santé sont à la croisée des chemins, leur construction et leur encadrement juridique nécessitent la participation active de tous et dicte à chacun de prendre ses responsabilités en amont de toute action. L'approche transversale de la révolution numérique au service de la santé, mettant en lumière une vision anthropocentrée de la législation, laisse émerger des questions éthiques portant sur le sort de l'homme et l'évolution vers le transhumanisme, et des questions de responsabilité juridique des acteurs impliqués. À l'image de la Charte de 2004, qui impose à toute personne de prendre part à la sauvegarde et à l'amélioration de l'environnement et de répondre des dommages qui lui sont faits. Par exemple il faudra, dans l'environnement de demain, pouvoir appréhender les questions liées aux dommages causés par la technologie numérique dans son utilisation au service de l'environnement ou de la santé ; particulièrement dans le cas des intelligences artificielles. Il est question de fixer dans la loi les règles de responsabilité et de savoir si un dommage causé par la technologie sera le fait d'une « fiction juridique » bien qu'autonome dans une certaine mesure et donc par prolongement celui d'une personne physique/humaine ou s'il sera admis qu'une technologie puisse être responsable de ses propres faits indépendamment de l'Homme. La question de la réparation a été peu traitée, mais se pose de façon cruciale et complexe dans la mesure où dans un tel domaine, les dommages ne sont pas reconnus aisément et relèvent souvent d'une temporalité qui peut s'étendre sur plusieurs décennies et méritent à nouveau d'être explorés tant à un niveau individuel que collectif. Le principe fondamental « pollueur-payeur »[33]

(30) S. Maljean-Dubois, *Quel droit pour l'environnement ?*, UMR 7318, Aix-Marseille Université, 7 mai 2013.

(31) Ce concept insiste sur la nécessaire reconnaissance des liens entre santé humaine, santé animale et environnement. Ce concept a été largement repris par l'ensemble des organisations mondiales de santé humaine et animale et de protection environnementale.

(32) É. Sadin, *L'administration numérique du monde*, éd. L'Échappée, 2013, p. 67.

(33) Le principe du pollueur-payeur est, avec le principe de précaution, un autre des grands principes du droit de l'environnement. Il est issu de la Charte de l'environnement de 2004, article 4 qui dispose que « toute personne doit

en matière de protection de l'environnement consiste à faire supporter au pollueur les atteintes portées à l'environnement. En matière de santé, le principe est celui de la responsabilité de droit commun qui permet également d'amener la personne à réparer les conséquences de son acte. La question de la reconnaissance de la responsabilité d'une personne morale a été déjà traitée par le Conseil d'État. En effet, le 8 février 1873, dans une jurisprudence célèbre en droit administrative le Conseil d'État a reconnu pour la toute première fois la responsabilité de l'État[34]. En revanche, la mise en place d'une sanction adéquate est plus subtile et plus complexe et aucune réponse n'a pas encore été donnée à ce propos.

En aval de la réparation, dans le sillage du principe de précaution, se trouve la gestion des risques. Cette gestion repose sur l'articulation de différentes fonctions : l'expertise, suscitée par les pouvoirs publics et passant par la mobilisation des connaissances produites par des agences spécialisées et/ou des organismes de recherche (organismes scientifiques, universités) ; la décision, assumée par les pouvoirs publics (que ce soit au sein des administrations ou à des niveaux plus politiques) ; l'information ; la concertation (prise en charge par les pouvoirs publics, en lien avec les agences et organismes). La gestion des risques repose également sur une séparation des fonctions, l'expertise devant *a priori* être indépendante des intérêts économiques et des pouvoirs publics, la décision devant quant à elle préserver des capacités d'arbitrage, de choix entre différentes options. La gestion repose enfin sur l'affichage d'un certain nombre de principes (recherche de l'objectivité scientifique, transparence de l'expertise, responsabilité des pouvoirs publics en matière de sécurité collective, procédures démocratiques, *etc.*). À la suite de l'émergence de nouvelles catégories de problèmes (menaces) échappant à la catégorie du risque (dans laquelle les faits numériques peuvent être inclus), les critères de la gestion des risques ont été complétés par l'exercice de la vigilance[35], de la veille scientifique et de la mise en œuvre du principe de précaution[36]. La sécurité dans les activités à risques apparaît essentiellement construite sur la connaissance *a priori* des risques, l'élaboration de normes, règles et procédures visant à empêcher leur réalisation et la mise en place de dispositifs de contrôle garantissant la bonne application de ces règles. L'objectif est d'éviter la survenue de défaillances de tous ordres (panne technique, erreur humaine, dysfonctionnement organisationnel, *etc.*) susceptibles de remettre en cause la sécurité. Dans cette perspective, la sécurité est considérée comme une priorité quasi absolue appelant une très forte mobilisation sur le plan de la connaissance et de l'action[37].

contribuer à la réparation des dommages qu'elle cause à l'environnement », complété notamment par l'article L. 110-1 du Code de l'environnement qui dispose que « les frais résultant des mesures de prévention, de réduction de la pollution et la lutte contre celle-ci sont supportés par le pollueur ».

(34) T. confl., 8 févr. 1873, n° 00012, publié au recueil.

(35) D. Torny et F. Chateauraynaud, *Les sombres précurseurs : une sociologie pragmatique de l'alerte et du risque*, Paris, éd. de l'École des Hautes Études en sciences sociales, 1999, 480 p.

(36) O. Godard et *al.*, *Traité des nouveaux risques*, Gallimard, coll. « Folio actuel », 2002.

(37) C. Gilbert, *Propositions pour une nouvelle approche des risques de santé-travail et santé-environnement*, *in* Document d'orientation scientifique, 31 mars et 1er avril 2005, organisé par le ministère délégué à la Recherche le CEA, le CEE, le CNRS, la CPU, l'INED, l'INRA, l'INSERM, l'Institut Pasteur, l'IRD, dans le cadre du Plan national santé environnement et du Plan santé travail en liaison avec le ministère des Solidarités, de la Santé et de la Famille, le ministère de l'Écologie et du Développement durable, le ministère de l'Emploi, du Travail et de la Cohésion sociale.

La question prégnante est ainsi posée par le secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL), qui se demande « comment réguler sur un territoire déterminé un phénomène par nature déterritorialisé ? ». Pour la CNIL, la réponse consiste à affirmer qu'outre les enjeux de territorialité du droit, et donc de souveraineté juridique, il convient de rechercher une « réponse européenne et des échanges plus importants entre autorités »[38]. La théorie de la gestion des risques par un organe de contrôle et de surveillance public spécifique appliquée au numérique et à l'environnement a été implémentée en France par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). En effet, l'ARCEP a intégré dans ses décisions tant les dimensions collectives qu'européenne posées par le sujet et a publié en mai 2020 un document intitulé « Accord de Paris et urgence climatique : enjeux de régulation », un travail issu d'une réflexion commune de huit autorités administratives ou publiques indépendantes[39]. Mettant en place une expertise nécessaire à la bonne gestion des risques du numérique, les travaux de l'ARCEP s'inspirent des réflexions de divers organismes qui tentent, déjà depuis plus ou moins longtemps, d'établir une stratégie permettant de pallier l'insuffisance actuelle des connaissances des impacts du numérique sur l'environnement. De ces réflexions ont émergé notamment un « Livre blanc : Numérique et environnement »[40] et un principe de sobriété numérique[41]. L'ARCEP a précisé travailler plus avant sur la question numérico-environnementale en coopération avec l'Agence de l'environnement et de la maîtrise de l'énergie (ADEME), avec laquelle elle a accepté en 2020 une mission ministérielle portant sur la quantification de l'empreinte environnementale des infrastructures des réseaux et sur l'identification et l'évaluation des différents facteurs qui permettent de quantifier cette empreinte. Ces travaux feront l'objet d'un rapport spécifique à la fin de l'année 2021. Également, le 11 juin 2020, une plateforme de travail « pour un numérique soutenable » a été lancée[42] et les résultats de cette initiative ont été publiés par l'ARCEP le 15 décembre 2020 dans un rapport, lequel fait onze propositions pour conjuguer développement des usages et réduction de l'empreinte environnementale du numérique. Le rapport de l'ARCEP s'inspire en outre de textes légaux visant à mettre en place une normalisation croisée. Il cite, entre autres, la

(38) É. Geoffray, *Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? : Nouveaux Cah. Cons. const.* 2016/3, n° 52, p. 5 à 16.

(39) ARCEP, *Accord de Paris et urgence climatique : enjeux de régulation* : « Réunis depuis 2017 au sein d'un groupe informel, l'Autorité de la concurrence, l'Autorité des marchés financiers (AMF), l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), l'Autorité de régulation des transports (ART), la Commission nationale de l'informatique et des libertés (CNIL), la Commission de régulation de l'énergie (CRE), le Conseil supérieur de l'audiovisuel (CSA) et la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) publient leurs réflexions sur l'urgence climatique et sur les enjeux de régulation que celle-ci représente ».

(40) Iddri, FING, WWF France, GreenIT.fr, *Livre blanc Numérique et environnement : « Faire de la transition numérique un accélérateur de la transition écologique : 26 propositions pour lancer le débat »*, 2018.

(41) The Shift Project, think tank français sur la transition énergétique, dans son rapport *Lean ICT, pour une sobriété numérique* (14 oct. 2020) s'intéresse au développement exponentiel du numérique et de la façon dont son développement peut interagir avec les objectifs décarbonisation de nos sociétés.

(42) Les cinq thématiques de travail étant les suivantes : adapter les pratiques commerciales, lutter contre les obsolescences, choisir nos réseaux, penser les services et contenus numériques et façonner les réseaux.

proposition de loi du 12 octobre 2020[43] visant à réduire l'empreinte environnementale du numérique en France rédigée à la suite d'une mission d'information « Empreinte environnementale du numérique : faut-il s'inquiéter ? » lancée en janvier 2020. Ce rapport législatif recommande au gouvernement « de saisir l'occasion de ce texte pour faire avancer notre engagement en matière de transition numérique durable, et pour permettre à la représentation nationale de débattre de manière éclairée sur des mesures qui, loin de n'être que techniques, sont essentielles pour assurer le respect des engagements climatiques de la France dans le cadre de l'Accord de Paris »[44]. À son tour, le rapport de l'ARCEP invite les organes politiques à se mobiliser, car ce sont eux les décisionnaires finaux[45]. Assez rapidement après ces déclarations, le 12 janvier 2021, le Sénat a adopté la proposition de loi sus-citée, laquelle doit permettre au secteur du numérique de réduire son empreinte environnementale et à la France de tendre vers un numérique plus sobre. Selon le rapport du Sénat, l'objectif est d'orienter le comportement de tous les acteurs du numérique, qu'il s'agisse des consommateurs, des professionnels du secteur ou encore des acteurs publics, afin de garantir le développement en France d'un numérique sobre, responsable et écologiquement vertueux. Cela confirme qu'il s'agit d'éviter, afin de réussir la transition écologique, que le numérique ne devienne pas une source de pollution exponentielle. Quatre chapitres composent cette proposition de loi. Premièrement, des dispositions destinées à faire prendre conscience aux utilisateurs que le numérique a un impact sur l'environnement. Suivies de mesures destinées à lutter contre l'obsolescence programmée. Un troisième chapitre vise à promouvoir des usages numériques écologiquement vertueux. Enfin, la quatrième partie concerne la réduction de la consommation d'énergie des *datacenters*. La proposition doit encore faire l'objet d'une relecture par la Commission du développement durable et de l'aménagement du territoire avant d'être finalement examinée par l'Assemblée nationale. Le sénateur Patrick Chaize, auteur de la proposition, explique à ce propos : « Ce secteur (…) représente 2 % de notre empreinte carbone aujourd'hui, mais ce sera 7 % demain si nous ne faisons rien. Je suis heureux de voir se concrétiser une initiative parlementaire inédite, au-delà des habituels clivages partisans, avec près de 130 signataires issus de tous les groupes ».

Depuis le XIX^e^ siècle, à l'échelle de la planète, les modifications majeures de l'environnement liées à l'homme concernent essentiellement l'urbanisation, le changement de pratiques agricoles, et maintenant le numérique. Ces aménagements sont à la fois sources de progrès socio-économique et objets d'inquiétude pour l'avenir de l'humanité. Dans le cas du numérique et de ses conséquences

(43) AN, Prop. de loi, visant à réduire l'empreinte environnementale du numérique en France (https://www.assemblee-nationale.fr/dyn/15/dossiers/DLR5L15N40696).

(44) Rapp. Sénat n° 555 (2019-2020), fait au nom de la commission de l'aménagement du territoire et du développement durable, déposé le 24 juin 2020.

(45) ARCEP, environnement, 15 mai 2020 : « La mise en place d'une régulation environnementale du numérique est une décision qui relève d'abord du pouvoir politique et l'ARCEP intervient ici comme force de proposition. C'est à lui qu'il appartient de définir le niveau d'ambition et en particulier la trajectoire dans laquelle il souhaite inscrire le secteur numérique pour que celui-ci participe pleinement à la stratégie bas carbone. C'est aussi au pouvoir politique de définir, par la loi les outils de transparence, d'incitation et le cas échéant de contrainte qui permettront de donner corps à cette régulation, ainsi que les institutions en charge de leur mobilisation ».

sanitaires, cette dichotomie entre bénéfice socio-économique et coût sanitaire n'est pas particulièrement évidente. Mais l'observation doit être réalisée de façon plus systématique et plus globale. Force est de constater que, quelle que soit l'acception de la santé à laquelle on se réfère, état de bien-être ou absence de maladie, l'état de santé des populations résulte de très nombreux facteurs, parmi lesquels la composante environnementale occupe une part considérable, et que l'identification et la prise en compte des interactions santé-environnement deviennent plus explicites au fil des ans, notamment au travers des législations et des politiques territoriales. Cédric O, secrétaire d'État chargé de la transition numérique, affirme à ce sujet : « Je crois au progrès technologique. C'est une condition de l'émancipation. C'est l'ADN de la France que d'assumer ce chemin vers la modernité, condition de prospérité et de réduction des inégalités. Mais l'innovation n'est pas bonne en soi si elle n'est pas maîtrisée. Prenons le temps d'entrer dans le détail des dispositions proposées. Le progrès doit être mis au service de la préservation de l'environnement. La transition énergétique ne sera possible qu'avec le concours du numérique, qu'il ne s'agit pas de brider *a priori* »[(46)].

SECTION 2

## ÉVOLUTION DE LA POLITIQUE TERRITORIALE ET DYNAMISATION DES TERRITOIRES

Comme a pu le rappeler Jacqueline Gourault, nouvelle ministre de la Cohésion des territoires et des Relations avec les collectivités territoriales : « Nous avons mis 100 ans à apporter le téléphone aux Français ; 90 ans à électrifier le territoire ; nous mettrons 10 ans à relier chacun à Internet. L'aménagement numérique est le grand chantier de la décennie »[(47)]. L'accès des citoyens au numérique est donc aujourd'hui placé comme une réelle priorité et son accès est jugé aussi essentiel que celui à l'électricité.

Cette volonté d'être toujours plus connecté, soutenue par l'État français, n'est pas anodine face à l'évolution des enjeux économiques, écologiques et sanitaires. La rapidité et la simplification des échanges renforcent l'attractivité du numérique, lequel s'impose partout dans notre société. Les politiques territoriales en sont affectées et le dynamisme préétabli des territoires en France modifié.

En facilitant les échanges, le numérique permet de relier des territoires qui étaient sinon oubliés, du moins mis de côté. De nombreux services, auparavant compliqués à mettre à disposition de la France « de la Zone blanche »[(48)], sont aujourd'hui à portée de clic des citoyens.

(46) Sénat, Compte rendu analytique officiel, 12 janv. 2021, relatif à la proposition de loi visant à réduire l'empreinte environnementale du numérique.
(47) Discours lors du premier Congrès national des élus au numérique, 29 et 30 janv. 2019.
(48) En France, une « zone blanche », d'après l'ARCEP, est une zone qui n'est couverte par aucun opérateur mobile.

Dans cette optique, l'État se poste comme l'instigateur d'une France complètement connectée (§ 1), ambitieuse dans l'application de ses principes (§ 2).

## § 1. – L'État : moteur essentiel de la France « 100 % connectée »

### I. – L'édiction des principes par le gouvernement

Le gouvernement, avec l'arrivée d'Internet et son utilisation croissante, se rend compte qu'une réelle fracture se met en place au sein même de la population française. Se crée une inégalité entre ceux ayant accès au numérique dans des conditions optimales et ceux qui ne sont pas assez formés ou qui n'ont pas du tout accès au réseau. L'imminence de cette fracture entrait directement en contradiction avec la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, dite « loi Léotard ». Cette loi prévoit une déréglementation du secteur des télécommunications telle que la privatisation de TF1 (imputée à Bouygues), la libéralisation du secteur des réseaux câblés ainsi que de la téléphonie mobile (entrée de Itineris et SFR).

Le 17 décembre 2009 est publié le texte de la loi n° 2009-1572 relative à la lutte contre la fracture numérique. Ses deux volontés principales, formant par ailleurs ses deux titres, sont tout d'abord la création d'une facilité de transition vers la télévision numérique et ensuite la prévention de l'apparition de cette fameuse fracture, spécifiquement dans le très haut débit. La majorité des articles viennent modifier directement le texte de la loi Léotard afin d'adapter son contenu aux problématiques contemporaines. Cette modification restera d'ailleurs, jusqu'à ce jour, la plus importante jamais apportée. Une nouveauté apportée par l'article 4 de cette loi de 2009 renforce le rôle central qu'ont les collectivités en requérant l'institution dans chaque département d'une commission de transition vers la télévision numérique.

Le deuxième changement législatif important se tient en la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, tendant elle aussi à préparer la France aux enjeux de la transition numérique et de l'économie de demain. Cette loi vise à adapter le triptyque classique des valeurs françaises au numérique et se traduit par « Liberté d'innover, Égalité des droits, Fraternité d'un numérique accessible à tous » auxquels vient s'ajouter « l'Exemplarité d'un État qui se modernise ». Ses trois points essentiels tiennent en une plus grande circulation des savoirs et des informations afin de garder une compétitivité certaine pour la France, la création d'un cadre clair notamment en matière de protection des données personnelles et, pour terminer, la construction d'une République numérique ouverte et inclusive permettant un accès aux outils numériques à l'entièreté des citoyens français, peu importe leur territoire ou leur situation financière.

La volonté de porter une plus grande attention à la gestion des données personnelles en adéquation avec le déploiement de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés apparaît alors clairement. La

loi pour une République numérique place, une fois de plus, la France comme pionnière en matière de protection des données. L'Europe, inspirée, unifiera le processus avec le règlement (UE) n° 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, dit « RGPD ».

En décembre 2021, la Commission européenne propose une réforme de l'espace numérique[49] contenant de nouvelles règles applicables à tous les services numériques tels que les médias sociaux, les *marketplaces* et les plateformes en ligne actives au sein de l'Union européenne. Son but principal est la protection des consommateurs au sein du marché unique, mais aussi l'innovation, la croissance et la compétitivité afin de toujours fournir de nouveaux services en ligne aux utilisateurs européens. L'Union européenne montre une nouvelle fois sa fonction de garde-fou quant à la protection du marché unique et du consommateur européen face aux innovations et à la modification du marché qui se trouve de plus en plus numérique.

En plus de cette protection importante, elle renforce la position du gouvernement et de l'État français concernant sa quête d'une « France 100 % connectée ».

Les bases sont posées par le gouvernement, et précisées par une explication du but « Accès au numérique pour tous » par le ministère de la Cohésion des Territoires et des Relations avec les collectivités territoriales. Une France connectée passe par un accès efficace à Internet et au réseau de téléphonie mobile. Certaines parties du territoire françaises ne sont desservies par aucun réseau, ces zones sont appelées « zones blanches ». La visée principale du gouvernement est de combattre le sentiment d'isolement des zones blanches et de permettre un meilleur accès aux services. Depuis 2009, les zones blanches sont couvertes par un accord de partage de l'Association française des opérateurs mobiles (AFOM) entre les trois principaux opérateurs de téléphonie mobile. Cet accord de partage se révèle essentiel pour la cohésion des territoires français. À travers la « loi ELAN » promulguée le 23 novembre 2018, l'État français s'est fixé plusieurs objectifs dont la couverture numérique du territoire[50]. Cette loi vise notamment : l'accélération de la couverture numérique du territoire, les propriétaires, les opérateurs, mais surtout les collectivités territoriales qui sont placées en acteurs essentiels du déploiement du réseau.

Néanmoins, pour mettre en place ces dispositifs, la place des collectivités territoriales est centrale.

## II. – La place centrale donnée aux collectivités territoriales

Le Gouvernement français souhaite placer les collectivités territoriales comme moteur de la résolution de la fracture numérique. Celle-ci se voit notamment par la publication du « Guide à destination des maires, Plan de relance » présenté

(49) *Digital Markets Act* et *Digital Services Act*, 15 déc. 2020.
(50) L. n° 2018-1021, 23 nov. 2018, portant évolution du logement, de l'aménagement et du numérique.

conjointement par Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance, et Jacqueline Gourault, ministre de la Cohésion des territoires et des Relations avec les collectivités territoriales en décembre 2020.

C'est évidemment en ce sens que les lois publiées pour résoudre la fracture numérique mettent les collectivités territoriales en acteur principal. Ce sont elles qui connaissent le mieux leurs particularités et leurs difficultés. Cette déconcentration des pouvoirs de l'État permet surtout une mise en place homogène des mesures décidées par le gouvernement.

Les collectivités territoriales se sont vu attribuer une mission principale par la loi ELAN : la simplification des démarches administratives pour l'accélération du déploiement des réseaux. Ainsi, sont facilitées bon nombre de démarches, par exemple le déploiement d'antennes qui devaient auparavant respecter la continuité de l'urbanisation existante en zones de montagne. Aujourd'hui, elles bénéficient d'une dérogation à ce principe[51].

La notion de très haut débit, depuis le début de cette partie, se résume à un accès à un Internet performant permettant rapidement la réception et l'envoi d'un grand nombre de données. La Commission européenne définit d'ailleurs un standard à 30 Mbit par seconde pour qualifier un débit de « très haut ». Ce standard provient du Plan « France Très Haut Débit » approuvé par la Commission européenne en 2016. Les collectivités territoriales doivent donc s'attarder sur l'accès au très haut débit pour tous, mais doivent aussi enclencher le second grand chantier qui concerne la 4G et bientôt la 5G. Fin 2018, les opérateurs privés ont pris des engagements en faveur d'un investissement massif pour l'amélioration et l'extension de leur réseau mobile.

Les collectivités, après s'être penchées sur la qualité du réseau et sa mise à disposition des populations les plus isolées numériquement, doivent aussi former des personnes qui n'avaient pas pour habitude d'avoir accès à ce genre de technologies. Ainsi, les collectivités territoriales ont rassemblé autour d'elles opérateurs de services publics, acteurs locaux et entreprises dans le but d'atteindre plusieurs objectifs par la mise en place d'actions concrètes efficaces. La première est l'identification et l'accompagnement des publics éloignés par tous moyens afin de les orienter vers la bonne solution. La deuxième est l'offre d'un Pass numérique sous forme de chéquier donnant droit à des heures de formation au numérique dans des lieux de formation à proximité. Une troisième action est l'émergence de ces lieux de formation (les « hubs France Connectée »)[52] et l'accompagnement de ceux qui ne seront pas formés par des aidants numériques.

Les citoyens ne sont pas les seuls à devoir être formés sur le numérique : les collectivités territoriales, les élus et agents publics doivent l'être également. Sur ce point, une Masterclass leur est dispensée et deux plateformes de ressources en ligne sont ouvertes afin de leur venir en aide si nécessaire.

(51) D. n° 2018-1123, 10 déc. 2018, relatif à l'extension du régime de la déclaration préalable aux projets d'installation d'antennes-relais de radiotéléphonie mobile et à leurs locaux ou installations techniques au titre du Code de l'urbanisme.

(52) Terme utilisé par la Stratégie Nationale pour une France Connectée, pilotée par M. Mahjoubi, secrétaire d'État chargé du numérique auprès du Premier ministre, qui vise à inclure l'ensemble des territoires et des citoyens dans la transition numérique.

Le gouvernement et les collectivités tendent à agir de concert afin de combler cette fracture numérique de la population française. Les principes étant posés et les collectivités territoriales disposant d'outils adaptés, vient le temps de l'application de ceux-ci.

## § 2. – Une application ambitieuse

Les engagements du gouvernement sont ambitieux et, afin de les appliquer au mieux, des actions incitatives sont mises en place (I) pour tenter de mettre fin définitivement à la fracture numérique et à l'« illectronisme »[53] (II).

### I. – La mise en place d'actions incitatives

Pour supporter les actions des collectivités territoriales, des outils ont été mis à leur disposition tels que le Plan « France Très Haut débit » (A), les tiers-lieux et les Fabriques de territoire (B), le Label « Territoires, villes et villages Internet » (C) et le Forum numérique en commun et France Relance (D).

#### A. – Le Plan « France Très Haut débit »

Ce Plan « France Très Haut Débit » (PFTHD) manifeste une volonté de couvrir l'intégralité du territoire français en très haut débit. Il est adopté le 28 février 2013 par le gouvernement. Son échéance est d'abord placée en 2022 avant d'être repoussée à 2025, voire 2030 pour certaines régions. Une spécificité de ce PFTHD est la liaison entre l'État, les collectivités territoriales, mais également des opérateurs privés afin de moderniser et monter en débit les réseaux.

Les collectivités détiennent une compétence légale leur allouant une place centrale dans la conception de ces réseaux locaux. Parfois, pour mettre en place cette initiative, elles se regroupent pour obtenir plus de moyens.

L'État rappelle, en février 2020, qu'une mobilisation de 280 millions d'euros serait allouée à ce chantier. Il est à noter que le financement de ce déploiement de réseau très haut débit sera conditionné à la présentation des collectivités territoriales et des opérateurs privés du projet devant le Comité de concertation « France Très Haut Débit ».

Le guide à destination des maires présenté par Bruno Le Maire et Jacqueline Gourault le 15 décembre 2020 présente notamment ce point en précisant un calendrier de mise en œuvre ambitieux et ouvrant l'appel à projet suite à la publication du cahier des charges. Des mesures sont donc mises en place pour tenter de résorber plus efficacement cette fracture numérique en France et rapprocher les populations.

(53) Terme issu du Rapport de la mission d'information sur la lutte contre l'illectronisme et pour l'inclusion numérique du 17 septembre 2020.

### B. – Les tiers-lieux et Fabriques de territoires[54]

Afin de lutter contre l'isolement et de dynamiser les territoires, les citoyens créent des tiers-lieux afin de rétablir des liens entre eux et « faire ensemble ». Plus que du *coworking*, ces tiers-lieux permettent un réel développement économique et une activation de ressources locales plus importante. Ces tiers-lieux peuvent prendre beaucoup de formes différentes telles que des garages solidaires, friches culturelles, campus connectés… Chaque lieu possède son propre fonctionnement, son propre financement et sa communauté. En septembre 2018 près de 1 800 lieux comme ceux-ci ont vu le jour. Y sont dispensées des formations pour apprendre, fabriquer et faire ensemble. Ces tiers-lieux, plus que des initiatives locales et indépendantes, s'organisent en Conseil national des tiers-lieux. Les représentants de tiers-lieux sont consultés par les pouvoirs publics afin de jouer un rôle d'instance de représentation et de dialogue de filières. De plus, le Conseil national des tiers-lieux examine les candidatures pour les Fabriques de territoire. Ce concept est financé par l'État, à hauteur de 45 millions d'euros afin d'en identifier trois cents d'ici 2022. L'État choisit d'accorder une attention particulière aux initiatives liées au numérique.

Les initiatives qui partent d'une organisation citoyenne sont largement encouragées par l'État afin que ce système se développe plus largement et que le numérique soit accessible à tous. Cette action, mise en commun avec le Pass Numérique, les « hubs France Connectée » et le programme « Europe Numérique », permet une mise en œuvre du tout numérique et une éducation de la population beaucoup plus efficace.

### C. – Label « Territoire, villes et villages Internet »

Les 29 et 30 janvier 2019 s'est tenue à La Défense à Paris la première édition du Congrès national des élus au numérique organisé par l'association « Villes Internet ». En 2019, c'est plus de deux cents collectivités territoriales qui ont reçu le label national « Territoires, villes et villages Internet » afin de sanctionner leur engagement pour le développement de services numériques locaux pour leurs citoyens. Julien Denormandie, ministre chargé de la ville et du logement, rappellera : « Le numérique est un droit pour tous ». Ce label, à l'instar de celui de Ville Fleurie, possède une graduation d'une à cinq arobases (@).

Ce label permet la reconnaissance des villes et villages mettant en œuvre une politique forte pour promouvoir l'Internet citoyen octroyant des services aux habitants, multipliant les accès Internet publics et mettant en place des démarches administratives en ligne. L'association « Villes Internet », à l'origine de ce label, comprend des élus locaux aux bords politiques différents, mais rassemblés pour l'Internet citoyen et le numérique urbain. Ce label est distribué depuis vingt ans à environ deux cents villes et villages tous les ans.

Encore une action afin d'inciter les collectivités à agir en faveur du déploiement du numérique, rendant ces territoires plus attractifs pour les jeunes populations à venir.

(54) Dossier de presse « Nouveaux Lieux, nouveaux liens », 17 juin 2019.

### D. – Le Forum numérique en commun et France Relance

Face à la pandémie heurtant de plein fouet notre pays, le recours au numérique n'a jamais été aussi important. Dans cette optique, et afin d'assurer sa mission coûte que coûte, le Forum numérique en commun (NEC) s'est réinventé pour la troisième édition par l'organisation de la journée du 17 novembre 2020 mettant en lumière les huit parcours en ligne sur les différents sujets.

Le but du NEC est la construction d'un numérique inclusif, éthique et durable, ce qui démontre bien la volonté d'accès pour tous, sans que cela se fasse au détriment de l'environnement. Les actions menées par ce forum permettent de former tant les collectivités territoriales que les citoyens au numérique, mais aussi de leur faire prendre conscience que chaque projet numérique a un impact écologique sur notre planète.

Lors de l'édition 2020 du Forum NEC, Jacqueline Gourault, ministre de la Cohésion des territoires et des Relations avec les collectivités territoriales a annoncé les principales mesures du plan de relance en faveur de l'inclusion numérique en association avec Cédric O, secrétaire d'État chargé de la transition numérique. 250 millions d'euros seront mobilisés pour rendre accessible le numérique dans le quotidien de tous les Français, avec trois actions principales : la mise en place de 4 000 conseillers numériques afin de développer des ateliers et formations directement sur le terrain pour une somme de 200 millions d'euros ; 40 millions d'euros seront consacrés à la conception et au déploiement de kits d'inclusion numériques pour les mairies, bibliothèques, tiers-lieux et associations caritatives. Les 10 millions restant seront mis à la disposition du service public numérique pour l'opération « Aidants Connect » et l'amélioration des compétences numériques des aidants.

Ce dispositif de financement par l'État est encore une fois solidement ficelé avec l'aval des collectivités territoriales dont l'action est essentielle à la bonne transition numérique.

## II. – Un indéniable mais timide recul de la fracture numérique en France

Face à la mise en place de tant de procédés et d'opérations, on pourrait croire que la fracture numérique territoriale n'est qu'un lointain souvenir et qu'elle a disparu. En réalité, ce n'est pas le cas. La lutte contre la fracture numérique territoriale est une bataille de chaque instant, de plus en plus de nouvelles technologies arrivant sur le marché. L'information des citoyens et des collectivités territoriales constitue une préoccupation continue. Afin de limiter cette fracture du côté technique, il faut bien évidemment rappeler l'accord du 14 janvier 2018 entre les quatre plus grands opérateurs mobiles (Free, Orange, Bouygues et SFR) afin que tous les territoires français puissent avoir un accès décent au réseau mobile.

En plus de cette difficulté liée à la multiplication des technologies et à l'augmentation exponentielle de l'utilisation du numérique, il faut se ranger du côté du Sénat qui dira dans son rapport d'information du 8 juin 2020 : « L'illectronisme ne disparaîtra pas d'un coup de tablette magique ! ». Ce propos résume bien son avis sur la

stratégie nationale pour un numérique inclusif qui est selon lui « sous-dimensionnée et sous-financée ». Ce propos est particulièrement vrai face à l'échec du Pass Numérique.

La fracture se résorbe néanmoins indéniablement. Bon nombre de personnes en zone blanche ont accès plus facilement aux soins de spécialistes qui bien souvent se trouvent géographiquement trop loin de leurs patients. La téléconsultation, rendue possible *via* Care ou Doctolib, apporte un support essentiel à des personnes qui, autrement, auraient pu se trouver en situation critique ou compliquée. En ces temps de confinement et de contacts directs limités, résorber cette fracture n'a jamais été aussi important, tant au niveau de la santé qu'au niveau social.

Un aspect négatif cependant : le numérique est de plus en plus utilisé et est recommandé, parfois exigé. Ceci crée dès lors la nécessité de production d'appareils et de technologies qui ont un impact direct sur l'écologie.

SECTION 3

## L'IMPACT DU NUMÉRIQUE SUR L'ENVIRONNEMENT

« Il faut choisir ses batailles. Ma priorité, en France, en Europe, à l'international, ce sont les émissions de $CO_2$ et le réchauffement climatique. » Le président français Emmanuel Macron évoque le sujet de l'environnement[(55)] ; et celui lié au numérique qui attise les débats, notamment auprès des personnes concernées.

Alan Mathison Turing, célèbre mathématicien anglais du XX^e^ siècle, fut le premier à systématiser les ordinateurs, aujourd'hui source de pollution numérique incontrôlable. Après la Seconde Guerre mondiale, l'invention du transistor par ATT, le laboratoire de DELL, a permis de faciliter la conception d'équipements informatiques modernes et pratiques (la miniaturisation). Les années 1970 contribuent à l'essor d'Internet et à la mise en place d'outils technologiques sophistiqués qui sont connus du grand public aujourd'hui[(56)].

Selon l'ADEME, les émissions de $CO_2$ de ce secteur sont dues pour moitié au fonctionnement d'Internet (le stockage des données, la maintenance de l'infrastructure du réseau) et pour moitié à la fabrication des équipements de communication (les ordinateurs, les smartphones, les tablettes). Toutefois, l'étude menée par GreenIT en octobre 2019[(57)] précise que les 34 milliards de smartphones, ordinateurs, téléviseurs utilisés sur la Terre ont un impact non négligeable sur l'environnement. Il est compté 2,5 tonnes de matières premières, ce qui représente 350 kilos de $CO_2$. En d'autres termes, avant même d'être mis en service, un téléviseur génère plus de $CO_2$ qu'un vol aller-retour Paris-Nice.

En conséquence, toutes les nouvelles technologies induisent une surconsommation de matières premières.

(55) Le dimanche 17 décembre 2017, Emmanuel Macron intervient au journal de 20 heures. Le chef de l'État exprime son engouement à défendre l'environnement et la capacité à y parvenir.
(56) *La pollution numérique est-elle connue et comprise de tous ?*, Les Mondes numériques, 14 févr. 2017.
(57) V. le rapport sur « L'empreinte environnementale du numérique mondial.

Au-delà de tout ça, les ministères de la Santé des États membres de la Région européenne de l'OMS[58] contribuent davantage à la numérisation. L'OMS et l'Union européenne viennent en aide aux vingt-sept États membres afin de surmonter les obstacles qui empêchent l'adoption des technologies numériques et favoriser le renforcement numérique des systèmes de santé. De cette façon les États vont pouvoir étudier les pistes permettant d'améliorer la numérisation en faveur de la santé publique. Les évolutions numériques ne cessent de s'immiscer dans le secteur de la santé, et modifient la relation entre le personnel médical et le patient. Ainsi, la loi portant sur l'organisation et la transformation du système de santé : « télésoin »[59] a été adaptée le 24 juillet 2019. Celle-ci organise la pratique de soins à distance utilisant les technologies de l'information et de la communication (C. santé publ., art. L. 6316-2). Les outils en constante progression endurent le fonctionnement des systèmes de santé et de protection sociale européenne représentant en moyenne 27,7 % du PIB, la prise en charge des patients sur la notion de parcours médical et de soins s'intègre dans le programme de « Vivre et vieillir en bonne santé » fixé par la Commission européenne.

Les professionnels de santé, mais également ceux du secteur médico-social exigent des équipements pour le développement de la télémédecine qui suscite une incidence majeure pour la planète.

Néanmoins, s'il est constaté que la pollution numérique émane principalement des nouvelles technologies (§ 1), les acteurs du numérique, que ce soit les patients ou les professionnels de santé, mènent une lutte afin de réduire l'empreinte digitale sur l'environnement (§ 2).

## § 1. – La pollution numérique : une incidence engendrée par les nouvelles technologies

Le cycle de vie d'un objet, depuis l'extraction des matières premières qui le constitue jusqu'à sa disparition en fin de vie, provoque une importante diffusion de carbone (I). Quant à lui, le réseau Internet, n'est pas qu'« immatériel », comptant de nombreux équipements informatiques mis à la disposition des professionnels de santé ainsi qu'auprès des industries de santé (II).

### I. – La fabrication des équipements numériques : un poids écologique considérable

La phase de recherche et de développement est indispensable à la création des outils informatiques (A), toutefois, leur mise en place peut être préjudiciable à l'environnement (B).

(58) OMS, Rapport, « *Systèmes de santé, santé et prospérité* », 2008.
(59) L. n° 2019-774, 24 juill. 2019, relative à l'organisation et à la transformation du système de santé.

### A. – De l'exigence à la prospérité numérique

L'ordinateur, le téléviseur, les montres connectées, en somme les équipements de télécommunication : ces appareils sont des objets d'instance et de présence. Ce sont des sources de consommation d'énergie et de ressources non renouvelables allant de leur production jusqu'à leur commercialisation.

Le cycle de vie d'un équipement sollicite énormément d'énergie, plus que celle qui est utilisée à sa fabrication et sa mise en vente sur le marché médical. La chaîne de production de ces équipements est basée sur les énergies fossiles : l'extraction des composants, la production des pièces ainsi que leur transport, l'ajustement du produit fini puis son transport vers le pays de distribution. Par exemple, le smartphone est composé de nombreux métaux du monde entier, notamment, du tantale congolais, du lithium bolivien, de l'or australien, des terres rares chinoises avant de pouvoir accéder à l'e-santé[60].

L'innovation est dans l'ADN de l'être humain ; en conséquence, le concept de « dématérialisation » incite l'exploitation de la matière première. La miniaturisation et la complexité d'extraction des éléments assemblant le produit (tantale, indium), ce surpoids conduit à des effets sur l'environnement. L'usage des outils adaptés aux professionnels de santé ou encore au patient comme le dossier médical partagé (DMP), les e-prescriptions et le développement de la télémédecine, est vecteur de gain de temps, mais a un impact à long terme pour la planète.

### B. – Le numérique chiffré : une situation inquiétante

La production d'appareils médicaux énergivores nécessite d'utiliser 50 à 350 fois leur poids en matière première. Par exemple, 800 kilos de matière première sont nécessaires à la fabrication d'un ordinateur portable de 2 kilos seulement. Ce qui paraît démesuré avec le produit final. Le processus de production est plus énergivore que la phase dans laquelle le produit est utilisé par les consommateurs. Les émissions de dioxyde de carbone sont également en hausse, car de nombreux composants sont élaborés dans les pays asiatiques, notamment la Chine où l'électricité est extraite à partir du charbon, et a donc un impact sérieux sur l'environnement[61]. Leur transport, généralement aérien ou maritime, s'ajoute également au bilan des impacts environnementaux.

Afin d'imposer une restriction à ces derniers, il est important d'éviter les remplacements réguliers d'objets, car la reconversion des constituants électroniques est difficile et coûteuse.

Les objets connectés propagent à eux seuls 39 %[62] des émissions de gaz à effet de serre dans le monde numérique, et consomment 76 % des ressources naturelles non renouvelables de la planète. 75 % de la population française possèdent un smartphone, mais seulement 6 % d'entre eux sont recyclés en France[63].

(60) N. de Grove-Valdeyron, *E-santé dans l'Union européenne : regards sur la télémédecine*, PU Toulouse 1 Capitole, 2020.
(61) ADEME, Rapport, *La face cachée du numérique*, janv. 2021.
(62) Business Insider France : « En 2025, les objets connectés pourraient représenter la majorité de la pollution numérique mondiale », 21 nov. 2019.
(63) V. ADEME, Rapport janv. 2021, préc.

La propension actuelle n'est pas rassurante. En 2025, il y aura 48 milliards d'objets connectés (les montres, les smartphones) sur la planète, ce qui aura une répercussion trois fois plus importante sur l'atmosphère qu'en 2010.

La m-santé ne connaît pas la crise et s'introduit dans le système de santé[64]. Ces services proposent un accès aisé à la santé par le biais d'un appareil connecté à un réseau. L'utilisation croissante se traduit principalement par des besoins dus au vieillissement de la population et à la forte augmentation des maladies chroniques.

En ce qui concerne la durée de vie de ces équipements, ce n'est pas mieux. Leur conception n'offre pas un recyclage exhaustif ; seulement 1 % de tantale est réutilisé. Ainsi, 75 % des déchets disparaissent des filières de recyclage européennes et sont illicitement exportés vers d'autres pays émergents, débouchant à la création d'immenses décharges.

Le numérique, c'est 4,2 % de l'énergie primaire consommée par l'humanité dont une bonne partie d'hydrocarbure et de charbon, 5,5 % de l'électricité produite dans le monde et 0,2 % de l'eau disponible. Ainsi, si le numérique était un pays, il aurait environ deux à trois fois l'empreinte environnementale de la France.

## II. – L'utilisation du réseau Internet : un coût énergétique majeur

Du clic au déclic, il n'y a qu'un seul geste à déployer pour l'usager (A). Cependant, cet acte est loin de rester confidentiel, l'enregistrement s'établit auprès des serveurs des *datacenters* (B).

### A. – Un petit clic pour l'Homme, mais une grande consommation pour l'Humanité

Les technologies numériques continueront d'être produites et utilisées, ce qui entraînera des coûts énergétiques impressionnants. Selon l'ADEME, le secteur informatique représente actuellement 4 % des émissions mondiales de gaz à effet de serre, et la hausse de la consommation laisse à penser que cette empreinte carbone va doubler d'ici 2025 (le nombre d'utilisateurs mondial, de trois milliards aujourd'hui, est estimé à plus de 4 milliards d'ici 2030).

Ces dernières années, l'Internet destiné au secteur médical s'est institué tel qu'un objet de recherche à part entière. Les recherches ciblées sur les bases de données bibliographiques produisent une quantité indénombrable de références mentionnant l'utilisation des technologies de l'information et de la communication (TIC), associées à la santé[65]. La « e-santé » renvoie à l'application des technologies de l'information et de la communication à l'ensemble des fonctionnalités qui impactent la santé des citoyens et des patients. Par ailleurs, la recherche d'informations en ligne instaure globalement une approche efficiente de l'utilisateur,

(64) L. n° 2016-41, 26 janv. 2016, de modernisation de notre système de santé.

(65) J. Kivits, C. Lavielle et C. Thoër, *Internet et santé publique : comprendre les pratiques, partager les expériences, discuter les enjeux : Santé Publique* 2009/hs2, vol. 21, p. 5 à 12.

qui a pour effet de le réconforter dans ses attentes. De ce sens, les interventions et les consultations par l'intermédiaire d'Internet sont interprétées sous diverses perspectives, notamment, les programmes de prévention, la sensibilisation aux risques de santé, mais aussi les dispositifs d'accompagnement pour les personnes atteintes d'une maladie grave.

Cela étant, la diffusion de $CO_2$ augmente avec l'utilisation conséquente de combustibles de type fossile (gaz naturel et charbon), par déduction d'équipements électriques dans l'objectif d'agrémenter les centres de données.

### B. – Les *datacenters* : un stockage illimité de données personnelles

En France, 10 % de la production d'électricité est consommée seulement par les centres de données numériques ou *datacenters* régis par le RGPD[66], encadrant le droit à la protection des données à caractère personnel. Ainsi, sont appréciées telles que des données de santé « l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mental passé, présent ou futur de la personne concernée[67] ». Les renseignements sont ordonnés aux dépens de la santé du patient (handicap, maladie). En effet, le texte européen précise l'origine de ces données, c'est-à-dire un professionnel de santé, un patient, une industrie de santé ou bien encore un dispositif médical.

À la différence des données de santé, les données de bien-être peuvent dévoiler les caractères constitutifs de la situation médicale d'un patient, catégorisés comme des données sensibles.

Cependant, les systèmes d'information hospitaliers (SIH) réglementés par la circulaire du 6 janvier 1989[68], sont considérés comme une mine d'or. Les établissements de santé stockent de grandes quantités de données qui représentent une richesse d'éléments, notamment des données cliniques et des données médicales en tout genre. La surveillance des patients à domicile, par l'intermédiaire de l'Hôpital à domicile (HAD), permettra de recueillir de nouvelles données collectées *via* les objets connectés. Ces technologies modernes, comme les smartphones, les senseurs GPS permettent de mesurer l'activité des patients. Ces sources d'informations sont manipulables.

Depuis, la loi Moore datée de 1985, les nouvelles technologies permettent de traiter une énorme quantité d'informations dans un bref délai. Les *big data* favorisent le stockage de ces données qui s'incorpore au sein de plusieurs domaines tels que les statistiques, les bases de données ainsi que les technologies. L'activité en cours permet la captation et l'exploitation de données numériques rapidement. Le secteur de la santé est devenu inimaginable sans l'usage permanent de nouveaux équipements : la e-santé, les nanotechnologies, les sciences cognitives ou

(66) PE et Cons. UE, règl. (UE) n° 2016/679, 27 avr. 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 dit règlement général sur la protection des données.
(67) RGPD, art. 35.
(68) Circ. min. Santé n° 275, 6 janv. 1989.

bien encore les biotechnologies. Ces outils nuisibles pour la Terre sont néanmoins vitaux à l'industrie médicale.

À l'avenir, Internet pourrait être la principale source de pollution au monde. L'électricité est la source d'énergie primordiale d'Internet, mais également sa faiblesse. Afin de procéder à une amélioration en faveur d'un Internet plus respectueux de la planète, il est indispensable de s'engager vers quelques comportements propres.

## § 2. – La réduction de l'empreinte environnementale du numérique

De nouveaux acteurs, puissants, les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) prennent en considération l'empreinte carbone, et leurs efforts pour diminuer la pollution numérique sont basés sur les attentes des individus (I). Cependant, pour devenir une personne responsable de ses actes, plusieurs écogestes sont préconisés (II).

### I. – L'initiative des géants du numérique : vers un monde digital éco-responsable

Les protagonistes d'Internet sont soucieux de l'environnement (A), avec la mise en avant de consignes citoyennes adaptées au secteur médical (B).

#### A. – L'insistance des GAFAM au vert

Les GAFAM poursuivent leur percée dans la santé sous des aspects divers et partagés.

Google est une ressource primordiale en matière de santé.

Google Life Science, développé par Google, s'intéresse aux plateformes et aux algorithmes conçus pour identifier les causes et les facteurs d'une maladie, ainsi déterminer les meilleures méthodes de diagnostic pour un traitement des plus juste. Dans le cadre de ce mouvement, Google est affilié à de nombreux groupes pharmaceutiques impliqués dans des projets de biotechnologie et de santé, notamment les lentilles connectées avec Novartis pour le traitement du diabète.

Par ailleurs, Google lutte contre la désinformation en santé, particulièrement en période de pandémie. La mise au point d'un système de traçage basé sur la technologie Bluetooth permet d'identifier l'auteur d'une *fake news*.

Les publications partagées à travers Google sont apparentes à tout instant et un grand nombre de serveurs Internet doivent être réunis. Ils sont également installés dans des *datacenters*, où la nécessité d'un refroidissement constant constitue une fracture environnementale.

Apple a fait de nombreuses améliorations. Désormais, les utilisateurs pourront partager leurs données de santé et d'activités avec des chercheurs et des applications tierces grâce aux fonctionnalités *Research Kit* et *Health Kit*. Elle a développé

une application sur l'iPhone qui permet à chacun de suivre son activité physique, de recueillir et stocker des données sans aucune information sur la destination de ces données.

Microsoft est lui aussi actif dans le milieu médical, se rapprochant spécialement des professionnels de santé, des établissements de santé, des industries de santé et des patients. À travers son projet, *Healthcare NExT*, il coopère à la transformation des systèmes de soins et noue des accords partenariaux pour « co-produire des équipements de santé à partir des services technologiques dans le domaine de l'intelligence artificielle »[(69)].

Promoteur des technologies informatiques, Microsoft a choisi de rejoindre également Greentech. Il a énoncé que l'entreprise serait neutre en carbone durant dix ans. Mais l'entreprise n'envisage pas de s'arrêter là, et à l'horizon 2050, elle s'est fixé un objectif encore plus audacieux : réaliser une empreinte carbone négative ! En outre, Microsoft analysera l'ensemble des émissions de $CO_2$ antérieures dont elle est responsable.

Amazon, s'est basée sur les produits d'hygiène et de santé, ce qui a suscité d'énormes réactions sur la question de la qualification des produits de santé.

Ces entreprises s'efforcent de multiplier les actions écologiques tout en poursuivant leurs innovations technologiques utiles à la médecine.

### B. – La sobriété sur Internet

Il est envisageable d'aller de l'avant en consentant à un certain « civisme numérique », c'est-à-dire une sobriété numérique provenant de l'attitude des usagers d'Internet.

La sobriété numérique est une conception qui engage une personne à adopter un comportement recommandé face au monde numérique. Tandis que la notion de « civisme numérique » invite à faire du numérique un usage modéré. Peu à peu, la sobriété numérique entre dans les pensées des citoyens s'intéressant à l'écologie[(70)].

Désormais un individu peut prendre connaissance de son empreinte carbone diffusée sur les plateformes fictives. Ainsi, des structures telles que *The Shift Project* (laboratoire d'idées dont l'objectif est de réduire les impacts environnementaux) ont installé Carbonalyser (extension web qui comptabilise les émissions de $CO_2$ sur Internet). Le 1er janvier 2022, les opérateurs Internet informeront leurs consommateurs de l'ampleur de la pollution occasionnée par le temps passé sur les réseaux. Ces informations seront immédiatement facturées[(71)].

Vis-à-vis de l'usager, des démarches sont simples à mettre en œuvre sans forcément bousculer son quotidien.

(69) R. Moreaux, *Microsoft à l'offensive pour « démocratiser » l'usage de ses technologies en santé*, TIC Pharma, 10 mars 2017.
(70) The Shift Project, Rapport, *La sobriété numérique*, 14 oct. 2020.
(71) Novethic, *Orange, Free, SFR… Les opérateurs devront bientôt indiquer le bilan carbone de nos activités numériques*,13 mars 2020.

## II. – La lutte contre la pollution digitale : les éco-gestes recommandés

Vivre l'informatique au jour le jour n'est guère fastidieux. Des mesures simples et pratiques (A) rendent la reconversion numérique meilleure (B). Tout en tenant compte de l'aspect technologique face aux risques sanitaires (C).

### A. – L'adoption d'actes intelligibles pour la naissance d'un individu responsable

Depuis le début de l'épidémie de Covid-19, et particulièrement en période de confinement, l'usage d'Internet n'a fait qu'accroître. Son utilisation ininterrompue représente une pollution numérique qui n'est vraiment pas anodine.

L'information sanitaire sur Internet présente également des problèmes innés. L'information médicale sur Internet est difficile à encadrer, qui se traduit par sa complexité de contrôle et de qualité, et l'intérêt des patients varie considérablement en ce qui concerne ces informations. De mauvaises données médicales peuvent entraîner de graves dommages. Les patients peuvent se laisser porter par des informations erronées ou prendre des décisions importantes qui nuiront à leur santé actuelle. Internet permet l'ouverture de plateformes qui consistent à promouvoir une approche de la santé non scientifique. Les patients sont régulièrement dans une position délicate et beaucoup sont prêts à consentir toute information qui provoquera un réconfort[72].

Ainsi, les envies se multiplient de cliquer sur tel ou tel renseignement médical rencontré, mais il est fondamental de s'interroger sur le besoin. Si ce dernier est pressant, le téléchargement de la lecture vidéo est recommandé. Mais attention, la 4G sur nos smartphones émet vingt-trois fois plus d'énergie que le WiFi. Dès lors, l'activation du WiFi sur le smartphone est préférable.

Selon la circulaire concernant le recours au *cloud*[73], il est impératif de stocker uniquement les éléments essentiels et de désactiver la synchronisation avec le smartphone ou bien avec la montre connectée. Contrairement aux apparences, les données ne sont pas stockées dans le « nuage », mais bel et bien dans des *datacenters* énergivores. La pollution numérique peut-être limitée grâce au rejet des « objets connectés ». L'acquisition d'objets dernier cri est-elle primordiale ? Ces articles ont une valeur environnementale élevée, mais pas seulement, ils posent également un risque énorme sur notre vie privée.

Malgré la difficulté de ces pratiques qui ne sont pas encore familières, il faut avancer de manière optimiste avec la préconisation du recyclage.

(72) A. Winterbottom, H.L. Bekker, M. Conner et A. Mooney, *Does narrative information bias individual's decision making? A systematic review : Soc Sci Med.* 2008 ;67(12) :2079-88, Cyberpub, 24 oct. 2008.

(73) Circ. 8 nov. 2018, relative à la doctrine d'utilisation de l'informatique en nuage par l'État français (Légifrance).

### B. – Le système de recyclage : un service au profit des nouvelles technologies

Les producteurs de terminaux informatiques (ordinateurs, smartphones ou tablettes) se basent sur le caractère désuet de leurs produits et incitent à en acheter de nouveaux. Les astuces sont connues du large public notamment : la fragilité des produits, le coût de réparation excessif, le manque des pièces de rechange.

Des structures à but non lucratif telles que « Halte à l'Obsolescence Programmée » (HOP), créée en 2015 à la suite de l'instauration du délit d'obsolescence programmée dans le Code de la consommation, astreignent les entreprises du secteur à promouvoir ces meilleures pratiques. À titre d'exemple, l'ordinateur à l'hôpital composé de 40 % de plastique pourra être recyclé dans l'industrie automobile.

Toutefois, selon les dernières estimations en ligne, avec la croissance des réseaux et services des technologies de l'information et de la communication (TIC), environ 53,6 millions de tonnes de DEEE sont produites chaque année dans le monde entier, dont 17,4 % seulement sont collectées et recyclées(74). Les DEEE sont les déchets d'équipements électriques et électroniques, en référence aux appareils ménagers ou professionnels mis à la voirie qui comprennent des composants ou des circuits électriques et fonctionnent sur batterie ou une source électrique. Les déchets médicaux quant à eux sont soumis à un traitement spécifique. La collecte des déchets médicaux dangereux ou non dangereux est établie par des spécialistes du recyclage. Ensuite, les déchets sont transmis dans des centres de traitements agréés pour être valorisés(75).

La préservation de notre écosystème se perfectionne ; pour autant, un recul numérique s'impose et les nouvelles technologies peuvent créer une amélioration importante du corps humain.

### C. – Les bienfaits des écrans sur l'organisme

Les pratiques des professionnels de santé sont en évolution permanente ; de ce fait, les nouveaux usages numériques des individus se multiplient. Le rapport de 2015 sur la « santé connectée » du Conseil national de l'Ordre des médecins (CNOM)(76) illustre le bon usage de la santé mobile et numérique au service de la relation patients-médecins. Les dispositifs de m-santé, conditionnés par une fiabilité, peuvent contribuer à améliorer le respect des protocoles de prévention, de santé et de soins, et à favoriser la relation entre le médecin et le patient.

En télémédecine, les attentes en matière de m-santé se discutent principalement en cas de télésurveillance médicale (C. santé publ., art. R. 6316-1), en raison du potentiel des technologies à faciliter le suivi des paramètres cliniques et la transmission d'alertes. De plus, la télé-expertise permet à « un professionnel médical de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux par

(74) Ministère de la Transition Écologique, *Les déchets d'équipements électriques et électroniques*, 31 janv. 2020.
(75) Compagnie de gestion de traitement des déchets industriels, *Le cadre réglementaire des déchets médicaux*, 4 juill. 2016.
(76) CNOM, *La santé connectée*, 3 févr. 2015.

l'intermédiaire des technologies de l'information et de la communication »[77]. Ce qui permet aux professionnels de santé d'être impliqués et de collaborer sur un même dossier efficacement.

En plus, l'utilisation intense des outils informatiques peut avoir des conséquences néfastes sur la santé physique et morale telles que : l'anxiété, les problèmes de concentration, la fatigue oculaire, le cyber-harcèlement, la perte d'appétit. Internet est pourtant loin de rendre ignorants ses consommateurs. « Au contraire, cet outil peut développer notre intelligence si nous réussissons à garder le cap, à échapper aux pièges des interférences (images chocs qui attirent l'œil, phrases qui clignotent…), de manière à poursuivre notre recherche sur le web sans laisser fléchir notre attention », déclare Jean-Philippe Lachaux, chercheur en neurosciences cognitives et directeur de recherche au Centre national de la recherche scientifique (CNRS).

Le contrôle des équipements informatiques ne regarde que l'usager, l'entrée dans un labyrinthe sans issue peut paraître attractive au premier abord, mais il ne faut pas se laisser tenter par le chant des sirènes.

## CONCLUSION

Depuis les années 1970, les questions relatives au numérique et à l'environnement ont connu un essor exponentiel. La volonté de créer un territoire numérique respectueux de l'environnement est le fil rouge des législations modernes et un des plus grands défis du siècle.

Les termes modernes de « fracture » ou « disruption » renvoient pour l'un aux inégalités d'accès à la technologie informatique et pour l'autre à l'innovation numérique en rupture avec nos systèmes classiques (dont un des exemples les plus connus est l'« ubérisation »). Ces termes employés dans le champ du numérique démontrent que ce domaine constitue un défi d'adaptation. La question numérique s'intègre dans une dynamique globale avec une volonté de créer une société numérique innovante et unifiée – ou tout du moins harmonisée – et participant de la sauvegarde de l'environnement, plus particulièrement de l'être humain et sa santé.

Mais à tous niveaux, les alertes sont lancées sur les impacts du numérique sur l'environnement. Ces alertes questionnent sur l'opposition de ce nouvel environnement à celui d'un environnement sain déjà consacré comme droit fondamental, sur les atteintes irréversibles portées à celui-ci, sur la protection à mettre en place pour assurer la pérennité et la santé de l'espèce humaine.

L'environnement, la santé et le numérique sont à la croisée des chemins. Il est essentiel que les décisions d'aujourd'hui assurent à tous un avenir dans un monde sain. Mais, le chemin à prendre est encore très incertain ; entre avancées technologiques posant des questions éthiques de transhumanisme et freins à cette même

(77) Ministère des Solidarités et de la Santé, *La télémédecine*, 14 sept. 2018.

technologie pour des considérations environnementales, les décisions sont compliquées à prendre, parfois à comprendre et d'autant plus à mettre en œuvre.

Le droit (du) numérique n'a pas encore été consacré. L'environnement et la santé, accompagnés du principe de précaution, seront-t-ils des alliés de la révolution numérique ou un mur dressé sur son chemin ? Quels seront autrement les moyens évoqués ?

Ce chapitre a fait le choix de traiter de multiples aspects de la thématique numérique et environnement. Juridique et économique, découvrant les origines législatives de la protection environnementale et envisageant les potentielles issues des débats européens plus actuels. Politique, montrant la volonté de la République française de mettre en place des territoires numériques, bénéficiant à tous par le biais de mesures incitatives et inclusives. Écologique enfin, révélant l'aspect le plus négatif de cette double révolution à travers des données qui alertent sur l'ampleur et la gravité de l'impact numérico-environnemental et faisant émerger de nouveaux moyens permettant d'y remédier, avant que ne soit potentiellement atteint le point de non-retour.

CHAPITRE 12

# INTELLIGENCE ARTIFICIELLE ET FISCALITÉ DES INDUSTRIES DE SANTÉ

Alban LAMBOUROUD

## INTRODUCTION

La philosophie des grands nombres qu'induit l'intelligence artificielle trouverait un terrain bien fertile en cette matière, par essence faite à la fois de lettres et de chiffres, qu'est la fiscalité. Les deux font la paire, d'où peut-être l'intérêt des propos généraux qui suivent, propos dont il convient dès ici de noter la relativité (dans le temps notamment) tant la matière est évolutive, ce qui est avancé un jour pouvant se trouver obsolète le lendemain. Il n'en reste pas moins que les points abordés ci-dessous devraient eux avoir quelque pérennité quant à leur existence de principe.

Aucun pan de nos vies, professionnelle comme privée, n'échappe donc au développement de l'intelligence artificielle. La fiscalité ne fait assurément pas exception. Et moins encore la comptabilité, terreau de la première. Pas de fiscalité sans comptabilité, les règles du Code général des impôts (CGI) renvoyant à elle ce qui doit être révisé du résultat déterminé d'abord par celles du Plan comptable général. Comme partout ailleurs, ce développement suscite tout à la fois enthousiasme et crainte. Enthousiasme parce que la comptabilité et la fiscalité, comme toute fonction support, accompagnent ce que de progrès l'intelligence artificielle apporte aux réponses médicales à la maladie, volet prévention inclus. Crainte, parce que la fiscalité n'échappe pas aux doutes et aux critiques que suscite l'intelligence artificielle. Mais, au-delà de ces considérations qui ont davantage trait aux ressources humaines pour certaines, à l'humanité tout court pour d'autres, force est de constater que l'intelligence artificielle participe d'une révolution qui ne saurait laisser la fiscalité de côté, ne serait-ce que parce que celle-ci conditionne la viabilité de l'État en lui fournissant les moyens financiers de son existence.

L'auteur, qui par tempérament regarderait d'un œil méfiant tout ce qui participe de la négation de l'identité singulière, et plus encore cette certitude attendue des grands nombres (de données), compterait d'abord parmi les sceptiques. Un sceptique silencieux, laissant aux experts le soin de faire avancer le débat, lesdits experts en la matière eux-mêmes se chamaillant quant à la signification du « A » de « IA ». Artificielle ou Augmentée ? La nuance est de taille. Pour la suite, l'auteur ne sachant ici prendre parti, faute des compétences techniques nécessaires, l'acronyme « IA » sera utilisé, ne serait-ce que pour économiser quelques feuilles de papier.

Le développement de l'IA étant tel, au point de permettre la reconnaissance de cette identité singulière, les progrès thérapeutiques manifestes étant liés, l'auteur se trouverait enclin à basculer, si ce n'est parmi les enthousiastes, au moins parmi celles et ceux qui nourrissent quelque *ouverture* vis-à-vis de ce cette évolution parce que confiant(e)s non seulement en la fiabilité des garde-fous mis en place mais aussi en la possibilité de toujours pouvoir se différencier de l'algorithme et ainsi apporter cette valeur ajoutée émotionnelle que seul l'être humain « nu » sait créer. En attendant de basculer, ou pas, un certain nombre de considérations techniques s'impose. En la matière, les spécificités du monde de la santé n'existent que parce que l'IA la compte parmi ses terrains privilégiés d'exploration. Les généralités qui suivent, parce que face à cet univers encore bien inconnu il serait bien aventureux de trop s'avancer, n'en tenteront pas moins de rester aussi proches que possible de ce qui concerne particulièrement les industries de santé. Des généralités et des pistes plutôt que des développements dignes de travaux de recherche dont ce n'est pas le métier de l'auteur.

L'exercice consistant à rester dans le périmètre des industries de santé sera d'abord facilité par un constat : l'IA participe de la création de droits de propriété (et de possession) industrielle connus qui assoient l'activité du secteur (Section 1, § 1). Par la suite, les nouvelles questions fiscales à la grande acuité qu'elle suscite vont bien au-delà du secteur (Section 1, § 2). L'exercice demeurera impossible s'agissant de l'impact de l'IA sur l'organisation comptable et fiscale des industriels de la santé (Section 2, § 2) comme celle de l'administration fiscale chargée de vérifier que chaque contribuable paie sa juste part d'impôt (Section 2, § 1), ces deux points concernant aussi l'économie dans son ensemble.

Le plan de ces très brefs propos généraux étant posé, force est de constater que la période que nous vivons – à l'heure où ces lignes sont écrites il est trop tôt pour employer le passé – celle de la Covid-19, aura constitué un accélérateur de la pénétration de l'IA, chacun l'aura entendu et constaté.

Brefs et très généraux, les propos qui suivent, au-delà de conférer quelque vernis fiscal au lecteur dont la fiscalité n'est pas le pain quotidien, ont pour objet de donner un aperçu de la confiture plus ou moins aigre-douce tartinée sur son pain.

SECTION 1

# L'INTELLIGENCE ARTIFICIELLE, UNE NOUVELLE SOURCE CRÉATRICE DE VALEUR

Les applications de l'IA dans le domaine de la santé sont légion. Il est possible néanmoins de les regrouper en six principaux groupes[1] : la médecine prédictive, qui s'intéresse à la prédiction d'une maladie et/ou de son évolution ; la médecine de précision, qui permet la recommandation de traitements personnalisés pour chaque patient ; l'aide à la décision diagnostique et thérapeutique ; la prévention en population générale (anticipation d'une épidémie, pharmacovigilance) ; les assistants virtuels et les robots compagnons ; la chirurgie assistée par ordinateurs.

À chacun de ces groupes, l'IA apporte un plus qui accroît d'autant les valeurs thérapeutiques et économiques de ce dont il s'agit.

Nombreux s'accordent à considérer qu'à une IA correspond un algorithme, lui-même appliqué à des données organisées en réseaux plus ou moins complexes.

Un algorithme se définit, selon l'arrêté du 27 juin 1989 relatif à l'enrichissement du vocabulaire de l'informatique[2], comme étant « l'étude de la résolution de problèmes par la mise en œuvre de suites d'opérations élémentaires selon un processus défini aboutissant à une solution ». L'algorithme devrait donc correspondre à un principe mathématique, en conséquence de quoi, jusqu'à preuve du contraire, un algorithme fait partie d'un domaine non protégé en tant que tel par quelque droit de propriété intellectuelle que ce soit.

Ceci dit, il se peut tout à fait que l'IA soit incluse dans un droit lui en revanche protégé, brevet ou logiciel, l'IA étant insusceptible elle-même d'en être un. Alors accessoire d'un principal, l'IA mériterait d'être traitée comme ce dernier.

Sa création résulte d'un processus de recherche et développement, avec toutes les incidences comptables et fiscales qui s'y attachent, éprouvées, qu'elle soit individualisée ou annexée à quelque autre droit (§ 1). En revanche, dans le sillage des difficultés rencontrées pour taxer l'économie dite « numérique », l'appréhension de nouvelles aires de taxation, telle celle avant tout des données, voire à l'extrême celle des robots, pose bien des questions (§ 2).

## § 1. – L'IA, partie prenante à la création de droits connus

### I. – L'IA, outil de projets de recherche et développement

L'IA a un coût. Celui de ces développeurs, analystes, et de tout ce qui gravite autour. Celui de tous les moyens techniques et humains nécessaires à son éclosion.

(1) Article communication interne Janssen-Cilag SAS, groupe J&J, dont sa présidente, Emmanuelle Quilès, est par ailleurs présidente du programme « Intelligence artificielle (IA) et santé » du Comité stratégique de filière (CSF) des industries et technologies de santé (dépêche APM, 18 nov. 2019).

(2) *JO* n° 216, 16 sept. 1989.

Ces coûts sont amenés à suivre le même traitement que les frais de recherche et développement auxquels ils sont agglomérés.

### A. – Traitement fiscal des frais de R&D exposés

En la matière, la comptabilité tient la fiscalité en l'état : l'option comptable détermine l'option fiscale. Il faut cependant dissocier, ici ce qui a trait à la recherche, là ce qui a trait au développement. Point d'option pour la première, les frais de recherche sont des charges insusceptibles d'activation, fiscalement déductibles puisque participant de l'exploitation de l'entreprise qui met au point cette IA dans le cadre de son projet.

En revanche, l'alternative est la suivante pour les frais de développement : charges ou immobilisations, avec l'impact sur la trésorerie des entreprises qui s'y attachent[3].

Aux termes des normes françaises, un actif est un élément identifiable du patrimoine ayant une valeur économique positive, c'est-à-dire un élément générant une ressource que l'entité contrôle du fait d'événements passés dont elle attend des avantages économiques futurs (PCG, art. 211-1). Son immobilisation répond aux deux critères cumulatifs suivants :

1) il est probable que l'entité bénéficiera des avantages économiques futurs correspondants ;

2) son coût ou sa valeur peut être évalué avec une fiabilité suffisante.

Il est communément admis qu'il est bien aventureux, et donc peu prudent, de considérer que des frais de développement constituent un actif. Généralement la voie de la charge comptable s'impose, comme son corollaire fiscal visé à l'article 236-I du Code général des impôts[4] (déduction immédiate).

### B. – Traitement comptable et fiscal des fruits de R&D acquis

Il se peut aussi que l'entreprise fasse elle-même l'acquisition des conclusions de projets menés par d'autres, abritant ou à viser d'IA. Dans cette hypothèse, la dépense engagée ne constituera pas une charge mais devra conduire à la constatation d'un actif à son bilan, dont les modalités de dépréciation posent question.

S'agissant d'IA, la proposition consisterait à ne pas la traiter en tant que telle, à défaut d'être caractérisée par un droit de propriété spécifique, mais, accessoire d'un droit principal lui reconnu, de l'inclure dans le traitement de ce dernier.

Plusieurs hypothèses s'offrent alors, parmi lesquelles :

– si l'IA est incluse dans un logiciel acquis, alors elle pourra fiscalement faire l'objet d'un amortissement sur une durée de douze mois ;

– si elle l'est dans un brevet, c'est sur une durée de cinq ans au plus qu'elle se trouvera amortie ;

– si elle l'est dans les droits de possession industrielle que sont par exemple les dossiers d'autorisation de mise sur le marché, c'est d'une durée plafond de dix ans au plus dont il s'agira[5].

(3) Qui dit « charges » dit réduction immédiate du résultat imposable dont il s'agit, avec la baisse d'impôt dû qui va avec.

(4) BOI-BIC-CHG-20-30-30, n° 1, 1er mars 2017.

(5) V. FM Litec, Fasc. 48-10, n° 17.

### II. – L'IA utilisée en aval de projets de recherche et développement

Passée la phase de recherche et développement, et venu le temps de l'exploitation, il n'est vraiment que l'hypothèse de concession et de cession de l'IA qui pose question, lorsque celle-ci est incluse dans un logiciel ou un brevet objet de l'opération. Pour le reste, à savoir l'exploitation proprement dite, produits comme charges liés ne sont l'objet d'aucun traitement exceptionnel du droit commun.

S'agissant en revanche de concession et cession, qui peuvent être jointes au vu des dispositions de l'article 238 du Code général des impôts(6), une option existe pour exclure leurs produits respectifs, redevances et plus-values, d'une taxation au taux de droit commun de l'impôt sur le résultat et leur ouvrir le bénéfice d'un régime de taxation plus favorable.

La mesure vise donc tout à la fois les concessions et les cessions, soit de logiciels soit de brevets.

La concession peut indistinctement être exclusive ou non (exception faite du cas de sous-concession). Elle peut être conclue pour l'ensemble des territoires pour lesquels l'invention bénéficie d'une protection juridique ou pour une partie seulement de ceux-ci. Elle peut porter sur la totalité des droits ou sur certains éléments seulement (par ex., la concession peut ne concerner que certaines revendications d'un brevet, y incluse l'IA y attachée). Sans préjudice de certaines considérations comptables et fiscales susceptibles d'interférer, un contrat de sous-concession est juridiquement un contrat de concession.

S'ils n'ont pas été créés mais acquis par l'entreprise, les droits considérés doivent l'être à titre onéreux depuis au moins deux ans. Dans le cas où l'entreprise les aurait elle-même créés, et ce même en faisant appel à des sous-traitants, et en outre sans forcément les avoir immobilisés, ce délai de deux ans ne se trouve plus opposable et alors la mesure peut s'appliquer sur-le-champ.

L'objet de la mesure est d'imposer le résultat net du produit de concession ou de cession au taux réduit d'impôt sur les sociétés, à savoir 10 %, outre éventuelle contribution additionnelle (CGI, art. 219, I, *a*).

## § 2. – La participation de l'IA à la découverte d'une *terra fisca incognita*

L'IA, et plus largement l'économie du numérique, souffre pour les États de ne pouvoir être appréhendée fiscalement compte tenu de ce que les progrès technologiques ont pris une avance évidente sur les textes fiscaux. En France comme ailleurs. Ce n'est pas tant la taxation de l'immatériel qui pose problème, celle-ci est déjà effective, c'est tout à la fois ce que de disruptif abrite l'organisation des entreprises du numérique, les outils et ce sur quoi elles assoient leur activité.

(6) BOI-BIC-BASE-110, 22 avr. 2020.

La souffrance a été criante lors de la crise financière de 2008. Exsangues, les budgets étatiques ont fait le constat de ce que toute une économie passait entre les mailles des filets fiscaux[7]. L'économie numérique. Le contentieux « Google » en France en a été l'expression la plus criante, les stipulations actuelles de la convention fiscale franco-irlandaise ne permettant pas la qualification en France d'une entité française en établissement stable d'une entité irlandaise, faute pour la première de pouvoir juridiquement engager la seconde[8].

Autant des progrès sont en cours sous l'égide de l'OCDE (I), autant bien des questions sont pendantes quant à la taxation de l'or gris que sont les données (II). La taxation des robots demeure quant à elle du ressort de la science-fiction, quoique (III).

## I. – La taxation de l'économie numérique

La matière des prix de transfert est actuellement en pleine mutation. Un prix de transfert est un prix auquel une entreprise transfère des biens ou rend des services à une entreprise associée (*i.e.* du même groupe). Ils supposent deux entreprises liées établies dans deux États distincts, et donc le transfert de masse imposable d'une souveraineté à une autre, d'un État à un autre.

Peu ou prou sous l'égide du G20, l'OCDE a lancé en juillet 2013 un plan d'action concernant l'érosion de la base d'imposition et le transfert de bénéfices (BEPS)[9], qui recense quinze actions spécifiques à engager afin de doter les pouvoirs publics des instruments nationaux et internationaux permettant de relever ce défi. Cet ensemble de mesures, révélé en octobre 2015[10], a pour objet de faire en sorte que le lieu d'imposition d'un revenu corresponde autant que faire se peut au lieu d'effectivité des activités économiques générant ledit revenu.

Dans cette tâche, une seule de ces quinze actions à date reste à élaborer tant elle est complexe, justement celle qui a trait à la taxation de l'économie numérique dont l'IA compte parmi les principaux moteurs (Action #1).

Un Groupe de réflexion sur l'économie numérique, organe subsidiaire du Comité des affaires fiscales (CAF) de l'OCDE auquel des pays du G20 non membres de l'OCDE participent en qualité d'associés, avait pourtant été créé pour ce faire en septembre 2013 et chargé de rédiger pour septembre 2014 un rapport permettant de recenser les problèmes fiscaux soulevés par l'économie numérique et de proposer des solutions détaillées permettant de les résoudre.

(7) Extrait du rapport BEPS OCDE : « Dans le monde entier, les dirigeants, les médias et la société civile expriment une préoccupation croissante vis-à-vis des pratiques d'optimisation fiscale des entreprises multinationales, qui exploitent les failles provoquées par l'interaction entre les différents systèmes fiscaux pour réduire artificiellement leur bénéfice imposable ou pour transférer des bénéfices vers des pays à faible fiscalité dans lesquels leur activité économique est très modeste, voire inexistante. Pour répondre à cette préoccupation, et à la demande du G20, l'Organisation de coopération et de développement économiques (OCDE) a publié en juillet 2013 un Plan d'action sur l'érosion de la base d'imposition et le transfert de bénéfices (le Plan d'action, OCDE, 2013). L'action 1 du Plan d'action sur l'érosion de la base d'imposition et le transfert de bénéfices appelle à engager des travaux pour relever les défis fiscaux posés par l'économie numérique ».

(8) CAA Paris, 25 avr. 2019, n° 17PA03069, *Min. c/ Sté Google Ireland Ltd.*

(9) OCDE, *Les actions du projet BEPS, L'érosion de la base d'imposition et le transfert de bénéfices*, juill 2013 (www.oecd.org/fr/fiscalite/beps/actions-beps.htm).

(10) OCDE, *BEPS : Rapports finaux 2015, Réformer les règles fiscales internationales pour endiguer l'évasion fiscale des entreprises multinationales* (www.oecd.org/fr/fiscalite/beps-rapports-finaux-2015.htm).

Son constat est clair. L'économie numérique s'assimilant de plus en plus à l'économie proprement dite, il serait difficile, pour ne pas dire impossible, de la distinguer du reste de l'économie dans une optique fiscale.

Devant ce constat principal et certains diagnostics comme celui qu'ont éprouvé les autorités françaises dans l'affaire « Google » quant à la définition contemporaine de l'établissement stable, le groupe de l'OCDE a dû prendre acte de ce que cette économie soulevait également des défis fiscaux plus larges pour les responsables de la politique fiscale, problèmes ayant trait en particulier aux questions de lien, de données et de caractérisation des bénéfices dans le cadre de la fiscalité directe qui, souvent, se chevauchent. L'économie numérique soulève également des défis quant à la collecte de la taxe sur la valeur ajoutée (TVA), notamment lorsque les biens, les services et les biens incorporels sont acquis par des particuliers auprès de fournisseurs installés à l'étranger.

En conséquence de quoi, quand chacune des autres actions BEPS se trouvait dévoilée et déclinée dans bien des législations internes, l'action #1 du programme BEPS propre à l'économie numérique reste à date à inventer. De nouveaux travaux ont été élaborés, de nouvelles propositions faites. Tous et toutes ont pour caractéristique d'inclure l'économie dite « réelle », ou la « vieille » économie, dans le traitement fiscal de l'économie numérique, parce qu'il est dorénavant évident qu'aucune frontière n'existe vraiment avec l'économie du numérique. Les GAFAM et consorts nourrissent déjà nombre de projets industriels, quand l'industrie fait du numérique et de l'IA son fer de lance de ses activités futures, ce aussi et surtout dans le domaine de la santé. La participation d'industriels aux travaux et réflexions sur la taxation du numérique est du reste notable[11].

En attendant, pressés tout à la fois par leur opinion publique et leurs contraintes budgétaires, une multitude d'États ont fait le choix de faire cavalier seul en instituant leur propre taxe locale sur l'économie numérique. Comme en France, celle-ci est généralement une taxe sur le chiffre d'affaires assise sur un nombre, une proportion de clics permettant de localiser quelque consommation numérique[12].

## II. – La taxation des données

Mis en exergue par le groupe de travail de l'OCDE dédié à la fiscalité du numérique, le cas des données mérite une mise en lumière toute particulière. Et ce ici d'autant plus qu'elles sont le ferment de l'IA. Le XX$^{e}$ a eu le pétrole, le XXI$^{e}$ a les données (avec peut-être malheureusement l'or bleu…).

Souvent issues des « travailleurs » « gratuits » que sont les internautes, les administrés et autres consommateurs, les données peuvent être catégorisées. Il y a tout d'abord les données observées qui résultent du recueil des traces d'utilisation d'une application (clics, survols, toutes informations horodatées et géolocalisées). Il y a ensuite les données soumises par l'utilisateur qui ont fait l'objet d'une saisie

(11) OCDE, Intervention de Louise Weingrod, VP tax director du groupe Johnson&Johnson, leader mondial des industries de santé, 22 nov.2019 (https://oecdtv.webtv-solution.com/5967/or/Public-consultation-on-the-Secretariat-Proposal-for-a-Unified-Approach-under-Pillar-One.html).

(12) CGI, art. 299 à 300 et 1693 *quater* à 1693 *quater* B.

explicite par ce dernier. Il y a enfin les données dites « inférées », déduites de traitements, en particulier de recoupements pratiqués à partir de données personnelles.

Toutes nourrissent l'IA et participent d'une chaîne de valeur dont la création se trouve être hors norme quant à ses montants et sa rapidité d'occurrence à l'échelle de l'histoire.

Le constat s'impose : à ce jour, l'appréhension fiscale de ce que nous nommerons l'or gris est confrontée à des difficultés d'ordre tout à la fois pratique, juridique et économique(13). Il est vraisemblable que ces difficultés participent de l'incapacité qu'a eue jusqu'à ce jour l'OCDE d'élaborer un modèle de taxation de l'économie numérique, chacune de ces deux taxations étant intrinsèquement liées.

## III. – La taxation des robots

Il n'a pas fallu attendre le XXIe et le développement de l'IA pour envisager un monde où les robots eussent quelque personnalité. Il n'y a qu'à penser à certaines œuvres cinématographiques, comme *Terminator* ou encore *2001 L'Odyssée de l'espace*.

La fiction devenant réalité s'agissant de la présence de robots parmi nous, la question d'une telle personnalité émerge. Où le débat quant au « I » de l'IA trouve quelque acuité. L'intelligence dont il s'agit est-elle augmentée, alors propre à l'être humain et aux fictions juridiques y attachées qu'il a créées telles les sociétés commerciales(14), ou bien artificielles, alors susceptibles d'affubler un robot ?

La perspective d'une taxation propre des robots a pris une dimension médiatique pendant la campagne des élections présidentielles en 2017. C'était l'une des propositions du candidat socialiste Benoît Hamon aux fins de financement d'un revenu universel, comme caractéristique d'une société nouvelle.

Issu du terme tchèque *robota* signifiant « sevrage », le robot qu'il s'agirait de taxer est tout autre du robot ménager ou de la machine-outil, eux déjà appréhendés sous couvert de stock et d'immobilisations comptables. Il répondrait à cinq caractéristiques selon le Parlement européen, qui a adopté le 16 février 2017 une résolution concernant des « règles de droit civil sur la robotique »(15) : l'autonomie, la capacité d'auto-apprentissage, l'enveloppe physique, la capacité d'adaptation à son environnement et l'absence de vie au sens biologique.

L'intérêt de la taxation des robots serait de compenser les pertes fiscales et de cotisations sociales qui risquent d'accompagner, quoiqu'on en dise, le remplacement de l'homme par le robot dans un certain nombre de tâches. Nonobstant les nouveaux emplois que l'automatisation et l'IA vont créer, bien des experts s'accordent à considérer que le bilan risque d'être négatif, d'où le projet de société et de revenu universel envisagé que les robots seraient amenés à financer.

Les conditions de taxation des robots pourraient être diverses. Sans aller jusqu'à affubler les robots d'une personnalité fiscale, quoique, deux modes de taxations possibles émergent. Tout d'abord, il serait envisageable de créer un impôt réel

(13) Rapport « Collin et Colin » sur la fiscalité du numérique, janv. 2013.
(14) Yuval Noah Harari, *Sapiens : Une brève histoire de l'humanité*.
(15) PE, *Règles de droit civil sur la robotique*, Résolution du PE du 16 févr. 2017 contenant des recommandations à la commission concernant des règles de droit civil sur la robotique (2015/2103(INL)) 2014-2019 (www.europarl.europa.eu/doceo/document/TA-8-2017-0051_FR.pdf?redirect).

sur les robots. À l'image de taxes foncières ou de la cotisation foncière des entreprises (CFE), son propriétaire ou son utilisateur seraient imposés. Ensuite, on pourrait tout à fait imaginer une taxation spécifique du bénéfice généré par l'activité du robot. Mais dans l'un et l'autre cas, le risque d'achopper sur la valorisation des bases est forte et renvoie à la complexité de fiscaliser économie numérique et données, et *de facto* ce que recouvre l'IA.

En attendant que le robot fasse l'objet de mentions spécifiques dans les textes fiscaux, il est déjà à l'œuvre sous couvert d'IA en support de ceux qui font de la fiscalité leur pain quotidien.

SECTION 2

# L'INTELLIGENCE ARTIFICIELLE, UNE NOUVELLE FONCTION SUPPORT

## § 1. – Une fonction support aux mains de l'administration fiscale

### I. – Une aide d'ores et déjà effective

Les médias grand public s'en font déjà l'écho, l'IA est un outil d'ores et déjà mis en œuvre par l'administration fiscale dans ses politiques et pratiques de vérification.

Exemple parmi d'autres, citons la chronique économique matinale de France Info (groupe Radio France) du 18 février 2020 :

« Grâce à l'intelligence artificielle, Bercy croise les fichiers, analyse les milliers de données des différentes administrations, fait des recoupements, c'est ce qu'on appelle le *data mining :* cela lui permet notamment de repérer les profils de contribuables qui présentent le risque le plus élevé de fraude et donc d'améliorer le ciblage des contrôles. Rien que ces outils technologiques ont permis de récupérer 785 millions d'euros cette année, soit deux fois plus qu'en 2018. L'utilisation de ces logiciels est d'autant plus intéressante que cela ne coûte pas trop cher à l'administration »[16]

L'administration fiscale disposant de nombreuses bases de données, elle est on ne peut mieux placée pour nourrir l'IA dédiée. Une IA à qui il est appris à déceler les contradictions entre fichiers, les changements notables visibles en comptabilité. Des *data-scientits* ont été recrutés à cette fin. Ils s'emploient à déployer de nouveaux outils informatiques à la fois pour mieux cibler la fraude fiscale et pour optimiser la programmation des contrôles fiscaux grâce aux avancées de l'IA.

Le fait n'est pas si récent. En soutien apporté au contrôle fiscal des comptabilités informatisées (« CFCI »), l'utilisation de technologies numériques au service de la lutte contre la fraude fiscale s'inscrit dans une démarche initiée dès 2008 avec la création de la Délégation nationale à la lutte contre la fraude (DNLF). Depuis 2013, l'administration

(16) Décrypte Eco du 18 février 2020, par F. Guinochet (www.francetvinfo.fr/replay-radio/le-decryptage-eco/le-decryptage-eco-lutte-contre-la-fraude-fiscale-9-milliards-d-euros-recuperes_3812583.html).

fiscale développe un traitement automatisé de données dénommé « ciblage de la fraude et valorisation des requêtes » (CFVR) qui consiste à appliquer des méthodes statistiques sur des informations en provenance de diverses bases de données.

En parallèle, l'administration multiplie du chef des contribuables les obligations déclaratives susceptibles de venir gonfler les bases de données, nourritures de l'IA. Parmi ces obligations, peuvent être citées :

– depuis 2014, l'obligation de fournir en tout début de contrôle fiscal le fichier (informatisé) de ses écritures comptables (« FEC »)[17] ;

– dans le même temps, l'obligation de fournir, dans les six mois du dépôt de sa liasse fiscale, une documentation de prix de transfert dite « allégée » (« 2257 »)[18] ;

– dans la droite ligne des travaux OCDE/BEPPS, l'obligation pour tout groupe international de fournir la cartographie mondiale de ses ressources humaines, de ses marchés, de ses revenus, *etc.* (« CBCR »)[19] ;

– issue d'une directive européenne[20], avec application rétroactive sur 2018 dès le premier trimestre 2021, l'obligation de révéler tout schéma, toute opération, susceptible de participer quelque optimisation fiscale (« DAC 6 »).

Dernier événement en date, la loi de finances pour 2020, en son article 154, autorise à titre expérimental l'administration fiscale et l'administration des douanes à collecter et exploiter au moyen de traitements informatisés et automatisés les contenus librement accessibles publiés sur Internet par les utilisateurs de plateformes en ligne afin de détecter les comportements frauduleux.

Cet outil vient enrichir le traitement automatisé de données (*cf.* CFVR), confirmant la volonté de l'administration de s'appuyer davantage sur l'IA pour améliorer le ciblage des contrôles fiscaux.

Ceci dit, pour entrevoir les limites opposables à telle volonté, le Conseil constitutionnel, soutenu en cela par la CNIL, n'a pas manqué à cette occasion d'en rappeler certaines, non sans avoir partiellement censuré cet article en restreignant légèrement son champ d'application[21].

## II. – Des limites tout autant juridiques que factuelles

Si du côté juridique c'est la CNIL qui mène la danse d'une certaine résistance au développement de l'IA ici en matière de contrôle fiscal, du côté des faits, les limites envisageables tiennent, c'est en tout cas le point de vue de l'auteur, à la nature même de l'IA.

### A. – Limites juridiques

En matière fiscale comme par ailleurs, la CNIL veille. Elle veille notamment à ce que les droits fondamentaux des personnes soient respectés quant à l'usage fait de leurs données personnelles.

(17) LPF, art. L. 47 A-I ; BOI-CF-IOR-60-40-10.
(18) BEPS, action #13.
(19) CGI, art. 223 quinquies B.
(20) Cons. UE, dir. (UE) 2018/822, 25 mai 2018, modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal en rapport avec les dispositifs transfrontières devant faire l'objet d'une déclaration.
(21) Cons. const., 27 déc. 2019, n° 2019-796 DC.

Les conditions d'adoption de l'article 154 de la loi de finances pour 2020, qui était à l'origine l'article 54 du projet de loi dont la presse grand public s'était fait l'écho à l'automne 2019, constituent une bonne illustration des limites opposées à l'usage de l'IA en matière de vérification fiscale.

Dans son avis du 12 septembre 2019[(22)], la CNIL avait émis une réserve de fond quant à la possibilité pour l'administration de recourir à des technologies de type « auto-apprenantes », usuellement utilisées en matière de détection et de prévention de la fraude, et qui peuvent conduire à une aspiration excessive de données.

Par ailleurs, la question du traitement des données sensibles reste suspendue. Si les données sensibles doivent faire l'objet d'une suppression dans les cinq jours de leur collecte (quand la CNIL préconise leur destruction immédiate), leur traitement éventuel par l'administration n'est pas véritablement encadré par la loi. Quand le Conseil constitutionnel semble considérer que ces données ne peuvent faire l'objet d'aucune exploitation à des fins de recherche de manquements ou d'infractions[(23)], l'article 154 de la loi de finances pour 2020 n'exclut pas le traitement de telles données.

Un rapport devra être remis au Parlement ainsi qu'à la CNIL six mois avant la fin de cette expérimentation, soit à l'été 2022, afin d'évaluer, d'une part, la pertinence et l'efficacité du dispositif, d'autre part, si l'amélioration de la lutte contre la fraude fiscale – qui constitue un objectif à valeur constitutionnelle – est proportionnée à l'atteinte portée au respect de la vie privée.

À suivre…

## B. – Limites factuelles

L'instauration de l'obligation de fournir un fichier des écritures comptables au début de toute vérification fiscale avait fait craindre le développement des contrôles à distance et digitaux. Ni la lecture d'un fichier des écritures comptables ni l'intervention de l'IA n'exonérera les membres de l'administration fiscale et les représentants des entreprises de se rencontrer et de discuter. Ce au moins pour deux raisons.

D'abord, ce qui manque à l'IA c'est le sens commun, celui qui permet de lire au-delà de ce qui est présenté. L'exemple présenté par Yann Le Cun du Collège de France, père et spécialiste de l'IA[(24)], est illustratif de ce qu'est le sens commun : « C'est grâce à l'apprentissage non supervisé que nous pouvons interpréter une phrase simple comme "Jean prend son portable et sort de la pièce". On peut inférer que Jean et son portable ne sont plus dans la pièce, que le portable en question est un téléphone, que Jean s'est levé, qu'il a étendu sa main pour attraper son portable, qu'il a marché vers la porte. Il n'a pas volé, il n'est pas passé à travers le mur. Nous pouvons faire cette inférence, car nous savons comment le monde fonctionne. C'est le sens commun ». On comprend avec cet exemple, parce qu'à date l'IA ne saurait véritablement apprendre par elle-même, que tout ce qui participe aux choix

(22) CNIL, avis n° 2019-114, 12 sept. 2019.
(23) Cons. const., 27 déc. 2019, n° 2019-796 DC.
(24) Y. LeCun, *Recherches sur l'intelligence artificielle*, 2015-2016 (www.college-de-france.fr/site/yann-lecun/Recherches-sur-l-intelligence-artificielle.htm).

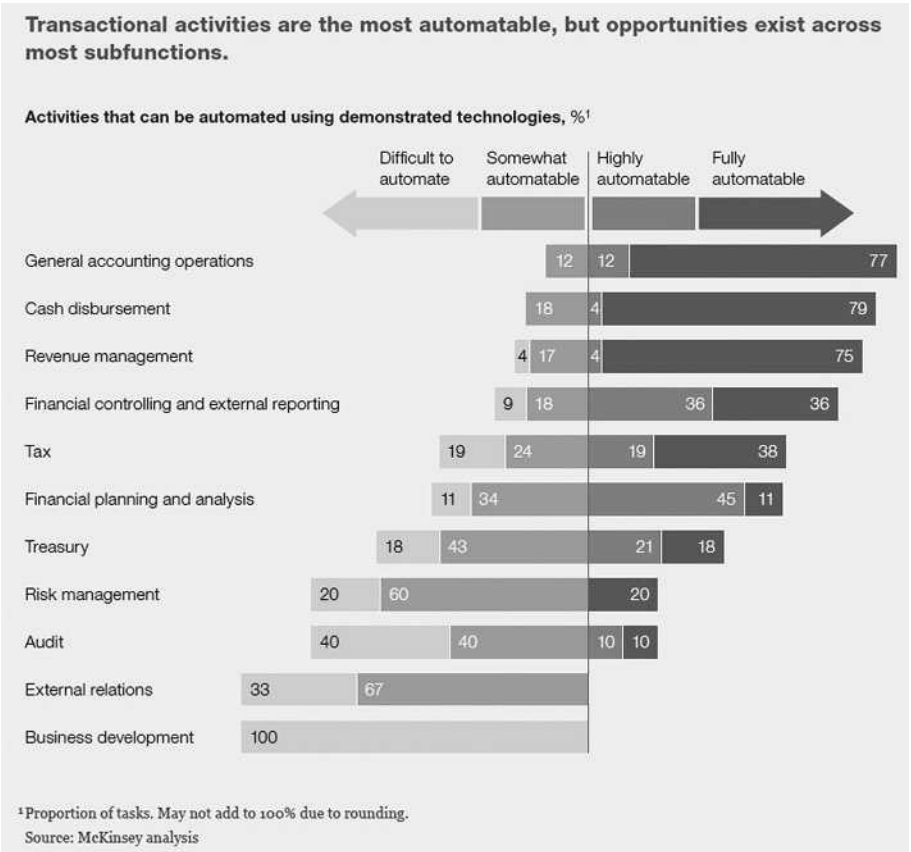
comptables et fiscaux faits par les entreprises ne saurait complètement être abrité dans une écriture de compte et/ou dans la case d'une déclaration fiscale. Cet autour inhérent au sens commun méritera toujours de devoir être explicité de vive voix.

Également, par référence au concept de *biais*, l'IA ne sera que ce que son créateur humain en aura fait. Et par nature celui-ci ne saurait avoir l'objectivité froide d'une machine, jusqu'à pouvoir se tromper dans les règles dictées à sa création. Là aussi, ce ne sera que par la voie de voix humaines qu'un semblant d'égalité et de justesse de traitement pourra être (r)établi au cas où quelque déviance serait observée.

## § 2. – Une fonction support dans l'entreprise

### I. – Une aide prometteuse

Elle est loin l'image du comptable fiscaliste en bras de chemise crayon à la main. Elle est bientôt loin également celle du même col blanc expert du fichier Excel. Les publications sont légion sur ce que l'IA permettrait d'engranger d'économies et de gain de temps dans la sphère financière. Ce n'est effectivement pas seulement la comptabilité et la fiscalité qui sont concernées, mais toute une série de fonctions au sein des directions financières (V. Figure 1).



L'IA et ce qu'elle recouvre a pour objet de limiter les interventions manuelles, sources d'erreurs et consommatrice de temps, un temps susceptible d'être consacré à des activités à plus forte valeur ajoutée. C'est ici comme une aide à la décision qu'il faut voir l'IA. Exemple parmi d'autres, la réalisation d'une documentation de prix de transfert, particulièrement clé dans le secteur des industries de santé[25], devrait être facilitée. En effet, si l'analyse fonctionnelle devrait rester l'apanage de cerveaux humains, le tri réalisé dans les bases de données de façon à en extraire ces entreprises comparables à qui se référer devrait être grandement facilité.

Ceci dit, ce n'est pas seulement l'IA qui ici intervient. Entre automatisation et l'intelligence artificielle, il existe un domaine qui a les avantages de la première (gagner en productivité, en fluidité, en sécurité et en performance) sans les inconvénients de la seconde consistant en la suppression de la place de l'humain, au profit de la machine et d'algorithmes qui prennent les décisions à sa place, ce qui suscite des craintes légitimes) : c'est le domaine de la robotisation. Ce que l'on nomme la *Robotic Process Automation* (RPA) permet de robotiser des tâches répétitives relativement simples, par exemple la saisie d'informations, la copie de données ou les connexions à des applications. Un processus peut être robotisé s'il est à la fois récurrent et dématérialisable, tout en utilisant des règles simples (comparaison de factures, vérification d'adresses, saisie de données dans différentes bases, *etc.*), critères qui caractérisent la fonction comptable. Pour alors citer un autre exemple, et cette fois rester plus strictement dans le domaine des industries de santé, on peut tout à fait imaginer qu'à moyen terme, une IA se connecte au portail de l'URSSAF et procède à la déclaration des contributions sectorielles dues[26], non sans au préalable avoir extrait des systèmes d'information de l'entreprise de quoi y procéder.

## II. – Limites... et conclusion

Les mêmes limites juridiques et factuelles à l'intervention de l'IA en support de l'administration fiscale sont ici opposables à son développement entre entreprises. Question de bon sens et de biais, si ce n'est de confiance. La vie en entreprise est faite de grains de sable que seul un esprit humain sait nettoyer de l'engrenage des systèmes d'information. L'IA ne sait faire que ce qu'on lui a appris à faire sur la base de généralités et d'expériences passées. Or le quotidien est fait de nouveautés et de singularités. Certes, les équipes comptables et fiscales des entreprises n'auront plus à être aussi fournies qu'elles peuvent l'être. Il n'en reste pas moins qu'il se trouvera toujours une opération, une stipulation, une situation, toutes singulières, qui rendront nécessaire l'intervention humaine pour leur rendre leur juste traitement au cas où elles fussent prises par erreur dans le flux des généralités.

(25) V. FM Litec, 48-10, n° 86.
(26) Contributions sur les dépenses de promotion et contributions sur les ventes, V. FM Litec, 48 et 48-10.

L'intuition, la création, l'imagination et la prise de risque font des métiers de la fonction fiscalo-comptable des métiers qui ne sauraient être entièrement dévolus à l'IA. Il n'en reste pas moins qu'entre les activités qui lui sont effectivement transférées et le rôle d'aide à la décision qui lui sera attribué, elle a vocation à trouver une place de choix dans les organisations, sans pour autant jamais ne devoir s'autonomiser, sans quoi ce ne serait pas de société mais d'ère dont nous aurions changé.

Décembre 2020

CHAPITRE 13

# L'IMPACT DU NUMÉRIQUE DANS LES RESTRUCTURATIONS EN SANTÉ

Béatrice ESPESSON-VERGEAT

*en collaboration avec*
Abdelaalim KEDDAD
Mohamed MOKADDEM
Sandrine NTETE

Le secteur de la santé[1], entendu au sens large, est fortement touché par des vagues de restructurations et réorganisations liées à sa nature intrinsèque. Dans le domaine de la santé, l'innovation médicale, biologique, pharmaceutique suscite l'appétit des investisseurs. Ces derniers s'engagent de plus en plus à apporter un capital financier aux petites *startups* qui ont des moyens limités, mais un potentiel d'innovation exponentiel. Cela s'explique par l'efficience des outils de recherche et développement (R&D), en utilisant notamment des technologies nouvelles comme l'intelligence artificielle et la *blockchain* (*cf.* Chapitre 6).

L'industrie des produits de santé tout particulièrement a connu des pics de restructuration correspondant aux phases d'innovation forte. Les aléas liés à la fin des *blockbusters*, et la chute des brevets dans le domaine public ont conduit à une réorganisation du marché, et les cartes ont été rebattues avec l'entrée dans le secteur des *startups* innovantes, des prestataires de services numériques, ou encore des fabricants de produits génériques et biosimilaires[2]. Les opérations de restructuration visent les fusions-acquisitions, autrement appelées M&A (*Merger and Acquisition*).

Désormais, ce sont les acteurs impliqués dans le monde du numérique qui jouent un rôle déterminant dans les restructurations du secteur de la santé, soit parce qu'ils permettent de renforcer la valeur et l'innovation des activités initiales,

(1) Le secteur de la santé comprend l'ensemble des activités en lien avec la santé, produits de santé, services numériques en santé, établissements de santé et médico-sociaux, activités périphériques de prestations de services numériques.
(2) P. Nauwelaerts, *Les fusions-acquisitions créent-elles de la valeur aux actionnaires des entreprises de l'industrie pharmaceutique ?*, Louvain School of Management, Université catholique de Louvain, 2017.

soit parce qu'ils deviennent des acteurs incontournables du développement de la santé globale, dans la perspective de la stratégie « Ma santé 2022 ». La crise sanitaire liée à la Covid-19 a d'ailleurs *in fine* intensifié le recours à ces opérations pour répondre aux nouveaux enjeux stratégiques de réorganisation, d'optimisation et de performance.

Les rapprochements entre multinationales et petites sociétés émergentes représentent de réelles opportunités de croissance externe, et permettent aux acteurs de l'industrie d'élargir leur portefeuille de produits, d'acquérir et de développer de nouvelles technologies ou savoir-faire et de se positionner sur de nouveaux marchés innovants(3). En effet, en Europe, l'activité des M&A a diminué de 21,9 % en 2019, par rapport à l'année 2018. Alors que le marché mondial assiste à des *mega deals*, notamment au cours de l'année 2020, il convient de remarquer la décroissance du marché européen. Les études économiques du LEEM indiquent en 2019 que le marché mondial du médicament a atteint 1 106 milliards de dollars de chiffre d'affaires (environ 977 milliards d'euros), en croissance de plus de 5 % par rapport à 2018.

Le marché américain (États-Unis) reste le plus important, avec 47,5 % du marché mondial, loin devant les principaux marchés européens (Allemagne, France, Italie).

La France demeure le deuxième marché européen derrière l'Allemagne. Toutefois, elle voit sa part de marché reculer de 2,2 points en dix ans. Cela s'explique par une baisse des *mega deals*, c'est-à-dire des opérations de restructuration supérieures à 10 milliards de dollars. La part des M&A dans le secteur de la santé reste néanmoins très importante puisque parmi les cinq plus grosses opérations en 2019, trois fusions-acquisitions ont eu lieu dans le domaine des industries et laboratoires de santé(4). Dans la course apparaissent, aux côtés des *Big Pharma*, de petites entreprises innovantes(5) dont la valorisation est sans précédent dans le contexte nouveau de la pandémie.

La crise Covid-19 n'a pas ralenti les opérations au niveau international avec les plus gros *deals* réalisés dans le secteur(6). Les acteurs économiques qualifient même ces opérations de « coronafusion », visant ainsi les rapprochements entre les industries pharmaceutiques impliquées dans la recherche d'un traitement et vaccin contre le Covid-19(7). Mais dans cette course aux restructurations, il faut remarquer la situation de l'industrie française dominée par les grands groupes internationaux(8)

(3) Les Échos, *Année de fusions et acquisitions chez les géants de la pharmacie*, 30 mars 2018 (www.lesechos.fr/2018/03/2018-annee-de-fusions-et-acquisitions-chez-les-geants-de-la-pharmacie-987847).

(4) Alumneye, *Quel bilan pour le M&A en 2019 ?* (www.alumneye.fr/quel-bilan-pour-le-ma-en-2019).

(5) Y.-M. Chodankar, *Les petites entreprises pharmaceutiques indiennes, agents d'une globalisation alternative*, thèse Géographie, Université de Paris, Université Paris Diderot (Paris 7), 2020.

(6) Esteval, *Étude marché mondial des fusion et acquisition : exceptionnel regain d'activité au 4e trimestre 2020*, 10 févr. 2021 (www.esteval.fr/article.25263.etude-marche-mondial-des-fusions-et-acquisitions-exceptionnel-regain-d-activite-au-4-trimestre). – Le Figaro, *Le spectre d'une mégafusion plane sur l'industrie pharmaceutique*, 8 juin 2020 (www.lefigaro.fr/societes/le-spectre-d-une-megafusion-plane-sur-l-industrie-pharmaceutique-20200608).

(7) PwC, *Étude Global M&A Industry Trends*, réalisée sur les transactions dans le monde entier. L'activité des transactions à l'international a fait un bond par rapport aux six premiers mois de l'année 2020, avec une augmentation de 18 % en volume et de 94 % en valeur au total, deux chiffres également en hausse en glissement annuel. La progression en valeur des transactions sur la période s'explique en partie par une augmentation des *mega deals* (5 milliards de dollars et plus). Au total, 56 opérations de ce type ont été annoncées au second semestre, contre 27 au premier semestre.

(8) Le Monde, *L'industrie pharmaceutique française est dominée par de grands groupes transnationaux*, 5 févr. 2021 (www.lemonde.fr/idees/article/2021/02/05/l-industrie-pharmaceutique-francaise-est-dominee-par-de-grands-groupes-transnationaux_6068896_3232.html).

Les établissements de santé ne sont pas en reste avec des rachats nombreux et une forte concentration des groupes privés aux mains de quelques acteurs, de dimension européenne voire internationale. Les entreprises du secteur de la santé, qu'il s'agisse des industries de santé, des établissements de santé ou encore des laboratoires de biologie médicale, sont tout particulièrement touchées par les questions de restructuration[9] en raison de la spécificité liée à la politique de santé, du médicament et des produits de santé. Ce secteur, marqué par une innovation forte, par l'impact du numérique dans l'organisation des structures, par une évolution rapide des systèmes de santé et de la gestion hospitalière, connaît une innovation fulgurante, accélérée par la pandémie. Notamment, les activités de télémédecine, technologie qui a fait son apparition depuis des années, sont enfin devenues matures. En 2026, ce marché peut ainsi se chiffrer à 27 Md€ qui le positionnent à la troisième place de l'e-santé. Il se classe juste derrière le marché du dossier médical électronique qui pourrait atteindre les 34 Md€ en 2025. Le grand nombre d'applications mobiles, la plupart gratuites, conquièrent beaucoup d'utilisateurs. Ce marché se chiffrerait pourtant aux environs de 100 Md€ en 2025. Celui des objets connectés en santé généralement gérés par une application mobile lui emboîte le pas, tournant autour des 480 Md€. Ces marchés sont interdépendants. Une application mobile peut en effet être utilisée toute seule ou servir à une consultation à distance, ou encore pour gérer un objet connecté. L'IA, elle, s'applique en outre de manière transversale. À ces activités s'ajoutent toutes celles promues par les réseaux sociaux, et notamment dominées par les GAFAM.

L'activité de restructuration (M&A) est le point central de développement porté en interne par des services financiers dont la mission particulière consiste à identifier les petites PME intervenant dans les secteurs innovants dans un objectif d'intégration. Les moyens de télécommunication et les outils numériques ont permis une accélération de ces recherches et ont favorisé la mise en relation avec les grosses industries de ces petites entreprises et *startups* très généralement engagées sur la recherche et le développement en santé numérique (par ex., innovation basée sur de l'intelligence artificielle).

Cette pratique est encouragée par les politiques fiscales développées par les différents territoires, et notamment la politique fiscale française favorisant les restructurations. Il existe notamment un régime d'exonération et de sursis d'imposition pour les fusions de sociétés soumises à l'impôt sur les sociétés (IS). L'article 210 A du Code général des impôts annonce que les plus-values nettes et les profits dégagés sur l'ensemble des éléments d'actif apportés du fait d'une fusion ne sont pas soumis à l'IS[10].

L'innovation numérique constitue la valeur centrale autour de laquelle s'articulent les relations entre les structures dans un projet de restructuration, ce dans un contexte national et européen fortement tourné vers le numérique. Ces opérations se déroulent dans une dynamique d'encouragement législatif et réglementaire dans

(9) T. Mel, *L'étude des déterminants des opérations de fusions et acquisitions pour les entreprises innovantes : le cas de l'industrie pharmaceutique*, Économies et finances, Université de Lorraine, 2017.
(10) CGI, art. 210 A.

le développement du numérique en santé, dans l'industrie, comme dans les établissements de santé ou laboratoires de biologie médicale, voire dans l'articulation des missions des professionnels de santé sur la base de plateformes numériques de prise de rendez-vous. Ces développements conduisent à des levées de fond spectaculaires dont les montants s'envolent car elles ouvrent la voie à une nouvelle forme d'organisation de la santé numérique.

La question de la valeur d'une société est centrale avant toute transaction. En amont d'une opération de restructuration, il faut valoriser les actifs. Plusieurs méthodes existent pour cela : estimer la parité entre les titres anciens et les titres nouveaux, la valeur de la capitalisation boursière de la société absorbée, l'étude de l'excédent brut d'exploitation(11).

Ces techniques comptables traditionnelles sont utilisées depuis des décennies. Néanmoins, les tendances actuelles penchent vers une offre numérique et digitale qui définit une valorisation des titres de manière optimale, et reflétant au plus près la réalité(12). Le numérique suggère d'utiliser des outils novateurs dans la valorisation d'une société, notamment par sa propriété industrielle(13). Il est possible d'y exploiter les données en utilisant des algorithmes qui vont présenter de manière plus exacte l'entreprise qui fait l'objet de la restructuration. Cela permet d'analyser des leviers de croissance invisible par les comptes traditionnels (bilan et compte de résultat) mais qui sont susceptibles de dynamiser de manière considérable l'activité. La digitalisation favorise l'accès à des données financières, des opérations commerciales et même des informations réglementaires. Ce sont ces ensembles d'éléments qui vont orienter le meilleur choix d'investissement.

Dès lors, les différents outils numériques sont des clés fondamentales dans la néo-valorisation des sociétés.

Le numérique apparaît alors dans les opérations de restructuration tout à la fois comme un moyen ou un outil permettant d'améliorer et accélérer les opérations par l'analyse optimisée des cibles, mais aussi comme un objectif ou cible sur lequel les entreprises souhaitent investir et s'engager.

Le numérique intervient dans les opérations de financement comme outil de la restructuration et dans l'objectif de santé innovante à atteindre(14). Dans les deux cas, le numérique se caractérise par le développement d'outils basés sur l'intelligence artificielle, ou encore sur des outils tels que la *blockchain* qui permettent de réaliser la restructuration et d'atteindre l'objectif d'innovation en santé.

(11) R. Obert, *DSCG 4 Comptabilité et audit*, Dunod, 2019-2020.

(12) Les Échos, *Les fusions acquisitions à l'heure du digital*, 13 juin 2021 (https://business.lesechos.fr/directions-financieres/financement-et-operations/fusion-acquisition/0211004487604-les-fusions-acquisitions-a-l-heure-du-digital-211313.php).

(13) A. Pepe, *Comment la transformation digitale du secteur des services financiers et l'arrivée de nouveaux acteurs amènent-elles les institutions financières à incorporer une gestion active de la propriété intellectuelle dans leur stratégie d'innovation ?*, Louvain School of Management, Université catholique de Louvain, 2020.

(14) T. Delaye et A. Collard, *Analyse des facteurs clés de succès de la transformation digitale au sein des entreprises (Analyse inter et intra sectorielle)*, Louvain School of Management, Université catholique deLouvain, 2020.

SECTION 1

# IMPACT DE LA VALEUR NUMÉRIQUE DANS LA STRATÉGIE DE RESTRUCTURATION DES STRUCTURES DE SANTÉ

Il va sans dire que le secteur de la santé est marqué par l'impact croissant du numérique et le sera plus encore dans les années à venir. La stratégie nationale « Ma santé 2022 » est placée sous le prisme de l'innovation numérique ; il en va de même de la politique européenne portant sur la santé et le numérique et consacrée dans le nouveau règlement *EU4Health*. Le développement du secteur de la santé est propulsé par les restructurations multiples et exponentielles. La crise de la Covid-19 constitue un cataclysme d'ampleur inédite. Ce choc ébranle de façon synchrone l'industrie, les services et la distribution, ce qui provoque une déstabilisation sans précédent de l'activité avec des facteurs de croissance inédits, notamment dans la biologie médicale, dans l'industrie pharmaceutique tout au long de la chaîne de vie du produit, ou encore dans l'organisation des établissements de santé. La crise est un accélérateur de l'innovation et le numérique en est la clé, tant dans l'organisation de la recherche de produits nouveaux que dans l'analyse structurelle de la valeur de l'entreprise.

## § 1. – L'impact du numérique dans l'émergence de nouveaux acteurs et produits de santé

Le flux d'innovation technologique croissant engendre la découverte de connaissances exclusives, détenues par de nouveaux acteurs de la santé. Dans un paysage économique longtemps dominé par les entreprises du *Big Pharma*, les avancées issues de la recherche sont menées par des entreprises de tailles modestes, qui plus est sur des marchés de niche, permettant la commercialisation de produits de santé à forte valeur ajoutée appelés ***blockbusters***. Cela a été rendu possible par une maîtrise hautement singulière des outils technologiques, et par un degré de qualification important. Ces acteurs bouleversent ainsi les stratégies de croissance externe traditionnelles (fusion-acquisition et partenariats inter-entreprises ayant les mêmes domaines d'activité). Plus apte à développer ces produits dans l'ère du numérique, la théorie qui indexe le potentiel d'innovation d'une entreprise à la taille de sa structure est mise à mal et pousse ainsi à repenser les stratégies de restructuration.

Biotech, Medtech, e-santé, ces entreprises de la ***HealthTech*** ont démontré ces dernières années qu'elles pouvaient endosser un rôle de *leader* au même titre que des laboratoires dont la présence remontait aux premières avancées majeures en santé. « Biogen » et « Genzyme » sont les premières biotechs à avoir émergé. Issues du « Hub » créé autour de la santé à Boston (Massachusetts), l'histoire qui les lie fut le résultat d'une prise de conscience sur la nécessité de réunir les forces en présence autour d'un but commun, celui de relever le défi numérique pour la santé.

Cette logique d'écosystème/*cluster* a prouvé son efficacité et véhicule aujourd'hui les facteurs clés de succès que sont la pluridisciplinarité, le transfert de connaissances et de technologies, la proximité des sous-traitants, et enfin la coopération publique-privée.

Basé sur l'excellence scientifique, ce modèle a été repris en France et est appliqué dès 2005. Il se traduit par une hausse des emplois et du chiffre d'affaires généré par les *BioTech*/*MedTech*.

Ces nouvelles entreprises doivent en partie cette croissance exponentielle à l'accompagnement dont elles bénéficient dans leur stratégie globale. En effet, la problématique pour les *startups* et TPE françaises (huit ans et vingt-quatre employés en moyenne) repose dans l'intégration de services inhérents à l'industrie tels que la logistique, la distribution et la réglementation. Cela s'explique par le caractère purement scientifique de leurs innovations. En effet, 81 % des dirigeants des *startups* et TPE de *HealthTech* sont scientifiques ou médecins de formation et 61 % de leurs collaborateurs sont diplômés de master au moins dont 25 % de doctorants. La réponse apportée sous forme d'initiative française pour venir en soutien de leur développement ne se limite pas à des investissements (qui avoisineront 6 Md€ en 2022) mais passe par l'accompagnement structurel. Se trouvent six pôles de compétitivités déployés qui sont dédiés à la science de la vie et à la santé. Des incubateurs, pépinières accélératrices d'entreprises assistent près d'un tiers des entreprises qui feront l'industrie de demain. Parmi elles, 52 % sont créées à partir de la recherche académique et publique.

L'enjeu est donc de faire de la France un *leader* mondial de la santé, ce qui explique le soutien inconditionnel de l'État, de Bpifrance et d'investisseurs étrangers au domaine de la santé. En effet, La France jouit d'un écosystème de recherche et d'innovation scientifique, académique et industriel particulièrement riche. Le poids de la R&D, tant en part de chiffre d'affaires qu'en effectifs est particulièrement élevé du fait de la forte mobilisation des entreprises sur l'innovation. Mais les entreprises sont confrontées à une concurrence forte des pays émergents et à une transformation de leur modèle économique, et notamment des sociétés indiennes et asiatiques.

Globalement, le marché de la santé a été impacté par l'essor du numérique, et les circuits d'acquisitions inter-domaine classiques laissent place à de nouveaux partenariats industriels et des *mega deals*. Une prise de risque et de l'appétence pour les sociétés innovantes de *HealthTech* permettent des opérations « Win Win » entre les industriels robustes et les *startups* expertes. Les *Big Pharma*, familiarisées avec les problématiques réglementaires et logistiques, apportent des compétences contre une expertise dans la recherche et l'innovation de niche (12 % des produits développés par les jeunes sociétés de la santé ont le statut de médicament orphelin).

La réglementation européenne de 2014[15] définit les catégories d'aides compatibles avec le marché intérieur et les sociétés qui peuvent en bénéficier. Elle exclut d'office, telle qu'elle est formulée, la majorité des TPE/PME du secteur de la santé

(15) Comm. UE, règl. (UE) n° 651/2014, 17 juin 2014, déclarant certaines catégories d'aides compatibles avec le marché intérieur en application des articles 107 et 108 du traité.

de plus de trois ans. Une révision partielle a été apportée à mi-parcours de l'exercice en 2017, ouvrant la voie à l'attribution d'aides à certaines *startups*. Néanmoins, Bpifrance et l'Agence nationale de la recherche (ANR) ne l'ont pas pris en compte dans leurs instructions d'attribution des aides.

Actuellement, un grand nombre de jeunes TPE/PME, notamment dans le domaine de la santé, sont privées des financements publics et des investissements privés adossés à une garantie Bpifrance. Le programme *EU4Health*, consécutif à la pandémie, propose un programme de relance de l'activité économique qui devrait permettre aux États membres d'accompagner activement les restructurations portant notamment sur le numérique en santé, considéré comme le fer de lance de la reprise économique.

Ce programme devrait permettre d'apporter une réponse et un soutien aux actions lancées en France et visant à propulser l'industrie de la santé dans un nouveau monde.

L'innovation pharmaceutique et médicale (vaccins notamment) et le développement de la médecine des « 4P » (Prédictive, Préventive, Personnalisée, Participative) sont deux réponses à ces problématiques. Elles reposent sur l'intégration de nouvelles composantes technologiques et numériques permettant de moderniser les systèmes de santé pour une meilleure prise en charge des patients, notamment avec le *cloud computing*, la cybersécurité, le *big data*, l'intelligence artificielle (IA), la robotique, la simulation numérique, les objets connectés (IoT) et la réalité augmentée.

L'innovation numérique a un rôle à jouer dans toute la chaîne de valeur de l'industrie de la santé : elle permet d'optimiser les pistes de recherche et développement, de digitaliser les processus de gestion des essais cliniques, de faciliter la transformation du modèle de démonstration de la valeur médicale, d'améliorer les systèmes de production et d'en augmenter la fiabilité, ainsi que de mieux gérer la logistique.

La multiplication des projets industriels est sans précédent et le déploiement de ces nouvelles technologies au sein des industries de santé devrait se généraliser en tirant les expériences de la phase pandémique.

Trois objectifs stratégiques sont à atteindre pour accélérer le développement du numérique dans les industries de santé, à destination des acteurs privés et des pouvoirs publics : il est indispensable de permettre aux acteurs d'exploiter les données de santé dans un cadre d'interopérabilité garantissant son acceptabilité par l'ensemble des acteurs en préservant la sécurité et la fiabilité des données. Il convient de favoriser la consolidation d'une filière industrielle structurée et compétitive grâce au levier du numérique, sous le pilotage du Comité stratégique de filière des industries et technologies de santé (CSF-ITS). Enfin, il est nécessaire d'adapter le système de santé aux nouvelles offres de santé numérique[16].

Lancés le 11 février 2021, les travaux préparatoires du Conseil stratégique des industries de santé (CSIS) se donnent d'emblée une ambition forte : faire de la France

(16) Institut Montaigne, Rapports *Innovation en santé : soignons nos talents*, mars 2018 ; *Médicaments innovants : prévenir pour mieux guérir*, sept. 2019 ; *E-santé : augmentons la dose*, juin 2020.

la première nation européenne innovante et souveraine en santé, et souhaitent établir un schéma d'orientation « Santé-Innovation 2030 »[17]. Cette évolution s'inscrit dans la perspective d'une action globale de la santé incluant l'ensemble des acteurs de santé autour du patient, et dynamisant l'activité industrielle et numérique dans un contexte de mondialisation[18].

## § 2. – Stratégies juridiques de restructuration des laboratoires du *Big Pharma*

### I. – Risques et responsabilités

Dans ce contexte, la réalisation technique des opérations de restructuration est particulièrement stratégique, et s'inscrit dans une temporalité souvent différente de celle liée à l'innovation. La difficulté majeure consiste donc à réussir les opérations dans le temps effectif de l'activité de recherche et développement. C'est pour atteindre ces objectifs de parallélisme dans la temporalité tout en respectant les procédures strictes tant au plan de la réglementation du droit de la santé, que de celles résultant du droit des sociétés et de la fiscalité, que le numérique trouve une application concrète. Une restructuration est une opération dans laquelle un ensemble organisé voit sa structuration remaniée pour atteindre une configuration nouvelle. Cette réorganisation englobe les différentes formes d'opérations juridiques telles que les fusions (fusion-absorption, fusion par création d'une société nouvelle, et fusion simplifiée), les scissions ainsi que les apports partiels d'actifs. Au niveau européen, les États membres sont soumis aux règles spécifiques nationales. En effet, le droit européen des sociétés est partiellement codifié dans la directive (UE) 2017/1132 relative à certains aspects du droit des sociétés, et les États membres continuent ainsi d'appliquer leurs propres lois sur les sociétés, qu'ils modifient en tant que de besoin pour se conformer aux directives et aux règlements de l'Union. Les efforts actuellement déployés pour mettre en place un droit et un cadre de gouvernance modernes et efficaces pour les sociétés européennes, les investisseurs et les salariés ont pour but d'améliorer l'environnement des entreprises au sein de l'Union. La réglementation de l'Union vise à permettre aux entreprises de s'établir n'importe où dans l'Union grâce à la liberté de mouvement des personnes, des services et des capitaux, à fournir une protection aux actionnaires et aux autres parties ayant un intérêt particulier dans les sociétés, à accroître la compétitivité des entreprises et à encourager les entreprises à coopérer au-delà des frontières[19]. Les dispositions européennes créent néanmoins un bloc commun permettant de protéger les actionnaires des sociétés installées dans les États membres.

(17) Ministère des Solidarités et de la Santé, *Lancement du Conseil stratégique des industries de santé 2021 (CSIS) : faire de la France la première nation européenne innovante et souveraine en santé*, 11 févr. 2021 (https://solidarites-sante.gouv.fr/actualites/presse/communiques-de-presse/article/lancement-du-conseil-strategique-des-industries-de-sante-2021-csis).

(18) Institut Montaigne, *Filière santé : gagnons la course à l'innovation*, mars 2021.

(19) TFUE, art. 49, 50, § 1 et 2, pt g), et art. 54, 2e al.

La fusion-acquisition (*Mergers and Acquisitions*) désigne la situation dans laquelle deux compagnies fusionnent pour ne former qu'une seule entité juridique, ayant une gouvernance unique. Le patrimoine de la société absorbée est transféré à la société absorbante par le mécanisme du transfert universel de patrimoine. Les buts de cette stratégie financière sont multiples. Cela permet à une société de se renforcer sur un type de marché qui est le sien, ou alors sur un secteur d'activité différent.

Ces opérations juridiques sont d'une lourdeur administrative conséquente. Dès le début des pourparlers, des négociations de toutes natures ont lieu entre les sociétés sur des questions relatives notamment à la valorisation des actifs, aux comptes et déficits, au développement et à l'investissement en R&D, à la protection de la propriété industrielle, à la gestion des contrats de production, distribution, à l'encadrement des ressources humaines, à la désignation des organes de gouvernance, à l'identification des procédures en cours et plus généralement à l'ensemble des questions liées à l'activité et à son développement économique. Ces opérations supposent un temps long, l'organisation d'une *data room* et l'encadrement de son accès. Ces opérations sont placées sous le régime du droit européen retranscrit en droit interne. La dixième directive sur le droit des sociétés – la directive 2005/56/CE sur les fusions transfrontalières des sociétés de capitaux – a pour objectif de faciliter les fusions transfrontalières entre sociétés de capitaux. Le transfert du siège d'une société de capitaux d'un État membre à un autre ainsi que sa fusion ou scission constituent des aspects inhérents à la liberté d'établissement consacrée par les articles 49 et 54 du Traité sur le fonctionnement de l'Union européenne (TFUE)[(20)]. L'éventualité du transfert transfrontalier du siège statuaire reste une question non résolue. Le droit européen offre par ailleurs les garanties sur les situations financières des sociétés en précisant que les documents relatifs aux comptes sociaux (comptes annuels, comptes consolidés et agrément des personnes chargées du contrôle légal de ces comptes) donnent à leurs lecteurs une image fidèle du patrimoine, de la situation financière et des résultats des sociétés. L'ensemble des directives et règlements encadrent les activités financières des entreprises en vue de protéger les tiers, et les actionnaires notamment dans les opérations de restructuration[(21)]. Le Parlement européen a quant à lui adopté une résolution en 2019 sur les opérations de fusion-acquisition[(22)]. Le numérique a fait son entrée dans l'organisation de ces opérations qui se déroulent sur plusieurs territoires, afin d'assurer la rapidité, la sécurité, la transparence et l'efficacité de ces opérations[(23)] particulièrement lourdes, complexes et risquées pour les sociétés absorbantes, ce qui explique la nécessité d'une connaissance parfaite de la cible absorbée et une transparence dans les informations communiquées. En effet, au niveau pénal, la jurisprudence de la Cour de cassation a ajouté une obligation supplémentaire depuis le 25 novembre 2020[(24)].

(20) CJUE, 16 déc. 2008, aff. C-210/06, *Cartesio*.
(21) Dir. (UE) 2019/2121, 27 nov. 2019, modifiant la directive (UE) 2017/1132 en ce qui concerne les transformations, fusions et scissions transfrontalières : *JO* 12 déc. 2019, n° L 321, p. 1.
(22) PE, Résolution législative sur la proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2017/1132 en ce qui concerne les transformations, fusions et scissions transfrontalières, 18 avr. 2019.
(23) PE et Cons. UE, dir. (UE) 2019/1151, 20 juin 2019 modifiant la directive (UE) 2017/1132 en ce qui concerne l'utilisation d'outils et de processus numériques en droit des sociétés.
(24) Cass. crim., 25 nov. 2020, n° 18-86.955, Fp-P+B+I.

La chambre criminelle de la Cour de cassation considère désormais qu'en cas de fusion-absorption d'une société par une autre société, la société absorbante peut, à certaines conditions, être condamnée pénalement pour des faits commis par la société absorbée avant la fusion. Ce revirement était attendu et trouve appui sur le droit européen. La Cour de justice de l'Union européenne, dans un arrêt rendu le 5 mars 2015, a en effet jugé que l'article 19 de la directive 78/855/CEE du Conseil du 9 octobre 1978, devenu l'article 19, § 1er de la directive 2011/35/UE du 5 avril 2011, relatif aux fusions internes de sociétés anonymes, s'interprète dans le sens qu'une fusion par absorption entraîne la transmission, à la société absorbante, de l'obligation de payer une amende infligée par décision définitive, après cette fusion, pour des infractions au droit du travail commises par la société absorbée avant ladite fusion(25). Dans un arrêt en date du 1er octobre 2019, la Cour européenne des droits de l'homme avait en effet déclaré irrecevable la requête formée par la société Carrefour France SAS, condamnée à une amende civile en application de l'article L. 442-6 du Code de commerce, s'agissant de pratiques anticoncurrentielles commises par la société Carrefour hypermarchés France, qu'elle avait absorbée(26). Les juridictions internes, « en prononçant contre la société requérante l'amende civile prévue par l'article L. 442-6 du Code de commerce, sur le fondement du principe de continuité économique et fonctionnelle de l'entreprise, (…) n'ont pas porté atteinte au principe de la personnalité des peines » la « société » s'efface au profit l'« entreprise », laquelle existe toujours au travers de la continuité de l'activité économique, et ce, malgré l'opération de fusion-absorption (…). Selon l'article L. 236-3 du Code de commerce, la fusion-absorption, si elle emporte la dissolution de la société absorbée, n'entraîne pas sa liquidation. De même, le patrimoine de la société absorbée est universellement transmis à la société absorbante et les actionnaires de la première deviennent actionnaires de la seconde. La société absorbante peut donc voir sa responsabilité pénale engagée et être déclarée coupable s'agissant de faits commis par la société qu'elle a absorbée. La troisième chambre civile de la Cour de cassation a, pour sa part, réaffirmé, le lendemain de cette décision, ce principe de transmission universelle du patrimoine de l'absorbée à l'absorbante en matière de responsabilité contractuelle(27).

L'aggravation de la responsabilité des sociétés absorbantes, à laquelle s'ajoute la complexité des procédures, explique la nécessité d'utiliser les outils numériques et notamment la technique *blockchain* afin de sécuriser les opérations de fusion. Pour éclairer tout risque d'opacité, la pratique a fait naître des rapports contractuels nouveaux qui facilitent les transactions. Cela consiste en la mise en place de pactes de partenariat entre les entreprises, ou encore à créer des conventions de collaboration sur un domaine particulier, validées par les autorités de contrôle (Autorité des marchés financiers et Autorité de la concurrence) et sécurisées par l'emploi des techniques numériques.

(25) CJUE, 5 mars 2015, aff. C-343/13, *Modelo Continente Hipermercados SA* c/ *Autoridade para as Condiçoes de Trabalho*.
(26) CEDH, 5e sect., 1er oct. 2019, n° 37858/14.
(27) Cass. 3e civ., 26 nov. 2020, n° 19-17.824.

## II. – Différentes formes de structuration des opérations

Les flux monétaires impressionnants qui circulent derrière les industries de santé laissent apparaître des prédateurs sur le marché. Ce terme, qui n'a pas forcément une connotation négative, est utilisé pour définir les acteurs qui sont intéressés par l'acquisition de tout ou partie d'une innovation en matière de santé. Ce sont la plupart du temps des fonds d'investissement, des laboratoires pharmaceutiques, des *business angels*(28), les GAFAM.

Dans ce secteur de la santé, les opérations dépassent largement les frontières nationales et de l'Union européenne. La structuration même de l'activité depuis la recherche jusqu'à l'organisation de la *supply chain* et la distribution des produits se développent sur de nombreux territoires au sein desquels sont exploitées les structures gérant les matières premières à usage pharmaceutiques (API), puis les sites de fabrication et production, les activités de transport, de façonnage, de distribution, éclatées au niveau planétaire dans un objectif d'optimisation fiscale et logistique. Cependant, la dépendance de l'Union européenne et de la France aux activités chinoises et indiennes notamment est à l'origine des risques de ruptures de stock et tensions d'approvisionnement. L'Union et les États membres s'engagent fortement dans une course à la relocalisation, qui génère des formes nouvelles d'accords entre industries pharmaceutiques, et en conséquence de nouvelles voies de restructuration(29). L'avenir des industries se joue à la sortie de crise de la Covid-19, avec de nouvelles formes stratégiques de restructuration basées sur l'emploi d'outils numériques et portant sur la promesse de santé digitale(30).

Les stratégies classiques sont désormais déployées au moyen d'outils numériques perfectionnés. La stratégie du *venture capital* signifie en français « le capital-risque ». Il désigne la stratégie d'une personne morale ou physique qui décide d'investir dans une activité risquée, en particulier dans des *startups* innovantes. La prise de participation au capital de la société peut se faire d'une manière partielle ou majoritaire. Au-delà de l'investissement financier, le *business angel* ou le fonds d'investissement apporte en général une expertise dans le domaine de l'innovation (des outils techniques, un réseau d'affaires, une expérience…). La caractéristique principale de cette stratégie est le fait de mettre à disposition des moyens conséquents à un stade précoce de la vie de la *startup*.

Le risque de ce processus est de faire appel à des investisseurs qui sont étrangers au monde de la santé. L'ensemble de l'écosystème éthique que possède un industriel en santé se voit mis à mal par les volontés capitalistiques de ses apporteurs financiers. L'intérêt du patient a de fortes chances de passer au second plan. La frontière entre ces deux ambitions devient très friable.

Cette stratégie peut être perçue comme une substitution à la recherche R&D des industries de santé. En ce sens, un laboratoire pharmaceutique peut décider

(28) Désigne une personne physique qui investit dans une société à un stade très précoce de son activité, misant sur l'innovation potentielle qu'elle va découvrir.

(29) AN, Rapport sur la proposition de résolution européenne (n° 2904) de M. F. Brunet et plusieurs de ses collègues relative à la relocalisation de la fabrication des médicaments et des principes actifs pharmaceutiques en Europe, 11 juin 2020.

(30) LEEM, *Étude prospective sur « La santé en 2030 »* (www.leem.org/frederic-collet-president-du-leem).

de réduire ses coûts de recherches en investissant dans une société qui a déjà subi l'ensemble de cette charge. Cela lui permettra par exemple de contourner la lourdeur des démarches d'attribution de brevet, de mener les essais cliniques ou encore de trouver, sur 10 000 molécules[31], celle qui sera utilisée pour le médicament.

Les sommes investies au terme des *venture capital* sont conséquentes. Ainsi à titre d'exemple, en 2019, les cabinets Dentons et Dechert LLP ont accompagné ImCheck, une société de biotechnologie, pour une levée de fonds de 48 millions d'euros. Selon le communiqué de presse d'ImCheck, cela a permis de faire progresser « son pipeline clinique d'anticorps ciblant les cellules T gamma delta contre le cancer et les maladies auto-immunes »[32]. Bpifrance et le laboratoire Pfizer font partie des investisseurs principaux de cette levée de fonds. Ces opérations se développent au niveau mondial et sont marquées par une relation très forte avec la Chine. Les activités de R&D se multiplient en Chine, Shanghai étant l'un des plus importants centres mondiaux de recherche sur les médicaments pour l'industrie pharmaceutique. Ces opérations sont basées sur des créations de structures et des pactes d'actionnaires, impliquant un strict respect , en France, des procédures visées par le droit des sociétés, les réglementations sur les placements financiers, la loi anticorruption[33]. L'Agence française anticorruption (AFA)[34] a publié, le 12 mars 2021, une version actualisée de son guide pratique sur les vérifications anticorruption dans le cadre des fusions-acquisitions. Ces opérations sont risquées avec de lourdes conséquences pénales. Les vérifications « anticorruption » peuvent permettre à l'acquéreur d'apprécier le risque d'engagement de sa responsabilité juridique pour des faits de corruption ou des manquements à l'article 17 de la loi du 9 décembre 2016, commis par la cible avant l'opération[35]. Le strict respect des procédures dans les délais impartis explique la nécessité de mobiliser les outils numériques et notamment la *blockchain* afin de sécuriser les informations et établir des éléments de preuve dans le cadre de la restructuration.

Autre procédure, le ***private equity*** associé au ***late stage*** est une opération par laquelle un investisseur va acheter des titres dans une société non cotée en bourse. À la différence du *venture capital*, les apporteurs financiers interviennent ici plus tard dans la vie de la société. Les fonds peuvent être utilisés pour augmenter les capacités de production des entreprises, ou encore pour restructurer une société en difficulté.

Le *late stage* est une technique ou l'investisseur intervient de manière tardive dans la vie de la société. À ce stade avancé de son existence, la société innovante

(31) LEEM, *Recherche et développement, un processus indispensable à l'innovation*, 2 oct. 2020 (www.leem.org/recherche-et-developpement).

(32) ImCheck lève 48 millions d'euros pour faire progresser son pipeline clinique d'anticorps ciblant les cellules T gamma delta contre le cancer et les maladies auto-immunes, communiqué de presse, 4 déc. 2019 (www.imchecktherapeutics.com/fileadmin/Presse/191204_ImCheck_Series_B_FR.pdf).

(33) L. n° 2016-1691, 9 déc. 2016, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

(34) Avis relatif aux recommandations de l'Agence française anticorruption destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêts, de détournement de fonds publics et de favoritisme : *JO* 12 janv. 2021.

(35) AMF, Audition de Robert Ophèle, président de l'AMF, Commission des lois de l'Assemblée nationale, Mission d'information sur l'évaluation de la loi dite « Sapin 2 », 24 mars 2021.

a déjà fait ses preuves en termes de créativité. L'efficience de son *business model* peut déjà être démontrée aux investisseurs potentiels. C'est donc à ce moment tardif que des fonds d'investissement peuvent acquérir avec moins de risques des titres dans la structure. Dès lors, si la société intervient dans un domaine peu innovant, comme par exemple dans le secteur d'une maladie connue et maîtrisable, elle n'aura pas la même valorisation qu'une biotechnologie intervenant dans la lutte contre le cancer. Le potentiel de rentabilité n'est pas le même.

Cette notion de valorisation est centrale, car il en va du montant investi dans la structure.

Le *venture capital* et le *late stage* sont deux stratégies financières intervenant à un stade temporel différent. Que ce soit au début ou à la fin des recherches cliniques, l'innovation est l'élément charnière dans la valorisation de la structure. C'est elle qui va attirer l'intérêt des investisseurs prédateurs qui peuvent être extérieurs ou non au domaine de la santé. Dans l'ensemble de ces opérations, le recours aux outils numériques permettant une évaluation financière très précise et offrant de nouvelles techniques d'acquisitions des titres s'impose, avec notamment toute l'intervention des opérations financières basées sur les cryptomonnaies ou encore les *blockchains* financières[36]. Mais c'est essentiellement l'impact du numérique dans l'activité de santé, telle que développée au cours des différents chapitres de cet ouvrage, qui conduit à valoriser et justifier l'intérêt des restructurations dans le secteur de la santé.

SECTION 2

## VERS UNE MUTATION DES OPÉRATIONS DE RESTRUCTURATION POUR LES INDUSTRIES DE SANTÉ PAR LE NUMÉRIQUE

**Le monde de la santé évolue vers de nouveaux paradigmes concentrés autour du patient actif et acteur de sa santé.** Cela conduit à de nouvelles formes de produits et services numériques, et donc à de nouveaux types de partenariats et relations entre les acteurs de santé. Ce changement de vision de la santé, largement initié mais qui doit encore se développer avec un marché exponentiel porté par l'émergence de nouvelles pathologies liées au vieillissement de la population ou encore aux facteurs environnementaux, conduit les entreprises de santé à intégrer le numérique comme un facteur clé de développement et de rapidité dans la recherche. La découverte de nouvelles formes de vaccins pour la grippe par une intelligence artificielle est une des manifestations de l'impact du numérique. L'intégration du numérique est le facteur déterminant dans les restructurations en cours, car il fonde la valeur prospective de l'entreprise de santé.

(36) A. Lourimi, A. Barbet-Massin, C. Pion, F. Fleuret et W. O'Rorke, *Droit des cryptoactifs et de la* blockchain, LexisNexis, coll. « Droit et Professionnels », 2020.

## § 1. – L'incorporation de l'intelligence artificielle dans l'analyse des restructurations

Le recours aux algorithmes intelligents permet une analyse plus rapide et plus fine de l'activité générale d'une entreprise, et tout comme elle permet la prévisibilité de l'évolution de la santé humaine et des développements pharmaceutiques, elle permet de prévoir les voies d'évolution des marchés pharmaceutiques et donc l'évolution de sa valorisation. L'analyse prédictive par le biais des intelligences artificielles permet d'anticiper l'évolution des marchés et en conséquence l'enjeu de réaliser des partenariats et pratiques de prédation sur les entreprises prometteuses.

Au plan juridique, l'essentiel de la question reliée à ces pratiques relève du droit de la concurrence, du contrôle des concentrations et de la détection des pratiques d'ententes ou d'abus de domination qui pourraient résulter de ces comportements de restructuration, conduits par l'utilisation de l'IA.

## § 2. – L'incorporation de la *blockchain* dans la structuration des industries de santé

Venant en complément et en coordination avec l'intelligence artificielle, la *blockchain* représente un avantage certain dans la valorisation des industries de santé et dans la réalisation des opérations de restructuration[37].

Cette technologie a été conçue, d'une part, pour permettre le stockage des informations et, d'autre part, pour la transmission de ces mêmes informations. Le système des *blockchains* consiste à confier l'organisation des échanges à un protocole informatique, réduisant les coûts de transaction ou de centralisation existant dans les systèmes traditionnels. Cela a ainsi permis des gains de productivité et d'efficacité.

La *blockchain* est un outil indispensable pour les industries pharmaceutiques puisqu'elle offre une traçabilité des produits. De plus, grâce à la *blockchain*, il y a une diminution du risque de contrefaçon des médicaments et une augmentation de la valorisation de l'industrie en cas de restructuration. La *blockchain* permet la mise en place d'une base de données de santé décentralisée en regroupant tous les acteurs de la chaîne logistique, hébergeant les échanges. C'est la garantie d'une traçabilité transparente et sécurisée de toutes les opérations réalisées au cours de la période de restructuration, et donc tous les échanges et opérations au cours de la phase de négociation, de projet et de réalisation de l'opération juridique à vocation internationale.

Cet outil numérique offre un service qui permet d'obtenir une confiance totale des parties. Cette confiance repose également sur le fait que les données contenues dans la *blockchain* sont immuables, elles ne peuvent pas être modifiées ou supprimées de la base de données. Pour que la *blockchain* puisse obtenir cette

(37) I. Yaqoob, K. Salah et R. Jayaraman, *Blockchain for healthcare data management : opportunities, challenges, and future recommendations*, Springer, 2021.

confiance, elle doit respecter le règlement « eIDAS[38] » n° 910/2014 du 23 juillet 2014. Cependant, on aurait tort de croire que le système de *blockchain* offre une sécurité à 100 %, car il est impossible de garantir une sécurité à 100 %[39] du fait de l'obsolescence.

Cette technologie a également donc une utilité forte dans la simplification des opérations de restructuration. La *blockchain* participe à la modernisation des outils de restructuration. Cette *data room* virtuelle facilite l'accès à l'information destinée aux acteurs impliqués : bilan financier, compte de résultat, litige juridique, audit de gestion, informations fiscales, gestion sociale de l'industrie. Ces documents sont accessibles aux agents sous la forme d'une plateforme virtuelle en ligne. La *due diligence* est fortement simplifiée et accroît les chances d'aboutissement des négociations. L'accès à cette *data room* est très souvent réglementé et soumis à des clauses de confidentialité.

La *blockchain* englobe plusieurs caractéristiques. Elle crée la confiance entre les acteurs, car il y a une plus grande transparence du fait de la lisibilité de l'information. Elle permet, de plus, une traçabilité des accès aux informations sensibles sans que ces dernières soient modifiées ou détruites. Les failles de sécurité sont dès lors considérablement amoindries.

Lors de la restructuration, les acteurs du monde de la santé doivent prendre en considération les conséquences de la violation des données personnelles. Cette violation des données peut être liée à une faille de sécurité dans leur *blockchain*, entraînant de manière accidentelle ou de manière illicite la destruction, la perte ou la divulgation non autorisée de données à caractère personnel.

Depuis l'entrée en vigueur du RGPD en 2016, la pratique a fait naître un coefficient de conformité concernant la protection des données. Il permet à la société absorbante de connaître le niveau de sécurité des informations détenues par l'industrie absorbée. Plus ce coefficient est bon, plus la valorisation de la société tend à augmenter. D'autant plus que les informations de santé sont des données sensibles au sens de la législation européenne. Il est impossible pour le patient de s'y opposer. Grâce à cela, une société qui aspire à une restructuration veille précieusement à avoir une politique RGPD efficiente. Cela s'exprime notamment par l'intervention des *Data Privacy Officers*. Ce sont des agents internes ou externes à la société qui vont s'assurer de l'application stricte du règlement européen. Ces agents contribuent eux aussi à la valorisation des industries. De nombreuses levées de fonds en cryptomonnaie pour des projets d'infrastructures de *blockchain* ou des fusions-acquisitions sont relevées dans les statistiques sur les restructurations au cours des dernières années[40].

Au-delà de l'utilisation de la *blockchain* dans l'opération de restructuration, la question se posera de savoir comment rendre compatibles des systèmes

(38) Le règlement eIDAS vise à instaurer un mécanisme de reconnaissance mutuelle des moyens d'identification électronique des États membres sur l'ensemble des services en ligne des autres États membres de l'Union européenne.

(39) Exemple de l'algorithme SHA-1 ayant été brisé et dont l'utilisation a été proscrite dans le cadre de la sécurité des signatures électroniques au titre de l'intégrité du document qui n'était plus garantie.

(40) F. Leal, A.E. Chis, S. Caton, H. González–Vélez, *Smart pharmaceutical manufacturing : Ensuring end-to-end traceability and data integrity in medicine production*, Elsevier, 2021.

numériques de *blockchain* détenant des données de la société absorbante et de la société absorbée[41].

Le recours aux outils numériques offre une opportunité d'accélération des procédures tout en garantissant sécurisation, transparence et protection des données collectées et conservées. Toutefois, la question majeure sera de préserver la scalabilité des systèmes qui devront s'adapter aux évolutions technologiques. Par ailleurs, le coût de la mise en œuvre de ces procédures et de leur interconnectivité est considérable. Ces points faibles expliquent le retard du secteur de la santé à utiliser ces outils numériques et notamment la *blockchain* par rapport à d'autres secteurs beaucoup plus avancés. Mais la crise de la Covid-19 est un accélérateur et modifie la situation.

(41) M. Vahdati, K.G. HamlAbadi et A.M. Saghiri, *IoT-Based Healthcare Monitoring Using Blockchain*, Springer, 2021.

CHAPITRE 14

# LA *BLOCKCHAIN* DANS LA STRUCTURATION ET LA RESTRUCTURATION DES ENTREPRISES DANS LE SECTEUR DE LA SANTÉ

Béatrice ESPESSON VERGEAT

*en collaboration avec*
Ibrahim TEMIRBOULATOV

## INTRODUCTION

L'industrie de la santé est entrée dans une phase d'évolution accélérée, notamment en raison de l'impact fort du numérique dans l'organisation de son activité, avec pour conséquence la multiplication des restructurations. Tout particulièrement au cours de ces dernières années, il y a une véritable course mondiale de la part de tous les acteurs de la santé vers les levées de fonds afin d'être les plus attractives et innovantes sur le marché[1]. L'innovation interne représente une difficulté pour les laboratoires pharmaceutiques qui ne peuvent plus se reposer sur leurs *blockbusters*, car les brevets portant sur ces médicaments sont tombés dans le domaine public[2]. Le secteur de la santé voit donc fleurir une multitude de *startups* tournées vers la recherche et développement[3] et la e-santé. Les grands acteurs du secteur de la santé, les *Big Pharma*, se sont donc engagés fortement dans une politique de développement numérique et de rapprochement

(1) Autorité de la concurrence, Après plusieurs mois d'instruction et une large consultation publique, l'Autorité de la concurrence rend les conclusions de son enquête sur le secteur de la santé, 4 avr. 2019.
(2) Challenges, *Sanofi rachète la biotech Kymab pour au moins 1,1 milliard de dollars*, 11 janv. 2021.
(3) Rapport de l'OPECST, *Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies*, V. Faure-Muntian, C. de Ganay, R. Le Gleut, 20 juin 2018.

accéléré avec de multiples *startups* plus agiles et plus innovantes. En effet, celles-ci peuvent conduire le développement du candidat-médicament jusqu'à l'obtention de l'autorisation de mise sur le marché (AMM), ouvrant ensuite la voie au processus d'acquisition et de restructurations par lesquelles les industries de la santé rachètent, intègrent, absorbent, s'allient aux jeunes pousses pour en assurer la croissance.

Classiquement, la restructuration peut être effectuée *via* plusieurs méthodes telles que la fusion-acquisition, la prise de participation (l'achat direct des actions ou l'achat par le biais d'une holding) ou la technique contractuelle, comme l'accord d'entreprise (*gentlemen-agreement*, *joint-venture*)[4].

C'est dans ce cadre qu'intervient la technologie de la *blockchain*, développée à partir de 2008. Cette technologie conçue dans un but de stockage et de transmission d'informations, a pour particularité de ne pas avoir d'organe central de contrôle, offrant ainsi une transparence et une sécurité dans son usage. La *blockchain* constitue une plateforme de valeur ajoutée pour les organisations et leur permet de se connecter et d'interagir de manière sécurisée à travers un large éventail de ces pratiques en plein essor.

L'Assemblée nationale, consciente de l'enjeu que représentent les *blockchains*, a rendu un rapport portant sur la mission d'information sur les usages des *blockchains* et autres technologies de certification de registre[5]. Ce rapport propose une définition de cette technologie : « Une blockchain est un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie ».

En d'autres termes, une *blockchain* est un registre, semblable à une immense base de données qui obéit à des règles fixées par un protocole, aux fins de sécurisation et authenticité de l'information grâce à la cryptographie. La *blockchain* permet ainsi une authenticité de l'information, mais également la sécurisation de l'information ou des transactions. Les écritures enregistrées sur ces blocs de chaînes sont inaltérables et infalsifiables.

Il semble donc intéressant désormais pour les entreprises pharmaceutiques d'étudier la stratégie juridique de restructuration en prenant en compte l'usage de la *blockchain* qui intervient comme un outil permettant d'apporter une sécurité dans l'organisation des opérations de restructuration (Section 1), mais aussi plus largement comme une technique de sécurisation et valorisation de l'activité économique de l'entreprise, favorisant le déroulement des restructurations (Section 2).

(4) *Fusions, apports partiels d'actif, scissions*, Mémento Lefebvre, éd. 2021.
(5) AN, *Mission d'information commune sur les usages des bloc-chaînes (blockchains) et autres technologies de certification de registres*, 12 déc. 2018.

SECTION 1

# L'INTÉRÊT DE LA *BLOCKCHAIN* DANS LA RESTRUCTURATION DES SOCIÉTÉS PHARMACEUTIQUES

Le mécanisme de restructuration des entreprises pharmaceutiques fait appel à l'application de l'ensemble des règles de droit des sociétés, et aux diverses méthodes comptables et financières permettant à toute entreprise d'évoluer et de rester compétitive sur le marché économique. Dans le secteur de la santé, les opérations de restructuration doivent prendre en compte non seulement les enjeux économiques des laboratoires, mais également les enjeux généraux de protection de la santé publique, en permettant ou favorisant le maintien sur le marché de produits indispensables aux patients. Ces opérations de restructuration peuvent, en conséquence, être volontaires ou imposées par les autorités, notamment sur un plan concurrentiel, afin de préserver les intérêts généraux des patients.

La restructuration peut donc passer par la fusion (C. com., art. L. 236-1) qui opère une transmission universelle de patrimoine d'une société à une autre, ou par création d'une société nouvelle. Elle entre dans le champ concurrentiel dans le régime des concentrations, qui s'inscrit dans le cadre légal des articles L. 430-1 et suivants et des articles R. 430-2 et suivants du Code de commerce.

L'intérêt pour ces entités d'user de la technologie *blockchain* lors de la réalisation d'une fusion, qui nécessite le transfert d'informations particulièrement sensibles, dans un cadre réglementaire rigoureux, est d'autant plus marqué lorsque l'opération est transfrontalière(6), comme cela est fréquemment le cas dans le secteur des produits de santé.

La restructuration peut se traduire également par la prise de participation d'une société dans une autre, par une procédure d'augmentation de capital ou de cessions de droits sociaux. La prise de participation peut prendre la forme d'une augmentation de capital au profit d'un actionnaire déterminé, ou d'un rachat d'actions de la société convoitée avec une prise de contrôle politique ou mathématique de la société, ce qui implique donc un changement d'actionnaire dominant ou changement du pouvoir de décision dans la gouvernance.

Enfin, la restructuration peut passer par des accords d'entreprises ; dans ce cas précis, la domination peut résulter d'un accord contractuel entre le dominé et le dominant(7), c'est notamment le cas lorsqu'une entreprise accepte de passer sous le contrôle d'une autre sans que cette dernière prenne dans l'immédiat des titres de participation. L'organisation d'une *joint-venture* entre deux structures qui décident d'en créer une troisième dans laquelle elles seront à égalité, constitue enfin une modalité de coopération classique entre structures du secteur de la santé dans

(6) PE et Cons. UE, dir. (UE) 2017/1132, 14 juin 2017, relative à certains aspects du droit des sociétés.
(7) M. Cozian, F. Deboissy et A. Viandier, *Droit des sociétés*, LexisNexis, 33e éd. 2020, p. 821.

lequel l'innovation, les droits de propriété industrielle, les autorisations de mise sur le marché des produits constituent les valeurs fondamentales à préserver.

En fonction des modalités de restructuration choisie, l'enjeu sera donc d'identifier les données qui pourront, ou devront, être communiquées aux différents acteurs, en préservant tout au long du processus leur confidentialité, sachant que les périodes de négociation peuvent être très longues, ce alors même que l'innovation scientifique évolue extrêmement rapidement et peut conduire à une valorisation positive en cas d'accès au marché de produits innovants, ou au contraire à une dévalorisation en cas d'échec dans la période scientifique, pharmaceutique et médicale. Afin de faciliter ces opérations, la technique de la *blockchain* apporte ici une solution.

## § 1. – La *blockchain* au service de la *data room* de la restructuration

Les opérations de restructuration, complexes par nature, requièrent, pour s'assurer de leur succès, différentes expertises se trouvant dans et hors de l'entreprise. Elles impliquent une mise à mise à disposition de l'ensemble des informations nécessaires sur les différentes structures concernées. Ces négociations comportent, en effet, des risques spécifiques dont la réalisation peut avoir des impacts financier, juridique et opérationnel significatifs. Il est fondamental dans ces conditions de procéder à de nombreuses vérifications, et notamment aux « vérifications anticorruption »[8]. Ces vérifications permettent d'affiner la connaissance des opérateurs, de mesurer les risques encourus en cas d'acquisition ou de fusion, et d'anticiper les conséquences au regard du dispositif anticorruption de l'acquéreur si l'opération est conclue[9]. Les vérifications anticorruptions peuvent permettre à l'acquéreur d'apprécier le risque d'engagement de sa responsabilité juridique pour des faits de corruption ou des manquements à l'article 17 de la loi du 9 décembre 2016, commis par la cible avant l'opération. Selon le Conseil d'État, il appartient donc à la société absorbante, « lors de l'opération de fusion-absorption, de recueillir toute information utile sur la situation de la société » absorbée[10]. La responsabilité civile de la société absorbante pourrait être mise en cause du fait des comportements de la cible et à raison de sa participation à des faits de corruption avant l'opération. Pour l'acquéreur comme le cédant, les vérifications « anticorruption » peuvent avoir pour objet de déterminer le risque de sanctions pénales encouru par chacun d'eux à raison des faits commis antérieurement à l'opération par la cible. Ces vérifications « anticorruption » peuvent conduire l'acquéreur à renoncer à l'opération si les contrôles ont mis en évidence

(8) L. n° 2016-1691, 9 déc. 2016, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

(9) Avis relatif aux recommandations de l'Agence française anticorruption destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêts, de détournement de fonds publics et de favoritisme : *JO* 12 janv. 2021.

(10) CE, 30 mai 2007, n° 293423, *Sté Tradition Securities ad Futures*.

des risques majeurs. À l'occasion d'une opération transfrontière, ces analyses devront prendre en compte l'ensemble des législations applicables pour mesurer correctement le risque de sanctions pénales. Le principe est que seul l'auteur est responsable pénalement[11]. Toutefois, si des faits de corruption se poursuivent après l'absorption ou la fusion, ils pourront être imputés, dans les conditions prévues par l'article 121-2 du Code pénal, respectivement à la société absorbante ou à la nouvelle société résultant de la fusion. Le risque est d'autant plus grand depuis le revirement de la Cour de cassation concernant la responsabilité pénale de la société absorbante. Par un arrêt du 25 novembre 2020[12], intégrant les positions de la Cour de justice de l'Union européenne[13] et de la Cour européenne des droits de l'homme[14] sur le sujet, la chambre criminelle de la Cour de cassation écarte l'obstacle tiré de l'existence de la personnalité morale de chaque société, sur lequel se fondait jusque-là sa jurisprudence pour refuser d'engager la responsabilité pénale de la société absorbante pour des faits commis par la société qu'elle a absorbée. Elle a ainsi considéré qu'en cas de fusion-absorption entre sociétés anonymes ou sociétés par actions simplifiées, la société absorbante pouvait être condamnée pénalement à une peine d'amende ou de confiscation pour des faits constitutifs d'une infraction, commis par la société absorbée avant l'opération de fusion ou d'absorption.

Ces opérations de contrôle « anticorruption » s'incorporent pendant la phase d'étude du projet, et doivent se dérouler avant le *signing*, et par la mise à disposition de l'ensemble des éléments nécessaires. Il importe de rappeler que les informations échangées sur la société cible doivent satisfaire aux exigences de la bonne foi, conformément aux dispositions de l'article 1112 du Code civil. Par ailleurs, en application du premier alinéa de l'article 1112-1 du même code, « celle des parties qui connaît une information dont l'importance est déterminante pour le consentement de l'autre doit l'en informer dès lors que, légitimement, cette dernière ignore cette information ou fait confiance à son cocontractant ». En général, au cours des négociations, une lettre d'intention, signée par le cédant et la société intéressée, formalise leur volonté de mener l'opération à son terme, en rappelant les conditions de sa réalisation telles qu'elles ont été négociées. L'acquéreur et le cédant définissent conjointement les modalités de communication des informations demandées. À cette fin, le cédant peut créer une *data room*. L'accès aux informations les plus sensibles peut être limité aux personnes tenues à une obligation de confidentialité. En outre, le responsable des vérifications anticorruption peut envisager de réaliser des entretiens avec le cédant ou, si cela est possible, avec la cible. La création de la *data room* avant le *signing* permet aux parties de prendre connaissance, à titre confidentiel, de toutes les données de l'opération. Dans le cadre de ces contrôles préalables à l'opération, la sécurisation par le recours à la *blockchain* est une voie possible. Le recours à la *blockchain* dans l'organisation de la *data room* permet de faciliter la restructuration (I) tout en assurant la sécurité du secret des affaires (II).

(11) « Nul n'est punissable que de son propre fait » (par ex., Cons. const., 1er juin 2018, n° 2018-710 QPC).
(12) Cass. crim., 25 nov. 2020, n° 18-86.955.
(13) CJUE, 5 mars 2015, aff. C-343/13, *Modelo Continente Hipermercados SA*.
(14) CEDH, déc., 24 oct. 2019, n° 37858/14, *Carrefour France c/ France*.

## I. – La complémentarité de la *data room* avec la *blockchain*

La *data room* est un lieu fictif sur un serveur informatique qui a pour objet de centraliser l'ensemble des données à caractère économique, technique, financier, fiscal, social, juridique et réglementaire, mis à disposition des parties prenantes dans le cadre du processus de restructuration. L'accès à la *data room* peut être plus ou moins réglementé selon le degré de confidentialité souhaité. La *data room* contient des informations portant sur la réalisation d'audits sur l'ensemble de la vie juridique de la cible permettant de pointer les éléments sensibles dans l'évaluation de l'activité et notamment les droits de propriété intellectuelle et industrielle détenue par l'entreprise pharmaceutique ciblée, ou encore les *datas* qui constituent la valeur forte dans le secteur de la santé.

La réunion de ces informations et données confidentielles dans la *data room* est faite avant toutes opérations risquées que sont les restructurations quelle qu'en soit la forme.

La *blockchain* garantit la confidentialité de la *data room* et permet d'obtenir une sécurisation des relations entre les parties lors des transactions. En effet, la confiance repose sur le fait que les données contenues dans la *blockchain* sont immuables et intangibles, et ne peuvent être modifiées ou supprimées. Pour que la *blockchain* puisse obtenir cette confiance, elle doit respecter le règlement « eIDAS » n° 910/2014 du 23 juillet 2014[15].

Par ailleurs, la *blockchain* assure la simplification des opérations de restructuration. Il est possible de stocker les documents juridiques tels que les contrats commerciaux, des brevets ou des contrats de vente, afin de protéger les engagements des parties. La technologie de la *blockchain* appliquée à la *data room* facilite et accélère l'accès des informations destinées aux différentes parties. Il y a quelques années encore, les représentants des entreprises pharmaceutiques qui envisageaient une fusion-acquisition se rencontraient physiquement dans une pièce pour partager toutes les informations qu'ils détenaient sur leur structure (bilan financier, compte de résultat, litiges juridiques, audit de gestion, informations fiscales, gestion sociale de l'industrie, *etc.*). Dès lors, les juristes ainsi que les collaborateurs financiers se réunissaient dans une pièce pour des raisons de sécurité et ils étaient confrontés à une certaine lenteur dans l'étude des documents sous format papier. Désormais, avec la technologie *blockchain*, l'ensemble des documents sensibles sont accessibles aux personnes accréditées, sur une plateforme en ligne, ce qui a pour conséquence d'accélérer toute la procédure de restructuration, tout en garantissant la confidentialité. L'évolution numérique permet une accélération de la relation juridique en phase avec les nécessités de célérité sur le marché des affaires.

Cette accélération des relations ne sacrifie pas au respect des obligations entre les parties tenues à une stricte obligation de confidentialité. L'accès à la *data room* est extrêmement réglementé, pour des raisons de sécurité, tout comme dans la procédure traditionnelle, toutes les personnes ayant accès à cette chambre virtuelle sont soumises à des clauses de confidentialité.

(15) PE et Cons. UE, règl. (UE) n° 910/2014, 23 juill. 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

### II. – La sécurisation des données confidentielles de la *data room* par la *blockchain*

Lors de la restructuration, les acteurs du monde de la santé doivent prendre en considération les conséquences de la violation des données confidentielles(16). Le secret des affaires est un enjeu crucial pour les entreprises, et ce tout particulièrement dans le secteur des entreprises de santé. Le secret des affaires est constitué par tout ce qui n'est pas connu du secteur professionnel, qui est également valorisable compte tenu du fait que cette information est secrète et l'entreprise prend des mesures pour la protection de ces données.

Les entreprises pharmaceutiques les plus innovantes sont exposées à la violation de leurs secrets d'affaires par la fuite d'informations sensibles, l'espionnage industriel et la cybercriminalité. Au cours d'une opération de restructuration, cette violation des données peut être liée à une faille de sécurité dans leur *data room* entraînant de manière accidentelle ou illicite la destruction, la perte ou la divulgation non autorisée de données à caractère confidentiel. Il est donc indispensable pour les entreprises pharmaceutiques de rechercher la protection la plus efficace du secret des affaires notamment par le recours à un dispositif clé comme la *blockchain*. Cette procédure permet non seulement de conserver tous les actes, mais également de tracer tous les passages dans la *data room*. Elle constitue une forteresse infranchissable pendant une phase de négociation sensible, dont la durée peut s'étirer dans une période de sensibilité liée aux innovations scientifiques et médicales en cours.

Il convient enfin de préciser que depuis l'entrée en vigueur du règlement général sur la protection des données (RGPD)(17) en 2016, la pratique a fait naître un coefficient de conformité concernant la protection des données. Il permet à la société absorbante de connaître le niveau de sécurité des informations détenues par l'entreprise absorbée. Plus ce coefficient est bon, plus la valorisation de la société tend à augmenter. Grâce à cela, une société qui aspire à une restructuration veille précieusement à avoir une politique RGPD efficiente. Cela s'exprime notamment par l'intervention des *Data Privacy Officers* (DPO). Ce sont des agents internes ou externes à la société, qui vont s'assurer de l'application stricte du règlement européen. Ces agents contribuent eux aussi à la valorisation des industries et seront donc impliqués, avec les contrôleurs « anticorruption », dans la certification des informations déposées dans la *data room* à la connaissance des parties concernées.

## § 2. – L'usage de la *blockchain* dans la technique juridique de restructuration

En raison de la sensibilité des informations échangées, qui portent au-delà des informations classiques sur la situation juridique, économique, financière, sur des

(16) C. com., art. L. 151-1.

(17) PE et Cons. UE, règl. 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.

données sensibles de santé constituant la valeur réelle et potentielle de l'entreprise, le renforcement de la sécurisation des échanges au cours de l'opération de restructuration dans le secteur de la santé s'impose. Ce sont désormais ces données qui attirent toutes les convoitises dans le milieu de la santé, mais aussi sur le marché de la cybercriminalité, d'où la nécessité de mettre en place les techniques de verrouillage les plus efficaces sur le plan technologique et juridique. Cette utilisation de la *blockchain* doit être adaptée à la méthode de restructuration utilisée par l'entreprise par fusion, apport partiel d'actifs, prise de participation (I). Dans tous les cas, en raison de l'automatisation des procédures grâce à la *blockchain*, cela permet une indépendance des entreprises pharmaceutiques vis-à-vis des intermédiaires (II).

## I. – Le rôle de la *blockchain* dans les diverses méthodes de restructuration des entreprises pharmaceutiques

### A. – L'usage de la *blockchain* dans la restructuration par fusion

La restructuration d'une entreprise pharmaceutique peut passer par la fusion (C. com., art. L. 236-1). Sans revenir sur le procédé de la fusion, il convient de rappeler qu'elle entraîne une transmission universelle de patrimoine (TUP) d'une entreprise à une autre, avec une complexité particulière lorsque la fusion est transfrontalière[18].

Le projet de fusion, sur lequel les actionnaires des sociétés concernées se prononcent et mettent en œuvre la phase préparatoire de la fusion, est déterminant. Cette obligation de monter le projet de fusion est issue de l'article L. 236-6 du Code de commerce. L'article R. 236-1 du même code décrit le contenu du projet de fusion qui doit notamment contenir les motifs, buts et conditions de l'opération. La mise en œuvre des règles du droit des sociétés[19] pourrait alors être optimisée grâce au recours à cet outil numérique. Le projet de fusion peut entrer dans une *blockchain*, par l'usage du système de *smart contracts*, permettant de lister une série de conditions indispensables afin d'aboutir à la fusion, sans devoir recourir à des tiers intermédiaires. À la date de la fusion entre les sociétés concernées, les actifs et passifs des entreprises vont se confondre. La fusion entraînera la perte de l'existence juridique de la société absorbée. Son patrimoine, dans ses éléments actifs et passifs, sera transmis de façon universelle à la société absorbante. La transmission universelle a pour effet d'entraîner une dévolution automatique du patrimoine, sans altérer la substance du bien transmis, et cela n'implique pas l'information individuelle des créanciers et débiteurs de la société absorbée[20], à l'exception des contrats *intuitu personae* pour lesquels les cocontractants doivent être consultés. Dans le cadre d'une fusion, la technologie *blockchain* peut être utilisée comme un outil de constitution du projet de fusion, pour sceller définitivement l'accord de fusion tout en assurant le secret professionnel des parties, et la réalisation des opérations

(18) Dir. 2017/1132, 14 juin 2017 et C. com., art. L. 236-25 à L. 236-32.
(19) V. Magnier et P. Barban, *Blockchain et droit des sociétés*, Dalloz, coll. « Études », 2019.
(20) Cass. com., 28 juin 2017, n° 15-27.605 : *RJDA* 12/2017, n° 807.

préparatoires dans un temps accéléré plus en phase avec la célérité de l'innovation scientifique qui fonde la valeur des entreprises pharmaceutiques.

Cet outil permet également de favoriser la constitution d'une société plus rapidement et plus simplement dans l'hypothèse d'une fusion par création d'une société nouvelle. Toutefois, une problématique se pose lorsque la société absorbée utilise déjà la technologie de *blockchain* pour stocker les données médicales qui constituent une partie de sa valeur. La question se pose alors de déterminer comment la société absorbante peut recueillir la *blockchain* et les données médicales contenues dans celle-ci. La transmission universelle de patrimoine emporte automatiquement le transfert des biens de la société absorbée, la question de la transmission de l'outil numérique et donc de la construction numérique de la *blockchain* comme moyen mis en œuvre pour sécuriser les données se pose, au regard de la nature juridique de cette *blockchain*. Il s'agit de droits de propriété intellectuelle, en principe transmis comme les autres droits sous réserve de leur caractère *intuitu personae* qui exige le consentement des parties. Or, les droits d'accès aux données médicales résultent de conventions *intuitu personae* qui ne peuvent être transmises qu'avec l'accord et consentement des propriétaires des données. Dans les fusions du secteur de pharmaceutique sont concernées les données issues de la R&D et des essais cliniques en cours impliquant la collecte de données du patient. La question se pose alors de savoir comment transmettre ces données. En principe, les données de santé sont anonymisées ou pseudonymisées. La question du sort des données doit néanmoins être résolue afin d'assurer l'efficacité de cette utilisation numérique dans les opérations de restructuration.

Sur le point de savoir si les données personnelles sont des biens au sens des articles 527 à 536 du Code civil, le législateur français a refusé d'appliquer aux données personnelles le régime du droit de propriété prévu aux articles 544 et suivants du même code[(21)]. Le législateur français refuse de patrimonialiser les données personnelles, et ce malgré l'opposition de nombreux acteurs. Ce refus du législateur se justifie du fait de la valeur qu'elles représentent[(22)] vis-à-vis du droit fondamental de la personne qui rend inaliénables les données personnelles de manière définitive. En France, il est clairement interdit par l'article L. 4113-7 du Code de la santé publique de vendre les données médicales, même lorsque la personne donne son consentement. Cela démontre la volonté du législateur de rendre les données personnelles inaliénables même par leur propriétaire. En d'autres termes, il est impossible pour les personnes de céder les droits dont ils disposent sur les données. Le législateur souhaite éviter le marchandage de ces informations, tout comme il est interdit pour les patients/personnes de vendre les éléments constitutifs de leur corps. Cependant, les dispositions issues de l'avis de la CNIL sur le projet de texte qui a abouti à la loi du 13 août 2004[(23)] réformant l'assurance maladie, autorisent la cession des données médicales lorsque la cession n'est pas faite à titre commercial.

(21) É. Dufour, *La donnée est-elle un bien comme un autre ?*, DafMag, 19 déc. 2019.
(22) Les travaux du Think Tank « Génération libre » militent pour « une patrimonialité des données personnelles ».
(23) L. n° 2004-810, 13 août 2004, relative à l'assurance maladie.

Malgré cette exception prévue par la loi du 13 août 2004, le RGPD prévoit qu'il ne sera pas possible pour l'entreprise de détenir les données personnelles qu'à titre temporaire. En effet, il est important d'utiliser la notion de « détention », car elle relève du droit et le détenteur précaire ne tient pas son pouvoir de l'emprise matérielle que le détenteur exerce sur l'objet, mais du titre qui lui octroie le droit de détenir la chose. Concernant les données personnelles et médicales, il s'agit du contrat que l'investigateur ou le médecin a fait signer au patient pour recueillir son consentement et l'autorisation de l'usage de ces données. Le droit d'usage de ces données limité dans le temps sera transmis à l'entreprise absorbante.

À partir de la fusion, l'automatisation de l'article L. 236-14 du Code de commerce s'applique, les créanciers de la société absorbée, et/ou tout autre débiteur de ce dernier, deviennent ceux de la société absorbante[24]. Par conséquent, la ou les personnes dont les informations sont comprises dans une *blockchain* pourront rechercher la responsabilité de la société absorbante et faire valoir leurs divers droits prévus par le RGPD (Droit d'accès ; Droit de rectification ; Droit à l'effacement ; Droit à la limitation du traitement ; Droit à la portabilité des données ; Droit d'opposition) dans la mesure où les protections initiales des données ne seraient plus respectées. Mais, au-delà du cas du transfert des données de santé, éventuellement protégées dans une *blockchain*, l'organisation de l'opération de fusion grâce à l'utilisation de cette technique numérique permettra d'assurer la traçabilité, la sécurité, la confidentialité, la rapidité nécessaires au déroulement d'une opération internationale, en limitant les risques d'échec de l'opération dus notamment à la sincérité des résultats sur les opérations de recherche et développement en cours dans la société cible. L'opération de fusion traduit une confiance de l'absorbante dans le potentiel de développement de la société absorbée fondé sur la nature de ses recherches et les résultats potentiels attendus[25]. En ce sens, cet outil numérique permet de garantir que les éléments n'ont pas été modifiés au cours de la négociation, et d'en garder la trace dans une hypothèse de recours ultérieur entre les actionnaires.

### B. – Le rôle de la *blockchain* dans l'apport partiel d'actif

L'apport partiel d'actif est une méthode de restructuration consistant pour une société (apporteuse) d'effectuer un apport en nature à une autre société (bénéficiaire) portant sur une branche autonome d'activité. Cela provoque l'augmentation du capital de la société bénéficiaire. Cet apport n'entraîne pas la dissolution de la société apporteuse, celle-ci va continuer à exister, son patrimoine est affecté par la branche apportée étant elle-même remplacée par les actions de la société bénéficiaire. Dans le domaine de la société, il est possible de citer l'exemple de l'apport partiel de l'actif effectué par Diagnostic Médical Systems SA (société apporteuse) à Hybrigenics SA (société bénéficiaire) le 8 juin 2019[26].

(24) Cass. com., 28 févr. 2018, n° 16-18.692 : *BRDA* 7/2018, n° 1.
(25) T. Sanchez, *La blockchain et le secteur pharmaceutique*, Sciences du Vivant [q-bio], 2019.
(26) Projet de traité d'apport partiel actif, *Diagnostic Médical Systems SA (société apporteuse) à Hybrigenics SA (société bénéficiaire)*, 8 juin 2019.

Cet apport permet généralement aux entreprises pharmaceutiques qui commencent à prendre une certaine ampleur en termes de taille, de réaliser les opérations de filialisation, à savoir les opérations par lesquelles une société décide d'abandonner toute activité opérationnelle et de se cantonner dans le rôle de holding. Lorsqu'une société pharmaceutique dispose de deux grandes spécialités, notamment les médicaments et les dispositifs médicaux, elle peut créer deux filiales et partager les spécialités entre ces deux sociétés.

Par conséquent, lors de cet apport, il y a toute une procédure à suivre pour la société pharmaceutique ; la technologie *blockchain* pourrait favoriser toute la procédure et sécuriser cette opération notamment dans la répartition des actifs et passifs entre les filiales. En effet, en inscrivant directement la description des caractéristiques des sociétés ; les motifs et les buts de l'apport ; les méthodes d'évaluation utilisées (l'évaluation des éléments d'actif et de passif afférent à la branche d'activité apportée), mais également la description des apports (la désignation de l'actif et du passif apportés par la société apporteuse, la propriété et la jouissance, *etc.*) dans la *blockchain*, cela aurait pour conséquence d'automatiser les formalités *via* les *smart contracts*. De plus, la *blockchain* pourrait être utilisée pour la mise en œuvre des différentes stipulations statutaires et extrastatutaires automatiquement par le biais de la technologie des *smart contracts*.

En outre, l'apport partiel d'actifs permet la dislocation d'une entreprise en plusieurs entités. Afin de la sécuriser, l'entièreté de cette opération devra s'enregistrer au sein d'une *blockchain*. La société apporteuse contrôlera à 100 % les deux filiales et aura ainsi dans son patrimoine seulement les actions des filiales. La fusion des données de santé/médicales devra être inscrite dans cette *blockchain*, puis l'accès à ces données devra être partagé entre les deux filiales.

L'apport partiel d'actif peut mener à la création d'une filiale commune lorsque deux groupes décident d'unir leurs efforts et cessent de se concurrencer dans un segment précis. Ainsi, dans cette opération précise, il faudra que les entreprises pharmaceutiques mettent en commun des données de santé/médicales qu'elles détiennent pour la création de cette filiale.

Ces données ont une très grande valeur, issues pour la plupart des recherches cliniques effectuées par les sociétés apporteuses. De ce fait, il est primordial de sécuriser cette cession de données de santé à une nouvelle entreprise, tout en sachant que la seconde société apporteuse devra également apporter ses propres données de santé, entraînant ainsi la fusion de ces données. Il faudra également intégrer les accords initiaux ayant permis la création de cette filiale afin d'éviter tout conflit.

La scission relève du régime de la fusion. Elle a pour effet une dévolution du patrimoine : « Sauf dérogation expresse prévue par les parties, communauté ou confusion d'intérêts ou fraude, l'apport partiel d'actif emporte, lorsqu'il est placé sous le régime des scissions, transmission universelle de la société (apporteuse), la société bénéficiaire de tous les droits, biens et obligations dépendant de la branche autonome d'activité qui fait l'objet de l'apport »[(27)].

(27) Cass. com., 23 juin 2004 : *JCP* E 2004, 1774.

La transmission universelle est la même qu'en matière de fusion, elle s'opère de plein droit lorsque les biens, les droits et obligations se rattachent à la branche d'activité apportée. Les biens, droits ou obligations ne peuvent être écartées de la transmission que s'ils sont étrangers à la branche d'activité apportée[28] ou s'ils ont été exclus par la volonté expresse des parties.

Par ailleurs, la traçabilité a une importance concernant la responsabilité de la nouvelle société envers le propriétaire de ces données notamment pour déceler s'il y a une fraude dans l'obtention des données. Les responsables de traitement des entreprises pharmaceutiques sont assujettis à des obligations, et notamment la mise en place d'outils destinés à garantir la protection des données personnelles dès la conception du traitement ou par défaut[29], la désignation d'un délégué à la protection des données[30], l'obligation de tenir une documentation spécifique comme le registre des traitements, ainsi que l'obligation de notification des violations de données à l'autorité de protection et dans certains cas à la personne concernée[31].

Étant donné que l'apport partiel d'actifs entraîne le transfert universel du patrimoine vers la nouvelle filiale, plus précisément le transfert du droit d'usage des données médicales, cela entraîne également le transfert des obligations qui sont liées à ce droit d'usage.

En effet, les propriétaires des données et les autorités pourront légitimement se tourner vers la nouvelle société bénéficiaire. Toutefois, les sociétés donatrices restent solidairement tenues du passif remis à la société bénéficiaire ; cela sous-entend qu'il est important de pouvoir connaître, au moment venu, les données transmises par chacune des sociétés apporteuses.

### C. – Le rôle de la *blockchain* lors de la restructuration par prise de participation

La restructuration peut passer également par la prise de participation dont le régime est celui des acquisitions et transferts de droits sociaux. La participation peut prendre la forme d'un rachat d'actions de la société convoitée. Ce rachat peut provoquer une prise de contrôle, impliquant donc un changement d'actionnaires dominants. La restructuration par prise de participation est une méthode très courante sur le marché pharmaceutique. La technologie *blockchain* a un rôle à jouer dans la prise de participation par achat d'actions (l'achat direct des actions ou l'achat par le biais d'une holding) ou encore par la prise de participation par augmentation du capital.

La prise de participation concertée peut prendre deux voies, celle de l'achat des actions des actionnaires dominants, c'est ce qu'on appelle « la cession contrôlée » et celle de l'augmentation du capital réservée aux nouveaux arrivants. Dans le système traditionnel, les détenteurs d'actions transfèrent les actions en faisant appel à un intermédiaire centralisé qui effectue le règlement généralement dans un délai de trois jours.

(28) Cass. com., 20 janv. 2015, n° 14-10.010 : *RJDA* 4/2015, n° 275.
(29) RGPD, art. 25.
(30) RGPD, art. 37.
(31) RGPD, art. 30.

La technologie *blockchain* permet aux entreprises pharmaceutiques de réduire ce délai à moins d'une journée. L'utilisation des *smart contracts* permet de coder toutes les exigences concernant le transfert des actions numériques, de sorte que les engagements pris pour la restructuration par prise de participation soient automatiquement respectés. En l'absence des exigences posées par les *smart contracts* et contenus dans la *blockchain*, la restructuration ne pourra pas avoir lieu. Le vote et autres opérations de société pourraient être simplifiés et les audits rationalisés. Les autorités pourraient également bénéficier d'un accès et d'une transparence en temps réel.

Les investissements dans les entreprises pharmaceutiques peuvent se faire *via* ces cryptoactifs. L'Autorité des marchés financiers met en garde les investisseurs qui souhaitent faire des investissements en cryptoactifs, contre les escroqueries fréquentes sur Internet. Il existe des intermédiaires pour sécuriser les transactions, c'est l'exemple des prestataires de services sur actifs numériques (PSAN)[32]. Recourir à des intermédiaires représente un coût et une procédure qui peut prendre un certain temps. Pour éviter ces intermédiaires, la technologie *blockchain* représente une solution alternative.

Il convient de préciser dans ces opérations à caractère international que les réglementations diffèrent concernant la reconnaissance des opérations capitalistiques au travers de ces outils numériques. Ainsi l'État de Delaware[33] aux États-Unis a modifié le *General Corporation Law*[34], et prévoit la possibilité d'émettre et de suivre des actions sur une *blockchain*. Les modifications doivent également permettre aux sociétés et aux actionnaires de profiter des avantages de la négociation électronique, tout en conservant la propriété de leurs actions. Les changements juridiques ont été établis par le biais d'amendements régis à l'article 219, le registre des actions doit être défini pour inclure les registres administrés au nom de la société pour permettre un système de tenue de registres utilisant des bases de données *blockchain*. Ainsi, les actions *blockchain* seront légalement considérées comme une forme de titre sans certificat.

Cette réforme prévoit désormais que l'ensemble des registres de la société sont conservés sur « un ou plusieurs réseaux ou bases de données électroniques ». La *blockchain* doit assurer la production d'un registre des actionnaires de la société, enregistrer certaines informations et garantir le transfert d'actions. En effet, la nature immuable des *blockchains* permet de combiner les avantages de l'unicité des actifs numériques et la certitude de la propriété avec la commodité de l'émission et du transfert électronique. Dans le cadre de la restructuration par le rachat des actions de la société convoitée, la *blockchain* pourrait *via* les *smart contracts*, ou les contrats intelligents lorsqu'une transaction est ajoutée à la *blockchain*, être validée par les utilisateurs. Une fois la certification effectuée, la transaction rejoint la *blockchain*, se retrouvant ainsi inscrite au sein de ce grand livre. Les *smart contrats* sont des programmes créés dans l'optique de faire exécuter directement et automatiquement

(32) AMF, *Investir en cryptoactifs : quel professionnel choisir ?*, 30 déc. 2020.
(33) Allen & Overy, *Delaware Passes Law Permitting Companies to Use Blockchain Technology to Issue and Track Shares*, 26 sept. 2017.
(34) The Delaware Code Online, *General corporation law*.

certains actes. La réalisation d'une condition ou la réunion des éléments nécessaires pour réaliser une action ou un résultat permettra de faciliter la politique de restructuration des entreprises pharmaceutiques.

## II. – La *blockchain* : l'instrument de l'indépendance des entreprises pharmaceutiques

La surveillance par la technologie *blockchain* de toutes les étapes permettrait un meilleur contrôle de ces opérations, car très souvent elles se font contre l'avis des dirigeants[35]. L'ordonnance du 8 décembre 2017[36] relative à l'utilisation d'un dispositif électronique partagé pour la représentation et la transmission des titres financiers ouvre la porte à des possibilités d'achat et de vente d'actions d'entreprises par voie numérique. La *blockchain* est similaire à un grand registre numérique ; de ce fait, elle contient l'intégralité des transactions entre les personnes qui appartiennent au réseau. Cela permettrait aux entreprises pharmaceutiques de supprimer les organes de contrôle ou l'intervention d'un tiers de confiance. Les utilisateurs pourront modifier la *blockchain* en ajoutant de nouvelles transactions. Toutefois, grâce au caractère immuable, il ne sera pas possible pour les actionnaires de l'entreprise pharmaceutique de procéder à la suppression des précédentes inscriptions validées par les utilisateurs. Cela permet d'effectuer des transactions parfaitement sécurisées.

Il sera possible d'analyser l'évolution des droits des actionnaires, mais également l'arrivée et le départ des actionnaires, permettant de retracer les transactions et d'accéder aux données et aux modifications. Cette technique permet également de suivre et garantir le respect des pactes d'actionnaires, concomitamment au transfert des titres[37]. Il sera également possible pour les utilisateurs de mettre en place un système de sécurité, en instaurant un consensus de validation *via* la *blockchain*. Ce consensus permettra de contrôler et de valider les nouvelles transactions, en application du règlement (UE) n° 2019/452[38] portant sur le filtrage des investissements étrangers. Les actionnaires majoritaires d'une entreprise pharmaceutique pourront se protéger de possibles atteintes contre l'indépendance de leur entreprise.

L'utilisation de la *blockchain* dans un objectif de sécurisation des opérations sur le capital d'une société pharmaceutique découle d'une conservation des titres non cotés présentant de nombreuses difficultés pour les *startups*. En effet, les sociétés pharmaceutiques ont l'obligation de tenir un registre de leurs titres, ceci pour éviter la falsification. L'ordonnance n° 2017-1674 du 8 décembre 2017 et le décret n° 2018-1226 du 24 décembre 2018[39] ouvrent la possibilité pour les entreprises de faire appel à un « dispositif d'enregistrement électronique partagé ». Les titres de ces sociétés pharmaceutiques pourront être enregistrés sur la *blockchain*, transmis et

(35) A. Viandier, *OPA, OPE et autres offres publiques*, F. Lefebvre, 5e éd. 2014.
(36) Ord. n° 2017-1674, 8 déc. 2017, relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.
(37) G. Bouillet-Cordonnier, E. Lamazerolles, J.-M. Moulin et M.-A. Godot-Sorine, *Pactes d'actionnaires et privilèges statutaires*, EFE, sept. 2020.
(38) PE et Cons. UE, règl. (UE) n° 2019/452, 19 mars 2019, établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union.
(39) D. n° 2018-1226, 24 déc. 2018, relatif à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons.

nantis comme le prévoit l'article L. 211-20 du Code monétaire et financier. La *blockchain* permet ainsi aux sociétés pharmaceutiques une inscription intangible et inaltérable des transactions. L'ordonnance n° 2017-1674 du 8 décembre 2017 octroie à cette inscription de titres dans une *blockchain* les mêmes effets qu'une inscription en compte de titres financiers.

SECTION 2

## L'UTILISATION DE LA *BLOCKCHAIN* DANS L'ORGANISATION DES ACTIVITÉS DES ENTREPRISES, OBJET DE LA RESTRUCTURATION

L'industrie pharmaceutique, tout particulièrement dans une perspective de restructuration interne ou externe, doit intégrer l'évolution numérique afin de renforcer sa valorisation sur le marché. Le concept de la technologie *blockchain* renvoie à la notion d'efficience. En effet, ce système accroît la qualité de la gestion des diverses activités de l'entreprise pharmaceutique.

Le système des *blockchains* permet des gains de productivité et d'efficacité. En effet, il est possible de stocker des documents juridiques tels que les contrats commerciaux, des brevets, des contrats de vente ou encore les données relatives à la recherche clinique, cela dans le but de sécuriser les engagements des parties. Cette technique permet la suppression de certains intermédiaires qui deviennent inutiles du fait de l'automatisation des relations entre les parties. Enfin, en cas de litige, la traçabilité des documents inscrits dans les blocs de chaîne permet de constituer les preuves nécessaires.

La *blockchain* peut être utilisée comme un instrument permettant le financement des nouveaux projets des entreprises pharmaceutiques *via* les *Initial Coin Offering* (§ 1). Une proposition de règlement de la Commission européenne du 24 septembre 2020 a été déposée pour harmoniser les réglementations de financement numérique sur tout le territoire de l'Union européenne, permettant ainsi aux entreprises et *startups* de bénéficier de nouvelles sources de financement (§ 2).

### § 1. – Le financement des entreprises *via* la technologie *blockchain*

La révolution numérique touche le mode de financement des entreprises, notamment par la possibilité pour les entreprises pharmaceutiques de recourir aux minibons *via* la *blockchain* ou encore les *Initial Coin Offering* (ICO) qui est un outil permettant le financement des nouveaux projets pharmaceutiques. Du fait de l'interdiction de l'ICO sauvage, le législateur a prévu la possibilité de recourir à *utility token via* la *blockchain* pour une levée de fonds (I). Le financement des entreprises pharmaceutiques *via* les cryptoactifs suppose également une fiscalité particulière (II).

## I. – Les techniques de recours aux financements numériques dans l'industrie pharmaceutique

### A. – La possibilité pour les entreprises pharmaceutiques de recourir aux minibons *via* la technologie *blockchain*

La *blockchain* est à l'origine un outil de financement pour les entreprises, c'est un mécanisme de coordination et d'attribution de crédit. Elle encourage les agents économiques à collaborer *via* un réseau de confiance absolue pouvant être utilisé seulement par les personnes accréditées. Cette technologie améliore la cohésion et l'efficacité de toute la communauté.

Les articles L. 223-6 à L. 223-12 du Code monétaire et financier permettent l'émission et la cession de minibons qui sont des titres de créance émis par un État ou par une banque. Les minibons permettent à l'entreprise pharmaceutique de pouvoir accéder à un financement faisant appel à un large public. Toutefois, l'article L. 223-12 du Code monétaire et financier est issu de l'ordonnance n° 2016-520 du 28 avril 2016, qui prévoit la possibilité de l'utilisation de la *blockchain* en matière de « minibons ». L'ordonnance la définit comme étant un dispositif d'enregistrement électronique partagé permettant l'authentification des opérations d'émission et de cession des minibons.

Les minibons permettent d'effectuer un placement pour une durée de cinq ans maximum. Ils sont notamment utilisés sur les plateformes de financement participatif. Toutefois un groupe de travail devra déterminer les conditions de réalisation d'un tel projet pour garantir que la technologie est assez sûre et mature pour assurer la tenue d'un registre électronique distribué fiable, sécurisé et susceptible d'être audité, ce qui est le cas pour la technologie *blockchain*. Cette technologie induit un coût de transmission minime pour les entreprises pharmaceutiques lorsqu'elles veulent recourir au financement par un large public.

### B. – Le financement des entreprises pharmaceutiques *via* l'émission de jetons *Initial Coin Offering*

*Initial Coin Offering* est un outil de financement des nouveaux projets pharmaceutiques. Dans la section dédiée à l'amélioration et la diversification des modes de financement, l'article 26 relatif à la création d'un régime des offres de jetons dispose qu'il serait possible *via* les offres initiales de jetons numériques, d'améliorer le financement des entreprises. Cela vaut également pour les entreprises pharmaceutiques et les laboratoires.

Cependant, le système de jetons numériques nécessite le dispositif d'enregistrement électronique partagé particulièrement *via* la technologie *blockchain*. L'étude d'impact a révélé que dans le courant de l'année 2017, plus de 4 milliards de dollars ont été levés par le biais de la *blockchain*.

Cet essor dynamique, conforté sur les premiers mois de l'année 2018, traduit l'attrait de ce nouveau mode de financement et d'investissement, en particulier au sein de l'écosystème *blockchain* mais aussi, plus largement, pour les entreprises innovantes comme les *startups* pharmaceutiques qui souhaitent attirer de nouvelles

catégories d'investisseurs ou de clients, selon des modalités inédites. Toutefois, cette étude d'impact reconnaît que la technologie et les opérations échappent au cadre juridique clair, c'est-à-dire qu'il y a une nécessité d'adapter les normes existantes à l'évolution technologique.

La situation dans les autres pays n'est pas si différente de celle de la France. En raison du caractère nouveau de cette technologie, aucun pays n'est aujourd'hui doté d'un cadre juridique dédié à cette technologie et à cette méthode de *fund raising*. Cependant, des pays comme la Suisse ou l'Allemagne ont mis en place des règles de bonnes pratiques, notamment dans le cadre pénal, afin de lutter contre le blanchiment. Ce flou juridique qui entoure les règles applicables à la technologie *blockchain* concernant la levée de fonds procure un sentiment d'insécurité chez les potentiels investisseurs.

Le terme de « dispositif d'enregistrement électronique partagé » (DEEP), employé dans l'habilitation, correspond à la technologie *blockchain*. Cette technologie est désignée par les dispositions de l'article L. 223-12 du Code monétaire et financier relatives aux minibons, introduites par l'ordonnance de 2016. La désignation « DEEP » reste cependant, très large et neutre vis-à-vis des différents procédés pour éviter l'exclusion des développements technologiques ultérieurs.

Toutefois, la dénomination « DEEP » recouvre les caractéristiques principales de la *blockchain*, notamment sa vocation à être un registre et son caractère partagé. Cette ordonnance a notamment permis de conférer l'inscription d'une cession de titres financiers dans une *blockchain*, mais également l'inscription des émissions de titres financiers dans la même *blockchain*. Cette inscription produit des effets équivalents à ceux d'une inscription traditionnelle en compte de titres financiers. Toutefois, cette ordonnance n'a en aucun cas créé une nouvelle obligation et n'a pas pour vocation d'alléger les garanties relatives à la représentation et à la transmission des titres. Cependant, les dispositions du Code monétaire et financier ainsi que du Code de commerce relatives aux titres financiers ont été ajustées pour intégrer cette innovation et permettre le recours à ce procédé.

La *blockchain* est un nouvel outil de financement des entreprises pharmaceutiques, car elle a permis l'émergence d'un nouveau mode de financement, notamment par l'émission de jetons *Initial Coin Offering*. Ce mode de financement s'oppose à l'*Initial Public Offering* (IPO) qui consiste en une levée de fonds sous forme d'actifs numériques en cryptoactifs, tandis que l'ICO n'offre aucun droit sur la gouvernance ou sur les résultats financiers. L'ICO est utile pour les *startups* pharmaceutiques, car elle permet le financement d'une idée au stade embryonnaire de la recherche et développement. Ainsi, cela évite aux *startups* de diluer leur capital et a pour effet de financer plus facilement le projet et de créer une communauté autour du projet de recherche.

Toutefois, les ICO accordent très peu de droits au porteur ; en effet, ces levées ne sont pas centralisées, elles échappent *de facto* à une régulation, donc elles évitent un processus de contrôle et peuvent être utilisées également comme un outil de blanchiment d'argent. De plus, la volatilité des cryptoactifs rend les opérations difficiles.

Mais les entreprises du secteur de la pharmaceutique peuvent se rassurer, car la loi PACTE du 9 octobre 2018 prévoit que certaines offres de jetons peuvent porter

le visa de l'Autorité des marchés financiers. Ce visa est un label (facultatif) que la société pharmaceutique émettrice peut solliciter, mais ce n'est pas une obligation. Pour obtenir ce visa, la société pharmaceutique doit établir un document d'information contenant des informations sur l'émetteur et sur l'offre de jetons. L'Autorité des marchés financiers (AMF) va procéder à la vérification des informations fournies par la société pharmaceutique émettrice. Le visa indiquera alors que l'AMF a vérifié que le document d'information de cette offre est complet et compréhensible pour les investisseurs. Ce visa sera présent dans la *blockchain* accessible aux investisseurs afin de garantir l'authenticité et la véracité des jetons.

### C. – La valeur d'un *utility token* dans la levée de fonds

Étant donné que les ICO sauvages ne sont plus possibles du fait de la loi PACTE, la méthode de levée de fonds fonctionne désormais *via* l'émission d'actifs numériques échangeables contre de la cryptomonnaie (cryptoactifs). L'actif numérique émis par une entreprise utilisant la *blockchain* peut être échangeable sur la *blockchain* de façon instantanée et sécurisée[40]. En effet, les jetons peuvent être échangés de pair-à-pair sans le consentement d'un tiers, comme une banque. L'opération est infalsifiable, et est personnalisée par l'entreprise pharmaceutique qui l'a créée pour être utilisée sur une application.

Les jetons sont très liquides, c'est-à-dire qu'ils peuvent être vendus à tout moment selon le prix délimité par le marché, puis utilisés lors de toutes les levées de fonds liées à des projets *blockchain*. Il existe deux types de jeton *token* : d'une part, les *security token* qui ne sont que de purs actifs financiers et représentent un investissement au sein d'une entreprise dans l'attente d'un profit ; d'autre part, les *utility token* ayant pour but final d'être utilisés dans le cadre d'un service spécifique, échangeables sur une *blockchain*.

## II. – La fiscalité des cryptoactifs

Le projet de loi de finances de 2019[41] a permis de révolutionner la fiscalité des cryptomonnaies (cryptoactifs). En l'occurrence, elles étaient considérées comme étant des valeurs mobilières classiques et taxées comme telles. Désormais, les cryptoactifs disposent d'une fiscalité qui leur est propre. Depuis cette loi de finances, les personnes disposant de cryptoactifs ont l'obligation de calculer et déclarer leurs gains imposables en cryptoactifs.

L'article L. 54-10-1 du Code monétaire et financier dispose que les actifs numériques comprennent les bons de caisse mentionnés à l'article L. 223-1 et les jetons mentionnés à l'article L. 552-2 du même code, sauf ceux remplissant les caractéristiques des instruments financiers mentionnés à l'article L. 211-1 du Code monétaire et financier. Dans son deuxième alinéa, l'article L. 51-10-1 dudit code élargit la définition à toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas forcément

(40) R. Chiaramonte, *Blockchain : utility token, le jour de gloire est-il arrivé ? : Forbes* 10 sept. 2018.
(41) L. fin. pour 2019, n° 2018-1317, 28 déc. 2018.

attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est toutefois acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.

Auparavant, les cryptoactifs étaient appréciés comme des biens meubles, et donc soumis à une taxation des plus-values de 36,2 % qui intervenait à chaque cession. Désormais l'article 150 VH bis du Code général des impôts prévoit une taxation à 30 % de la plus-value globale des actifs numériques. Il y a également la possibilité de recourir à une imposition au barème de l'impôt sur le revenu assorti de 17,2 % des prélèvements sociaux, si cela est plus avantageux. De plus, il y a un abattement de cession de 305 € par an si l'investisseur enregistre une plus-value égale ou inférieure à ce montant. Ces dispositions concernent tous les portefeuilles numériques[(42)] ; l'investisseur particulier devra prendre en compte l'ensemble des *wallets* détenus sur toutes les plateformes utilisées, tous cryptoactifs confondus, possédés et échangés au cours de l'année, pour déterminer le montant de ses plus-values imposables.

La loi de finances de 2019[(43)] n'applique aucune fiscalité sur les transactions entre les actifs numériques. Ce qui est positif, car cela permettra de conserver le caractère liquide, qui fait la particularité et l'intérêt du système des cryptoactifs. Ce mode de financement présente un intérêt certain pour les entreprises pharmaceutiques. En effet, l'administration fiscale encourage ce mode de financement avec un taux d'imposition revu à la baisse. Le passage d'un cryptoactif vers un autre cryptoactif ne sera pas fiscalisé, le fait générateur de l'imposition sur les gains réalisés interviendra seulement au moment de sa transformation fiduciaire.

L'administration fiscale imposera les éventuelles plus-values ou les moins-values qui auront été réalisées lors de la conversion des cryptoactifs en une devise ayant une reconnaissance légale ou sur les plus ou moins-values réalisées à l'occasion d'un échange des cryptoactifs contre un bien autre qu'un actif numérique. Les plus ou moins-values réalisées lors de chaque opération imposable sont calculées par rapport au prix de cession des cryptoactifs diminué d'une fraction du montant dépensé pour l'acquisition de ces cryptoactifs.

Les plus ou moins-values issues de cession de cryptoactifs devront être indiquées dans la déclaration de revenus dans la case « Plus ou moins-values sur actifs numériques »[(44)].

## § 2. – L'évolution de la réglementation européenne de la finance numérique

La finance numérique, qui représente une opportunité économique de premier ordre, n'est pas soumise à une réglementation européenne uniforme, créant ainsi

(42) Boursorama, *Cryptoactifs, Bitcoin : quid de la fiscalité sur les plus-values ?*, 8 févr. 2021.
(43) O. Placard, *Loi de finances 2019, quelle fiscalité en matière de cession de cryptoactifs ?*, Blog Happy-Capital, 8 janv. 2019.
(44) Formulaire n° 2086.

des clivages normatifs sur le territoire de l'Union européenne. Afin d'uniformiser le droit applicable à la finance numérique, la Commission européenne a présenté une proposition de règlement le 24 septembre 2020 (I). Cette proposition de règlement a pour objet de régulariser des outils financiers numériques tels que les *stablecoins* ou encore les *security tokens*, qui pourraient aider les entreprises du secteur pharmaceutique à trouver des investissements plus aisément (II).

## I. – La proposition réglementaire du 24 septembre 2020 portant sur une première régulation des méthodes de financement numérique

La pandémie de Covid-19 a révélé que les entreprises, qu'elles soient pharmaceutiques ou non, sont très dépendantes des technologies de l'information et de la communication pour garantir l'accès à distance aux services financiers. En effet, courant 2015 les transactions numériques effectuées *via* les technologies mobiles étaient de 20 % et, avec l'impact de la Covid-19, ces transactions numériques sont passées à 66 % au cours du premier semestre 2020[45]. Les investissements dans les nouvelles technologies ont augmenté du fait de l'utilisation de plus en plus importante des technologies mobiles lors des transactions monétaires ou encore pour la réalisation d'investissements financiers.

La Commission européenne a pris en considération l'importance de la finance numérique. Elle s'est prononcée le 24 septembre 2020 en publiant plusieurs textes qui mettent en évidence la stratégie économique de l'Union européenne. La proposition de la Commission européenne est fondée sur l'article 114 du Traité sur le fonctionnement de l'Union européenne (TFUE) visant à lever les obstacles à l'établissement et à l'amélioration du fonctionnement du marché intérieur.

Les propositions issues de ce règlement apportent un encadrement aux cryptoactifs, qui étaient encore jusqu'à présent très peu régulés par le droit de l'Union européenne[46] et laissés au pouvoir discrétionnaire des États membres. La Commission européenne souhaite ainsi saisir les opportunités offertes par la finance numérique pour revitaliser et relancer l'économie européenne. En effet, la finance numérique pourrait permettre aux consommateurs d'accéder à des produits financiers comme les *security tokens* émis par une *startup* pharmaceutique, permettant ainsi de moderniser l'économie européenne pour en faire un acteur numérique incontournable à l'échelle mondiale.

Cela représente une aubaine pour les jeunes *startups* pharmaceutiques qui peuvent ainsi espérer trouver des investisseurs plus aisément. En effet, la finance numérique débloque de nouveaux moyens de canaliser les financements vers les entreprises de l'UE et notamment les petites et moyennes entreprises[47]. Les *startups*

(45) C. Cartaud, *Fraud and identity*, EMEA, LexisNexis Risk Solutions.

(46) Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) n° 1060/2009, (EU) n° 648/2012, (EU) n° 600/2014 and (EU) n° 909/2014 – COM(2020)595. Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, COM(2020) 594.

(47) Communication from the Commission to the european Parliament, the Council, the european economic and social Committee and the Committee of the regions, On a Digital Finance Strategy for the EU, 24 sept. 2020.

pharmaceutiques ont généralement besoin de fonds très rapidement afin de pouvoir innover sur le marché de la santé. Cependant, les investisseurs sont réticents à investir *via* la voie numérique, car il n'existe pas de norme européenne uniforme encadrant sur tout le territoire de l'Union le financement numérique. Pour contourner ces obstacles, les entreprises pharmaceutiques pourraient, avec ce projet de règlement, recourir à des produits financiers innovants, qui représentent un coût moins important, car la *blockchain* met en relation directe les entreprises pharmaceutiques avec les investisseurs sans recourir à des intermédiaires qui représentent un coût et les acteurs réalisent un gain de temps lors de leurs transactions. Le projet de règlement permettra de simplifier et de banaliser les activités d'investissement *via* ces nouveaux outils d'investissements.

La Commission européenne a défini quatre grandes priorités :

– premièrement, supprimer la fragmentation du marché unique numérique afin d'apporter une sécurité juridique avec un cadre juridique solide définissant clairement le traitement réglementaire applicable à tous les cryptoactifs non couverts par la législation existante sur les services financiers ;

– deuxièmement, adapter le cadre réglementaire de l'Union européenne pour faciliter l'innovation numérique ;

– troisièmement, instaurer des niveaux appropriés de protection des investisseurs et d'intégrité du marché et promouvoir une finance axée sur les données ;

– quatrièmement, relever les défis et les risques liés à la transformation numérique en renforçant la résilience opérationnelle numérique du système financier.

Cette proposition de règlement européen sur les marchés de cryptoactifs prévoit :

– un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, comme la technologie *blockchain* ;

– une proposition sur la résilience opérationnelle numérique à l'attention des services financiers. Cette proposition s'appuie notamment sur des exigences déjà en vigueur dans le domaine de gestion des risques liés aux technologies de l'information et de la communication (TIC). Cette proposition a pour objet d'harmoniser les règles de gestion des risques liés aux TIC dans tous les États membres de l'Union européenne.

Cette proposition de règlement fait directement référence à la technologie *blockchain* et à son usage dans le domaine financier : « Les cryptoactifs sont l'une des principales applications de la technologie de la chaîne de blocs dans le domaine financier » et le mode d'investissement traditionnel se voit bousculé par l'avènement des « jetons de valeur stable de niveau mondial ». Les cryptoactifs sont des représentations numériques de valeur ou encore de droits, qui sont transférés et stockés sur une base de données électronique. Cette proposition de règlement est une opportunité pour les petites et grandes entreprises pharmaceutiques qui font face à la nécessité d'innover et à un besoin toujours plus important d'investissement financier résultant des coûts de l'innovation. En effet, la spécificité du secteur de la santé impose des contraintes budgétaires et légales pour encadrer les investissements financiers. Les entreprises pharmaceutiques, du fait de la complexité de leur secteur, ont recours à des financements internes plutôt qu'au marché des

actions pour financer leur programme de recherche et développement (R&D). Toutefois, cela n'est pas toujours possible et pourrait entraîner des risques de sous-investissement.

Cette proposition de règlement comporte également des garanties, notamment en imposant des exigences en matière de capital, la garde des actifs et une procédure obligatoire de dépôt de plainte pour les investisseurs. Les émetteurs de cryptoactifs adossés à des actifs importants seront soumis à des exigences plus strictes en matière de capital, de gestion des liquidités et d'interopérabilité.

Ces prépositions réglementaires pourront permettre aux entreprises pharmaceutiques d'évoluer vers de nouveaux outils de financement numériques pour éviter les risques de sous-investissement, sécurisés, rapides et leur permettront également de faire face aux nouvelles exigences du marché numérique à tous les stades de l'activité, notamment dans le secteur de la santé.

## II. – Les *stablecoins* et *security tokens* comme outils de financement numérique des entreprises pharmaceutiques

Le projet de règlement portant sur « les marchés sur cryptoactifs », encore appelé « MiCA », a pour objectif d'harmoniser les législations nationales en les remplaçant. Ce projet de règlement entraîne une véritable « tokénisation » des actifs financiers traditionnels, avec par voie de conséquence l'utilisation de la *blockchain* dans les services financiers des entreprises pharmaceutiques pour acquérir des investissements.

La proposition de règlement du 24 septembre 2020 de la Commission européenne inclut dans son périmètre un sous-ensemble relativement nouveau de cryptoactifs appelés « jetons de valeur stable » ou encore *stablecoins*. Ces jetons stables sont susceptibles d'être massivement utilisés et de devenir systémiques. Les jetons de valeur stable sont des nouvelles formes de monnaies digitales et leur traitement juridique (émission et échange de *stablecoins*) est également précisé dans le MiCA. La proposition réglementaire précise également qu'elle garantira la proportionnalité par sa conception, et cela en distinguant chaque type de services et d'activités en prenant en compte les risques associés afin que la charge administrative applicable soit proportionnée aux risques encourus en imposant des exigences les plus strictes pour les *stablecoins*. Ces derniers pourraient jouer un rôle important dans le financement des entreprises pharmaceutiques, notamment sur le plan fiscal. En effet, la fiscalité influence les entreprises pharmaceutiques dans la prise de décision de l'investissement *via* le mode de financement en rendant possible l'achat de ses actions par des *stablecoins*. En effet, pour les *stablecoins* il n'y a pas d'imposition dans le cas de conversion de cryptoactifs contre un *stablecoin*. Cette imposition aux investisseurs n'est pas imposable car elle ne génère pas de plus ou moins-value.

Dans le cas où ces *stablecoins* viendraient à être considérés comme étant des cryptoactifs non couverts par la législation existante de l'Union en matière de services financiers, la Commission prévoit certaines options. Par exemple, l'une de ces options porte sur le régime législatif sur-mesure pour répondre aux risques présentés par les *stablecoins* et les *global stablecoins*. Cette législation permettrait

de remédier aux vulnérabilités que pourraient créer les *stablecoins* pour la stabilité financière, en imposant des obligations d'information spécifiques aux émetteurs de *stablecoins* et de soumettre à certaines exigences la réserve à laquelle est adossé le *stablecoin*.

Le projet de réglementation européenne prévoit la création d'un dispositif de « régime pilote » pour le marché des jetons financiers *tokens* inscrits et échangés en *blockchain* ou *security tokens* avec un régime d'exemptions ciblées pour le marché de ces produits conditionnés à des limites de volume.

Les *security tokens* sont l'équivalent numérique d'une prise de parts de capital dans une entreprise. En utilisant les *security tokens*, les investisseurs peuvent s'attendre à ce que leurs parts de propriété soient préservées sur le « Grand Livre » de la *blockchain*. Par leur capacité à démontrer leur valeur financière, les *security tokens* sont susceptibles de faire évoluer les marchés financiers traditionnels vers de nouveaux modèles de *blockchains*. Les *security tokens* sont des instruments financiers et ils représentent une part d'une entreprise ou d'un actif. Ces jetons affichent les informations sur la propriété sur la *blockchain* qui protège les jetons de la fraude et de l'utilisation abusive. Il existe trois types de *security tokens* :

– les jetons d'équité, qui sont similaires aux actions traditionnelles. Ils représentent les actions par une entreprise, mais sont enregistrés sur la *blockchain*. Les propriétaires de ces jetons sont des ayants droit à une part des bénéfices de la société ;

– les *debt tokens* sont des titres de créance qui comprennent des hypothèques immobilières et des obligations d'entreprises. Ils représentent le capital levé par la dette et ils peuvent être comparés à un prêt consenti à l'émetteur ; les propriétaires des *debt tokens* ont droit au remboursement du principal et des intérêts périodiques ;

– les *asset backed tokens* représentent la propriété d'un actif spécifique tel que l'immobilier ou les matières premières.

Le projet de réglementation vient combler l'absence de réglementation sur les *utility tokens*. Cette absence signifie que les entreprises pharmaceutiques qui lèvent des capitaux peuvent aujourd'hui contourner le financement institutionnel mais également les coûts. En effet, pour les entreprises ou les *startups* du secteur de la pharmaceutique, les *security tokens offering* sont un moyen simple et relativement peu coûteux de lever des capitaux. Les *security tokens offering* offrent aux investisseurs un moyen d'investissement direct, sûr et transparent dans l'entreprise ou *startup* pharmaceutique.

Pour les *startups* pharmaceutiques qui viennent d'être introduites en bourse, cette place de marché secondaire pourrait apporter une source de liquidité au marché existant de ces actifs. En effet les entreprises, qu'elles soient pharmaceutiques ou non, mettent généralement plus de dix ans avant de pouvoir se prévaloir de leurs droits sur les actions. La *blockchain* offre un marché où ces droits peuvent être achetés et vendus de manière transparente, au bénéfice des détenteurs de droit.

Les entreprises pharmaceutiques ont plusieurs raisons de privilégier ce mode de financement numérique. Tout d'abord, si ces entreprises souhaitent lever des fonds, elles peuvent le faire *via* les *security tokens*, mais les entreprises devront se

conformer à la réglementation et divulguer certaines informations importantes sur leurs activités en publiant un prospectus pour augmenter la transparence. Cette transparence est garantie par la technologie *blockchain*. L'efficacité et la rapidité du processus des *security tokens* sont adossées à des actifs réels. Cela facilite l'évaluation de leur valeur. Enfin, les entreprises pharmaceutiques auront moins besoin de recourir à des intermédiaires qui représentent des coûts importants. Les *security tokens* rendent le processus plus efficace et minimisent les sources d'erreur.

Les *security tokens* offrent également des avantages sur le plan fiscal. En effet, cet outil de financement numérique représente un intérêt pour l'investisseur, qu'il soit une personne physique (l'opération est non imposable) ou une personne morale. Une particularité existe pour l'investisseur personne morale : lors de l'attribution des *security tokens*, l'opération est considérée comme étant fiscalement neutre et par voie de conséquence non imposable. Toutefois, si la cession entraîne une plus-value, la cession sera imposée au titre des cessions de valeurs mobilières, mais il existe des abattements qui peuvent être de 50 % de la plus-value entre deux et huit ans de détention et de 65 % au-delà de huit ans de détention.

Ces jetons peuvent être échangés 24 heures sur 24, 7 jours sur 7 avec une simple application mobile. Les *security tokens* sont un outil idéal pour les *startups* qui souhaitent lever des capitaux au lieu de se reposer sur le financement coûteux du capital-risque ou des investisseurs providentiels. Cet outil vient diversifier les possibilités pour les entreprises pharmaceutiques de faire des levées de fonds. Ces investissements numériques permettraient aux *startups* pharmaceutiques d'évoluer et de changer de niveau, passant du niveau *startup* au *scale-up*. Les petites entreprises ou les *startups* pourront ainsi accéder facilement et en toute sécurité au marché des capitaux pour un coût bien moindre que le coût traditionnel. De ce fait, les plus petits investisseurs auront l'opportunité d'investir dans des *startups* prometteuses et de bénéficier de leur augmentation de valeur potentiellement significative.

La proposition de règlement du 24 septembre 2020 de la Commission européenne pourrait, en cas d'adoption, uniformiser les finances numériques sur l'ensemble de territoire de l'Union. Ce règlement représente un enjeu stratégique pour toutes les entreprises européennes, mais il représente surtout une opportunité pour les petites *startups* pharmaceutiques de pouvoir accéder plus aisément à des fonds pour financer leur programme de recherche et développement. En effet, du fait de l'abolition des contraintes du système financier actuel, les investissements pourraient affluer et notamment de la part des petits investisseurs. Les outils financiers numériques tels que les *stablecoins* et *security tokens* offrent des avantages notamment fiscaux, qui devraient inciter les investisseurs à évoluer vers l'investissement par voie numérique plus rapide, moins coûteuse et plus transparente que la voie classique.

# Conclusion générale

« Droit numérique et santé », il s'agit là d'un sujet qui anime l'ensemble de la sphère scientifique, médicale et juridique, mais aussi plus largement économique et sociologique. Pas une journée ne passe sans qu'un écrit ne vienne s'interroger et illustrer les sujets soulevés par le numérique en santé. Pilier de la relation entre le patient et les acteurs de santé, le numérique, entendu au sens large, a envahi l'espace de santé et devient déterminant non seulement dans la technique à employer mais aussi dans l'analyse et l'évaluation du résultat de la recherche comme du diagnostic. La santé est désormais soumise au numérique, et plus spécifiquement à l'interprétation de l'intelligence artificielle. Si le sujet peut être dérangeant sur le plan éthique, sociologique ou moral, il l'est tout autant sur le plan juridique, dès lors qu'il est désormais non seulement incontournable, mais également indispensable dans l'organisation de la protection de la santé et l'innovation en matière de produits et services de santé dont dépendent les patients. Or, dans un contexte aussi mouvant que celui de la santé, où le juridique doit tout à la fois accompagner les évolutions scientifiques permanentes et dans le même temps freiner l'innovation et lui fixer un cadre, il est nécessaire de comprendre l'amplitude de la mission de régulation juridique en santé. Cette approche, dans sa globalité du monde des affaires et de la santé, faire ressortir le côté paradoxal du juridique qui doit imposer, contrôler, surveiller, interdire l'exercice des activités en santé, et dans le même temps favoriser, impulser, initier de nouvelles voies et approches de la santé. Gardien du temple et aventurier explorateur, telle est la posture inconfortable dans laquelle se trouve l'État, régulateur en santé, confronté à de nouveaux et puissants partenaires issus du monde du numérique.

En effet, au-delà de son rôle de gendarme de la santé, en charge de la protection de la santé publique, prompt à sacrifier la liberté d'entreprise au nom de la santé individuelle et collective, il doit initier et inventer de nouvelles architectures en anticipation des schémas économiques et sociétaux qui se profilent. Les exemples foisonnent en la matière et, pour ne prendre que les plus récents, la stratégie nationale de santé, ou encore le Ségur de la santé, donnent la feuille de route au ministère de la Santé pour adopter les mesures qui anticiperont le traitement des questions de santé de demain, et prévoient, au regard des statistiques et mouvements sociétaux, les évolutions vers lesquelles doit s'orienter l'économie de la santé. Le législateur donne alors le coup d'envoi des innovations en santé. Ainsi la nouvelle politique de santé, dans le prolongement de la stratégie nationale de santé, offre la possibilité de créer de nouvelles structures d'accompagnement de la personne âgée, constatant l'augmentation pour les années à venir de la population senior. Elle stimule la télémédecine et le recours au numérique pour résoudre les questions de désertification, urbaine ou rurale, et répondre aux divers besoins de santé fortement révélés pendant la crise sanitaire. Elle impulse le recours à la e-santé en favorisant juridiquement l'innovation et le développement des *startups* et licornes, par les entreprises de taille intermédiaire (ETI), petites et moyennes entreprises (PME),

par un accompagnement simplifié en droit des sociétés, social, fiscal, leur permettant de se déployer sur les territoires. Elle engage à la création juridique en promouvant des rapprochements publics et privés, dans un esprit de corégulation. Les vannes sont ouvertes pour favoriser l'inventivité du juriste à mettre en place des concepts innovants qui doivent permettre tout à la fois de réaliser une économie pour le système de santé et de créer une nouvelle offre de services et produits dans une vision de la santé globale portée par le recours au numérique.

Cette évolution juridique se situe dans une économie happée par le numérique et l'intelligence artificielle qui provoquent des prises de position radicales et antagonistes. L'adoption d'un dispositif juridique en faveur de la liberté d'innovation a pour revers la transgression des parois juridiques destinées à protéger les droits de la personne. Le passage au numérique global dans tous les domaines de la santé est un appel d'air pour les entreprises de services numériques situées dans le périmètre du monde de la santé, mais sans lui appartenir. La circonférence du monde des affaires et de la santé s'élargit pour englober toutes les activités de services, impliquées dans l'amélioration de la qualité de vie et placer en leur centre, comme déterminante, l'activité numérique, à l'instar de la place qui lui est accordée dans la société tout entière.

Le déploiement exponentiel du numérique dans l'univers des affaires et de la santé est une révolution, qui fait exploser les principes acquis de secret, confidentialité, *intuitu personae* historiquement au cœur de la santé, et nécessite, en droit, de repenser la relation entre les acteurs et la définition de leurs responsabilités. Au cœur du dispositif législatif européen et national, le patient est devenu un acteur, actif, informé, participatif autour duquel s'articule l'ensemble du système. Désormais, cette vision de la médecine globale oblige à une lecture juridique pluridisciplinaire en droit, et transdisciplinaire au sein des sciences sociales, médicales et scientifiques.

Ainsi, la protection de la santé publique doit désormais inclure la protection des données individuelles et de santé de la personne, la protection contre la cybercriminalité, qui peut mettre en danger la santé mondiale. L'utilisation des données en santé est fondée sur une économie de rupture avec l'entrée en transversalité d'acteurs extérieurs à la santé, informaticiens, mathématiciens, statisticiens, qui s'imposent désormais comme déterminants dans la relation de soins, en créant des intelligences artificielles autonomes, capables d'évaluer et soumettre un diagnostic plus fiable et rapide que celui délivré par l'homme. L'outil numérique prend alors le pas sur la capacité d'analyse humaine, mais ne lui enlève pas la responsabilité de la décision à prendre vis-à-vis du patient. Ce constat fleurit tout au long du cycle de vie du produit, constituant de nouveaux paradigmes auxquels le juriste est confronté dans l'analyse de la qualification et classification des faits juridiques, l'outil numérique envahissant aussi cet espace du droit et de la justice.

Dans ce contexte, les *startups* se sont emparées des découvertes et méthodes d'exploitation des données, devenues indispensables aux produits et pratiques de santé. Toutes les entreprises et établissements de santé, les centres de recherche, les *clusters* qui souhaitent par le biais de l'étude statistique de données améliorer ou

créer un mode de surveillance et prise en charge du patient plus global, rapide, efficient, complet, s'ouvrent à ces analyses.

Le patient joue un rôle souvent inconscient dans cette captation de données. Il donne gratuitement ses informations personnelles, qui entrent dans une valorisation économique. Cette transmission des informations personnelles est considérée comme une forme de « paiement ». La contrepartie est le service, la rapidité, l'information prédictive, préventive, personnalisée, participative qui est assurée par l'entreprise des produits de santé, et à laquelle le patient ne souhaite ou ne peut plus renoncer, quelle qu'en soit la conséquence en termes de protection de la vie privée. La question de l'information de la personne, et de sa bonne connaissance est un sujet majeur. Cette évolution, ou révolution, soulève un ensemble de problématiques complexes et transversales, qui vont bien au-delà de la question de la protection des données, et dont se sont saisies la Commission nationale de l'informatique et des libertés (CNIL), mais aussi la Haute Autorité de santé (HAS) pour l'intégration positive des algorithmes dans les techniques de soins. Les acteurs de santé se sont lancés dans cette technique sur des *Patient Support Programs* destinés à suivre le patient, la bonne observance du traitement, les effets indésirables du produit. La collecte et l'utilisation des résultats provoquent une rupture dans l'organisation et le fonctionnement traditionnel de la médecine, de la recherche, de la vigilance, en déplaçant les zones de responsabilité.

Il faut aussi noter le recours aux *blockchains*, nouveau concept qui envahit le secteur de la santé. Elle ouvre des perspectives multiples grâce à une meilleure continuité des soins, un enrichissement du dossier médical partagé (DMP) grâce à la transparence, une interopérabilité, un développement de la recherche, une certification des essais cliniques grâce à la robustesse et au caractère infalsifiable. Toutefois, le mécanisme, outre le fait qu'il est techniquement perfectible, présente des risques juridiques et réglementaires, portant notamment sur la récupération des données, le droit à l'oubli, le droit à l'information, la protection des droits de propriété industrielle et intellectuelle, la force de la relation contractuelle (*smart contract*), et aussi la sécurité et l'inviolabilité des données, la responsabilité civile, pénale des auteurs pour ne citer que les principales questions qui sont à résoudre. Le *big data* et les données de santé posent donc de réels enjeux éthiques que le juridique peut résoudre en adoptant une posture en anticipation des risques pouvant survenir au regard d'une notion de progrès de la société souverainement et collectivement définie.

Si l'intérêt du numérique au sens général est indéniable dans la santé et constitue une avancée majeure dans les soins et le suivi de la personne, il a, comme toute pratique, un revers très lourd. Outre le fait que le numérique est dépendant de la fiabilité du système technique et technologique, et n'est pas à l'abri de nombreuses failles qui paralysent les systèmes de santé en un instant, l'utilisation massive du numérique et des données peut conduire au développement d'un système de santé à plusieurs vitesses, dont le patient, en apparence seulement, acteur, actif, est en réalité un acteur dépendant, manipulé par un système statistique et algorithmique sur lequel les concepteurs n'ont d'ailleurs plus de vision claire et transparente, et dont le mode d'analyse leur échappe. Il convient donc de fixer avec urgence le cadre

juridique et réglementaire d'utilisation du numérique, par l'élaboration de pratiques de corégulation entre les acteurs incontournables et les pouvoirs publics, par la mise en place de chartes, *soft law*, *guidelines* que les acteurs privés s'engagent à suivre dans une vision de la société.

Sur le plan national, la politique de développement de la télémédecine en France, dans un contexte d'application du règlement européen sur la protection des données, du règlement européen sur les dispositifs médicaux et sur les recherches impliquant la personne humaine, devraient permettre de circonscrire certaines problématiques, sans toutefois les résoudre toutes, et notamment celles de l'exploitation et de la valorisation des données collectées. Après l'échec de l'application Stop Covid, c'est au tour du passeport vaccinal et de l'application permettant d'identifier les personnes non vaccinées de soulever des questionnements quant à la nécessité d'un système de contrôle contraignant au nom de la santé publique, au détriment du respect des libertés fondamentales des citoyens.

Désormais, la circonférence du monde des affaires et de la santé s'élargit pour englober toutes les activités de services, impliquées dans l'amélioration de la qualité de vie et des soins, allant jusqu'à la robotisation de la santé, conduite par l'intelligence artificielle. Dans sa mission de censeur protecteur, le droit agile doit anticiper les risques pour l'humanité et organiser un nouveau système de santé amélioré et non pas dominé par l'exploitation malheureuse de l'intelligence artificielle, au final devenue autonome par rapport à l'être humain qui l'a créée. L'imagination du législateur doit s'engager avec urgence dans cette réflexion d'avenir. Le programme de santé pour les années à venir, présenté par la France en parallèle de l'Union européenne, dans cette période frappée par la pandémie Covid-19 donne, dans un contexte malheureux et critique, l'illustration de la profonde préoccupation des pouvoirs publics à mettre en place un procédé qui permette tout à la fois de bénéficier du progrès sans en subir les effets indésirables.

En ce sens, « Droit numérique et santé » représente le trio gagnant dans la stratégie nationale et européenne de santé, visant la relance de l'activité économique, post-pandémique.

Le plan « Innovation Santé 2030 » présenté le 29 juin 2021 par le Président de la République a pour ambition de « faire de la France la première Nation européenne innovante et souveraine en santé ». Tirant l'expérience de l'épreuve de la pandémie Covid-19, le plan repose sur une volonté de décloisonnement des activités de santé avec, au cœur du système, le patient acteur, actif, moteur. Ce ne sont donc plus des objectifs théoriques, mais un changement radical de paradigme en santé qui pousse l'ensemble des acteurs, professionnels de santé, établissements, industries, *startups* et licornes du numérique à avancer ensemble sur l'ensemble du territoire. Du micro-projet des *startups* locales aux innovations internationales portées par les *big pharma* ou licornes numériques, le mouvement d'accompagnement vise tous les projets, qui doivent néanmoins être rendus compatibles, pérennes et garants des droits et libertés fondamentaux de chacun. Placé sous le signe de la souveraineté sanitaire, le plan « Innovation Santé 2030 » porte un projet de soutien aux filières de la biothérapie et de la bioproduction qui doivent se développer en accéléré notamment grâce au numérique dans la R&D, et surtout être localisées

sur le territoire national, afin de limiter les conséquences désastreuses de la dépendance aux territoires hors Union européenne. Perçu comme un facteur majeur d'accélération de l'innovation et de transformation des organisations, le numérique en santé bénéficie d'un nouvel effort budgétaire gonflant les montants accordés dans le cadre du Ségur de la santé[1]. Il est annoncé un programme « Paris Santé Campus », qui vise à fédérer les acteurs publics et privés autour de projets de recherche et d'innovations, avec la nécessité de préparer « la génération future » de la santé numérique, et de parvenir à un écosystème attractif pour valoriser les solutions numériques. Ces projets politiques et économiques ambitieux, en réaction face à la suprématie numérique des grandes puissances, USA et Chine, s'inscrivent dans une volonté européenne d'élever l'Union européenne au rang des acteurs influents. Mais, au-delà de ces considérations, l'encadrement juridique et réglementaire, qui sera nécessaire pour assurer la protection des droits des acteurs économiques ainsi que celle de l'ensemble de la population concernée, reste encore à construire sur le terrain et dans les territoires.

La période de pandémie Covid-19, désormais qualifiée de syndémie, révèle parfaitement l'ensemble des enjeux qu'il convient de relever au niveau juridique. La tâche est d'ampleur en ce qu'il convient d'imaginer et d'assurer un accompagnement juridique souple, agile, avec une levée des contraintes, des freins et blocages administratifs qui font prendre du retard aux projets. Ceci présuppose un engagement des acteurs vers de nouveaux concepts des relations juridiques, vers une corégulation publique-privée indispensable à la réussite des projets numériques, vers une adaptabilité ou scalabilité des montages, au sens du vocabulaire numérique. Mais cet encadrement agile et souple ne peut s'inscrire dans la durée que par une approche de rigueur et de cadrage garantissant la clarté, la transparence, et la compatibilité des projets, ce qui suppose une révision globale des schémas d'exploitation du numérique en santé. La volonté de recours à une institution nouvelle en charge de cet objectif place une strate supplémentaire dans la complexité des agences, autorités, acteurs publics et privés reliés dans le déploiement de cette stratégie.

Le projet pour 2030 contient un plan global, transversal, qui vise à financer plus largement les industries de santé et la recherche biomédicale, à garantir l'accès au marché de produits plus vite, plus tôt, mais aussi à bouleverser les pratiques en misant sur la formation, les collaborations « public-privé » avec de nouvelles formes de relations entre les acteurs implantés sur les territoires. Pour assurer le succès de ces démarches, la création de l'Agence de l'innovation en santé, prévue pour début 2022, aura pour vocation d'assurer le pilotage stratégique du plan, de simplifier les parcours de créations d'entreprises quelle que soit leur taille et notamment les *startups* et les entreprises de taille intermédiaire, avec pour ambition de dynamiser les territoires et de les relier à la grande innovation voulue dans une approche de souveraineté nationale en santé. La création de cette Agence de l'innovation en santé s'inscrit plus largement dans le grand programme de l'Union européenne en matière de santé. La Commission européenne a clairement affirmé sa volonté de

(1) Aux deux milliards d'euros prévus par le Ségur de la santé vont s'ajouter 650 millions d'euros, destinés à accélérer la dynamique.

créer une nouvelle autorité européenne en matière de santé calquée sur le modèle de la BARDA aux États-Unis[2] afin de préparer les États membres contre de futures crises sanitaires, constituer des stocks de médicaments stratégiques et investir dans la recherche et le développement pharmaceutique, notamment en renforçant le recours au numérique dans tous ses aspects et ses usages en santé.

Ces préoccupations, conduisant à de nouvelles formes d'engagements entre les acteurs publics et privés européens, afin de lutter contre les menaces sanitaires de la population européenne et mondiale, sont le facteur déclenchant d'une évolution accélérée vers une nouvelle ère des systèmes de santé au cœur desquels le numérique est le pilier central.

Dans cette dynamique, si l'encadrement juridique et réglementaire est un sujet maîtrisé et maîtrisable, notamment sur les innovants accords de coopération de R&D, de production et distribution dans le cadre des projets HERA, toute la question reste le déploiement actif et cohérent sur les territoires par l'ensemble des acteurs. Le projet « Fab UE » consistera à mettre sur pied un réseau de capacités de production d'urgence, à utilisateur unique et multi-utilisateurs, à technologie unique et multitechnologies, destinées à la fabrication de vaccins et de médicaments à l'échelle européenne. Le réseau Vaccelerate permettra la coopération et l'échange de données sur les essais cliniques. L'organisation en matière de propriété industrielle et de concurrence est pensée afin d'assurer le succès de ces projets.

L'adaptation nécessaire à cette crise s'est traduite par une utilisation agile du droit, manifestée par le recours à de nouvelles formes de relations cadrées et évolutives, dans une volonté commune, collective et solidaire de lutte contre l'ensemble des risques pandémiques, infodémiques, syndémiques auxquels sont exposées les populations, et ce tout en assurant une maîtrise technique réelle du numérique et de l'intelligence artificielle dans la décision de santé publique.

Dans ce tourbillon d'innovation et d'avancées majeures modifiant tous les paradigmes en santé, toute la question est d'appuyer l'innovation juridique sur les concepts préexistants et de déterminer ce qui relève de l'exploitation et de l'optimisation de la norme, ou de faire émerger des concepts et principes nouveaux sur lesquels s'adosse le progrès numérique en santé.

L'exemple de la question de la vaccination obligatoire, comme outil de lutte contre la pandémie, ou encore celui du passeport vaccinal européen posent clairement le sujet de l'identification des personnes non vaccinées par les professionnels de santé et les autorités nationales. La CNIL, gardienne des libertés, émet des réserves sur ces systèmes numériques envisagés pour contrôler l'état d'avancement du taux de vaccination dans la population par la collecte de données. À la suite de sa signature officielle, intervenue le 14 juin 2021, le règlement relatif au certificat Covid numérique de l'Union européenne a été publié le 15 juin et est entré en application le 1er juillet 2021[3].

(2) La *Biomedical Advanced Research and Development Authority* (BARDA) est un bureau du département de la Santé et des Services sociaux des États-Unis (HHS) chargé de l'acquisition et du développement de contre-mesures médicales, principalement contre le bioterrorisme, y compris les menaces nucléaires, radiologiques, biologiques et chimiques (NRBC), ainsi que la grippe pandémique et les maladies émergentes.

(3) https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_3343.

Entre protection des enjeux de santé publique et d'économie de la santé et protection des droits fondamentaux, il est difficile de placer le curseur à la bonne place. La grande question des années à venir portera sur la définition, ou redéfinition, des libertés fondamentales au regard des enjeux de santé publique et consistera à établir une vision cohérente dans l'utilisation de l'intelligence artificielle par l'intelligence humaine.

# Bibliographie

## 1. Ouvrages


C. AIGOUY et V. VIOUJAS, *La télémédecine dans les établissements de santé : Vade-mecum*, Bordeaux, Les Études Hospitalières, 2014.

G. BABINET et R. VASSOYAN, *Big data et objets connectés. Faire de la France un champion de la révolution numérique*, Paris, Institut Montaigne, 2015.

P.-Y. BADILLO et D. BOURGEOIS, *Santé et « influence » numérique. Le positionnement de Roche, Novartis et Sanofi*, in *Cybersanté*, Genève : [s.n.], 2019.

F. BECQUART, *L'égal accès aux soins : mythe ou réalité ?*, Bordeaux, Les Études Hospitalières, coll. « Mémoires numériques de la BNDS », 2011.

J. BÉRANGER, *Les Big Data et l'éthique : le cas de la datasphère médicale*, Londres, éd. ISTE, 2016 ; *Les systèmes d'information en santé et l'éthique : d'Hippocrate à e-ppocr@te*, Londres, éd. ISTE, 2015.

E. BILAL, L. DEVILLERS et G. DOWEK et *al.*, *Intelligence artificielle : Enquête sur ces technologies qui changent nos vies*, Paris, Flammarion, 2018, Cote QE10/0011.

Y. BISMUTH, *Le Droit de l'informatique*, Paris, L'Harmattan, 2017.

C. BOEDTS et A. FONTAINE, *L'analyse de l'attractivité d'un écosystème régional d'innovation en matière d'investissements et de Recherche & Développement*, Louvain School of Management, Université catholique de Louvain, 2020.

J.-M. BRUGHIÈRE et *al.*, *Le Droit de l'Internet*, Paris, LexisNexis, 2017.

D. CARDON, *Culture numérique*, Paris, Presses de Sciences Po, 2019.

A. COHEUR, *Révolution numérique, révolution ou évolution pour la mutualité, nouveaux rôles, nouveaux défis*, in *La santé connectée, une totale mutation ?*, éd. Euro Cos Humanisme & Santé, mars 2019.

J. M. CROELS, *Le droit des obligations à l'épreuve de la télémédecine*, Marseille, PU Aix-Marseille, 2006.

P. DEGOULET, M. FIESCHI et J. MÉNARD, *E-santé en perspective*, Paris, Lavoisier, 2017.

R. DEHOUSSE, *Politiques européennes*, Presses de la Fondation nationale des sciences politiques, 2009.

B. DONDERO, *Droit 2.0, Apprendre à pratiquer le droit au XXI^e siècle*, LGDJ, Lextenso éd., 2015.

B. ESPESSON-VERGEAT, J.-L. DUROUSSET, L. GEFFROY et *al.*, *Innovation juridique et transversalité des politiques liées au numérique, à la santé et aux territoires*, Actes du colloque tenu à Saint-Étienne le 28 septembre 2017, Les Éditions Hospitalières, coll. « Actes et séminaires », 2018.

H. EVRARD, *La pollution numérique : état des lieux de la prise de conscience de son impact et mesure d'efficacité relative de diverses techniques d'influence pour la résorber*, Louvain School of Management, Université catholique de Louvain, 2020.

V. FERNANDEZ, L. GILLE et T. HOUY, *Les technologies numériques de santé. Examen prospectif et critique*, Presses des Mines, févr. 2015, 112 p.

M. FIESCHI et J.-C. DUFOUR, *Traitement des données en santé : Approches systémiques*, Londres, éd. ISTE, 2018.

A. GARAPON et J. LASSÈGUE, *Justice digitale*, Paris, PUF, 2018.

H. GEBEL, *Synthèse*, in *La santé connectée, une totale mutation ?*, éd. Euro Cos Humanisme & Santé, mars 2019.

A. GRÉGOIRE, *Entre concurrence et santé : à la croisée des chemins. L'organisation des soins à l'épreuve de l'article 101 du Traité FUE*, Faculté de droit et de criminologie, Université catholique de Louvain, 2017.

C. HERVÉ et M. STANTON-JEAN, *Innovations en santé publique, des données personnelles aux données massives (Big data) : Aspects cliniques, juridiques et éthiques*, Paris, Dalloz, 2018.

E. HIRSCH et F. HIRSCH, *Traité de bioéthique*, t. IV « Les nouveaux territoires de la bioéthique », Toulouse, Erès, 2018.

O. ITEANU, *Quand le digital défie l'État de droit*, Paris, Eyrolles, 2016.

P. JENSEN, *Pourquoi la société ne se laisse pas mettre en équations*, Paris, Seuil, 2018.

C. KRYCHOWSKI (ss dir.), *Business models en e-santé*, Paris, Presses des Mines, coll. « Économie et gestion », 2020, p. 26.

F. LAU et C. KUZIEMSKY, *Handbook of eHealth Evaluation : An Evidence-based Approach*, Canada, University of Victoria, 2016, 504 p.

M. MICHEL, *Conférence introductive*, in *La santé connectée, une totale mutation ?*, éd. Euro Cos Humanisme & Santé, mars 2019.

E. MINVIELLE, *Le patient et le système. En quête d'une organisation sur mesure. Approches innovantes du parcours de santé*, éd. Seli Arslan, avr. 2018, 288 p.

B. NORDLINGER et C. VILLANI, *Santé et intelligence artificielle*, Paris, CNRS éd., 2018.

A. NORMAND, *Prévenir plutôt que guérir, la révolution de la e-santé : Objets connectés – Applis – Big Data – Médecine prédictive*, Paris, Eyrolles, 2017.

I. POIROT-MAZÈRES, *Santé, numérique et droit-s*, PU Toulouse 1 Capitole, 21 janv. 2019 ; *Rappel des cadres normatifs : quel(s) droit(s) en santé à l'heure du numérique ?*, in *Santé, numérique et droits*, Institut fédératif de recherche « Mutation des normes juridiques », Université Toulouse I, Séries « Colloques de l'IFR », 2018, p. 23-60.

A. RIBEIRO, *La Blockchain et ses potentielles applications*, Genève, 2016, 40 p.

G. ROUET, J. DEYDIER, E. CHAZARD et *al.*, *Algorithmes et décisions publiques*, Paris, CNRS éd., 2019.

B. SALGUES, *Industrialisation de la santé : Identité, biopouvoir et confiance*, Londres, éd. ISTE, 2016.

D. SICARD, *La santé connectée, une mutation ou une aliénation ?*, in *La santé connectée, une totale mutation ?*, éd. Euro Cos Humanisme & Santé, mars 2019.

P. SIMON, *Télémédecine. Enjeux et pratiques*, éd. Le Coudrier, 2015.

A. SPIRA, *La recherche en santé publique*, *in* F. BOURDILLON et *al.*, *Traité de la santé publique*, Lavoisier, coll. « Traités », 2016, p. 116 à 124.

A. de STREEL et JACQUEMIN, *L'Intelligence artificielle et le Droit*, Bruxelles, Larcier, 2017.

R. SUSSKIND, *Tomorrow's Lawyers : An introduction to your Future*, Oxford University Press, 2013.

A. TAILLEFAIT et M. LANNA, *Smart cities & santé*, Varenne, Institut Universitaire Varenne, 2019.

S. TISSERON, F. TORDO et A. LANCHON, *Robots, de nouveaux partenaires de soins psychiques*, Toulouse, Erès, 2018.

T. WICKERS, *La Grande Transformation des avocats*, Paris, Dalloz, 2014.

## 2. Articles

F.-M. ADEOTI, *Systèmes de santé : L'apport déterminant de l'e-santé et des technologies du numérique : Gestions hospitalières* 2018, 285-288.

F.-A. ALLAERT et *al.*, *Les enjeux de la sécurité des objets connectés et applications de santé : Journal de gestion et d'économie médicales* 2016, 34, 311-319.

AMBASSADE DE FRANCE AU ROYAUME-UNI, Service Enseignement supérieur, Recherche et Innovation, *Le paysage britannique de la santé numérique*, in *Science & Technologie au Royaume-Uni* oct. 2018, n° 82.

ANON, *Améliorer l'usage de la télémédecine en France*. 2e partie, « Les outils de développement de la TLMD », in *Responsable santé. La lettre bimensuelle d'information sur le risque médical et la démarche qualité* 26 oct. 2017, n° 290, p. 6.

T.D. AUNGST et *al.*, *How to identify, assess and utilise mobile medical applications in clinical practice*, in *Int J Clin Pract.* Feb. 2014, 68(2) :155-62.

E. AZRIA, *Le soignant et la standardisation des pratiques médicales : Laennec* 2013/3, t. 61, p. 32 à 41.

E. BARTHE, *L'intelligence artificielle et le droit*, in *I2D, Information, données & documents* 2017, vol. 54, 2.

H.-P. BASS, *La santé : quoi de neuf ?*, in *Le Journal des psychologues* mars 2019, n° 365, p. 58-65.

H.-P. BASS, D. BRUN et J.-C. SARDAS, *La santé : quoi de neuf ? : Le Journal des psychologues* 2019, vol. 365, n° 3, p. 58-65.

J. BATTIN, J.-F. DARTIGUES, B. BIOULAC et *al.*, *Les enjeux de la médecine de demain*, in *RGDM* sept. 2018, n° 68, p. 13-62 [en ligne].

A. BECUWE et C. THÉBAUT, *Les applications numériques en santé à l'épreuve du circuit de fixation de prix et de remboursement des produits de santé, l'exemple de Moovcare® : Marché et organisations* 2020/2, n° 38, p. 145 à 150.

J. BÉRANGER, *E-santé, m-health, big data médicaux : Vers une hiérarchisation des données médicales : Revue Hospitalière de France* 2015, 70-74 ; *Que (nous) font les big data ? : Revue internationale et stratégique* 2018/2, n° 110, p. 89 à 99.

S. BERNATCHEZ, *La certification en tant que droit de la gouvernance : Éthique publique* 2019, vol. 21, n° 1.

F. BERTUCCI et *al.*, *Santé numérique et « cancer hors les murs », Big Data et intelligence artificielle : Bull. Cancer* 19 sept. 2019.

C. BERU et S. SARUGGER, *La soft law européenne dans la mise sur agenda nationale. L'usage des instruments européens dans la construction des politiques d'e-santé en France et au Royaume-Uni*, in *Gouvernement et action publique* mars 2018, n° 3, p. 9-34.

P. BESSE, A. BESSE-PATIN et C. CASTETS-RENARD, *Implications juridiques et éthiques des algorithmes d'intelligence artificielle dans le domaine de la santé,*13 mars 2020, mise à jour 14 juin 2021.

M. BORGETTO, M. TRÉPREAU, D. CRISTOL et *al.*, Dossier *La stratégie nationale de santé : RD sanit. soc.* juin 2018, n° 3, p. 387-456 [en ligne].

C. BOURDAIRE-MIGNOT et *al.*, *Données de santé : les nouveaux outils numériques de collecte et d'exploitation des données renouvellent les problématiques du consentement du patient et de la relation de soins : La Revue des droits de l'homme* [en ligne], *Actualités Droits-Libertés*, 7 sept. 2018, consulté le 8 mars 2019.

C. BOURDAIRE-MIGNOT et T. GRÜNDLER, *La bioéthique de demain : Un CCNE plus fort et des lois moins bloquantes : La Revue des droits de l'homme*, *Actualités Droits-Libertés*, 16 déc. 2018.

L. BOURGEON, J.-F. PENCIOLELLI, J. ROCHE et *al.*, Dossier *Santé : La révolution numérique : Gestions hospitalières* avr. 2018, n° 575, p. 212-288.

R. BOURNE et *al.*, *Magnitude, temporal trends, and projections of the global prevalence of blindness and distance and near vision impairment : a systematic review and meta-analysis*, in *The Lancet Global Health*, vol. 5, Issue 9, p. 888-897.

L. BOUZLAFA, P.-H. BRÉCHAT, A. MALONE et *al.*, *Plan stratégique régional de santé et agence régionale de santé : bilan mitigé en faveur d'améliorations*, in *Revue Droit et santé, La revue juridique des entreprises de santé* nov. 2017, n° 80, p. 771-781.

B. BROUARD, *Chapitre 2. Utilisation des Big Data en santé : le cas des objets connectés : Journal international de bioéthique* 2017, 28(3) : 27-30.

J. CABY, *Industrie pharmaceutique du générique recherche rentabilité désespérément : The Conversation*, 29 août 2019.

C. CALINAUD et J.-F. DHAINAUT, *Un accélérateur de l'innovation en santé : le Lab Santé Île-de-France : Annales des mines – Réalités industrielles* mai 2017, p. 73.

T. CAMINEL et C. RICHARD, *Intelligence artificielle*, in *Gestions hospitalières* avr. 2018, n° 575, p. 265-267.

G. CANIVET, *Les facteurs de transformation du droit : Enjeux numériques : Annales des mines – Réalités industrielles*, sept. 2018, n° 3.

B. CHAIX, *Impact de l'intelligence artificielle dans la recherche clinique et la collecte de données en vie réelle : Actualités pharmaceutiques* sept. 2018, vol. 57, Issue 578, p. 22-24.

V.W. CHANG et D.S. LAUDERDALE, *Fundamental Cause Theory, Technological Innovation, and Health Disparities : The Case of Cholesterol in the Era of Statins*, in *J Health Soc Behav.* 2009, 50 : 245-260.

M. CHARPENTIER, É. DÉBOUCHE, C. ENDELIN et L. BLOCH, *L'intelligence artificielle en santé*, in *Bulletin juridique du praticien hospitalier (BJPH)* avr. 2019, n° 217, p. 7.

C. CHASSIN, Dossier *ADH PACA 2030, l'odyssée de la santé : Le journal de l'association des directeurs d'hôpital (JADH)* oct. 2018, n° 77, p. 8-21.

C. CHASSIN, A. MALONE, É. BALEZ, A. LARPIN et al., *2030 : Odyssée de la santé, Techniques hospitalières : La revue des technologies de la santé* déc. 2018, n° 773, p. 47-57.

E. CHELLE, *La complémentaire santé comportementale : un nouveau logiciel assurantiel ? RD sanit. soc.* août 2018, n° 4, p. 674-686 [en ligne].

S. CLAEYS et R. BONFILLON, *L'éthique comme médiation*, in *Techniques hospitalières : La revue des technologies de la santé* déc. 2018, n° 773, p. 76-80.

L. CLUZEL-MÉTAYER, Dossier *Les données publiques : RF adm. publ.* déc. 2018, n° 167, 736 p.

P. COZ, S. LANA et P. LE COZ, *Éthique et e-santé*, in *Objectif soins & management : La revue des cadres de santé* sept. 2018, n° 264, p. 50-53.

T. CYNOBER, *Enjeux des big data en santé : Actualités pharmaceutiques* sept. 2018, vol. 57, Issue 578, p. 25-29.

M. DAHAD, *Digitalisation de la santé au Sud : quand les firmes du numérique décident de l'accès au soin : Mouvements* juin 2019, n° 98, p. 120-32.

E. DEBIÈS, *Big data de santé et autodétermination informationnelle : RF adm. publ.* déc. 2018, n° 167, p. 565-574 [en ligne].

M. DEL RÍO CARRAL et *al.*, *Santé digitale : promesses, défis et craintes. Une revue de la littérature : Pratiques psychologiques*, août 2016.

E. DERIEUX, *L'intérêt général, pierre angulaire ou inégalitaire du droit de la communication ? : Légicom* 2017/1, n° 58, p. 105 à 120.

D. DESBOIS, *Le Marché unique numérique des données et la santé à l'heure du RGPD : les spécificités de la santé publique en Europe*, in *I2D – Information, données & documents* 2019, n° 1, p. 29-33.

S. DESMOULIN-CANSELIER, *L'évaluation des médicaments à l'ère de la médecine des données : RD sanit. soc.* déc. 2018, n° 6, p. 1043-1054 [en ligne].

S. DESVAUX (ss dir. scientifique), *Les nouvelles technologies et leur incidence en droit de la consommation : CDE* sept.-oct. 2019, n° 5.

N. DEVILLIER, *La coopération transatlantique en e-santé*, in *Droit, Santé et Société* mai 2018, n° 5-6, p. 42-44.

J.-F. DHAINAUT, O. BLIN et F. HERRY, *Recherche et innovation en santé : comment optimiser l'interface entre les startups/industries et les établissements de santé académiques ou non ?*, in *Thérapies* janv.-févr. 2020, vol. 75, Issue 1, p. 101-111.

V. DIEBOLT, I. AZANCOTB et F.-H. BOISSELC, *« Intelligence artificielle » : quels services, quelles applications, quels résultats et quelle valorisation aujourd'hui en recherche clinique ? Quel impact sur la qualité des soins ? Quelles recommandations ?*, Ateliers de Giens 2018, Recherche clinique : *Thérapies* 2019, vol. 74, Issue 1, p. 141-154.

J. DIRRINGER, *L'avenir du droit de la protection sociale dans un monde ubérisé : RF aff. soc.* 2018, n° 2, p. 33-50.

DOSSIER, *E-santé : les régions en action ! : DSIH* févr. 2018, n° 23.

DOSSIER, *IA et droit, dépasser la fiction pour une approche juridique raisonnée : Rev. Lamy dr. aff.* sept. 2019, n° 151, p. 21.

DOSSIER, *La e-santé se renforce*, Éditions Législatives, 2 déc. 2018, 6 p.

P.-A. DRUBAY, *Le pharmacien face à l'intelligence artificielle : Actualités pharmaceutiques* sept. 2018, vol. 57, Issue 578, p. 30-32.

P.-H. DUÉE, J. AQUILI et J.-F. DELFRAISSY, *L'avis 129 du CCNE : un regard éthique partagé avec la société : Contraste* 2019/2, n° 50, p. 135 à 154.

H. DUMEZ et E. MINVIELLE, *L'e-santé rend-elle la démocratie sanitaire pleinement performative ?*, in *Systèmes d'Information et Management* 2017, « Special Issue : Health IT », 22 (1), p. 9-37.

B. ESPESSON-VERGEAT, *Les objets connectés de santé et l'apparition du « patient-consommateur » : CDE* sept.-oct. 2019, n° 5, p. 37.

G. EYSENBACH, *What is eHealth?*, in *J Med Internet Res* 2001 ; 3(2) :e20.

F. FATEHI et R. WOOTTON, *Telemedicine, telehealth or e-health? A bibliometric analysis of the trends in the use of these terms*, in *J Telemed & Telecare* 2012, 18(8) : 460-464.

E. FOURNEYRON et *al.*, *Réalités et défis pour l'organisation du système de santé de premier recours : Med Sci* (Paris), vol. 34, « Numérique et santé », juin-juill. 2018, n° 6-7, 581-586.

G. GAGLIO et A. MATHIEU-FRITZ, *Les pratiques médicales et soignantes à distance. La télémédecine en actes : Réseaux* 2018/1, n° 207, p. 9-24.

A. GARAPON, *Les enjeux de la justice prédictive : JCP* G 9 janv. 2017, doctr. 31.

B. GARRETTE, *Missions et résultats de l'Observatoire de la e-santé dans les pays du Sud. Les opportunités du numérique dans la transformation des systèmes de santé en Afrique : Annales des Mines – Réalités industrielles*, août 2019, n° 3, p. 63-67.

C. GASULL et L. RIOM, *Healthcare and big data : digital specters and phantom objects*, in *Revue d'anthropologie des connaissances* avr. 2019, vol. 13, n° 1, p. 285-91.

G. GOURGUES et A. MAZEAUD, *Peut-on délibérer du big data en santé sans controverser ? Retour sur l'expérience d'un atelier citoyen français*, in *RF aff. soc.* 2017, vol. 4, p. 95-115.

D. GRAHAM et *al.*, *Understanding Health Literacy for Strategic Health Marketing : eHealth Literacy, Health Disparities, and the Digital Divide*, in *Health Marketing Quarterly* 2008, 25 :1-2, 175-203.

C. GRANJA et *al.*, *Factors Determining the Success and Failure of eHealth Interventions : Systematic Review of the Literature*, in *J Med Internet Res.* May 2018, 1 ;20(5).

K. GRATZERA, H. SERVY et L. CHICHE, *Des guidelines pour l'intelligence artificielle : La Revue de médecine interne* mars 2020, vol. 41, Issue 3, p. 189-191.

D. GRUSON, *Le numérique et l'intelligence artificielle en santé : surveillance généralisée ou avancée majeure ? : Les Tribunes de la santé* 2019, vol. 60, n° 2, p. 23-29.

J. HABIB et *al.*, *Appréhender les transformations organisationnelles de la santé numérique à partir des perceptions des acteurs : Systèmes d'information & management* 2017/1, vol. 22, p. 39-69.

L. HANCHER, *The EU pharmaceuticals market : Parameters and pathways. Health Systems Governance In Europe : The Role Of European Union Law And Policy*, in *Health Economics, Policy And Management* 2010, p. 635-682.

C. HANDERSON et *al.*, *Cost effectiveness of telehealth for patients with long term conditions (Whole Systems Demonstrator telehealth questionnaire study) : nested economic evaluation in a pragmatic, cluster randomised controlled trial : British Medical Journal* 2013, 346 : 2065-87.

J.-C. HENRARD, *La démarche stratégique en matière de politique de santé : pourquoi sommes-nous restés au milieu du gué ? : Santé publique* oct. 2018, vol. 30, n° 5, éditorial p. 597-599.

K. HOEYER, A. TUPASELA et M. BOGEHUS RASMUSSEN, *Codes d'éthique et travail éthique dans la recherche et le partage des données génétiques transnationales. Flux, non-flux et débordements*, in *Revue d'anthropologie des connaissances* 2019/2, vol. 13, n° 2, p. 455-478.

B. HOLTZ et *al.*, *Diabetes management via mobile phones : a systematic review*, in *Telemed J E Health* 2012 ;18(3) :175-84.

C. JAMIN, *Services juridiques : la fin des professions : Pouvoirs* 2012, n° 140.

S. KHOJA, H. DURRANI, R.E. SCOTT, A. SAJWANI et U. PIRYANI, *Conceptual framework for development of comprehensive e-health evaluation tool*, in *Telemed J E Health* Jan. 2013;19(1) :48-53.

P. KIERKEGAARD, *Interoperability after deployment : persistent challenges and regional strategies in Denmark*, in *Int J Qual Health Care* 2015, vol. 27, n° 2, p. 147-153.

A. KIYINDOU, *Introduction : réduire la fracture numérique, une question de justice sociale ? : Les Cahiers du numérique* 2009 ; 5(1) :11-7.

R.J. KORDA, M.S. CLEMENTS et J. DIXON, *Socioeconomic inequalities in the diffusion of health technology : Uptake of coronary procedures as an example*, in *Soc Sci Med* 2011 ; 72 : 224-229.

P. LABERRONDO, J.-B. GALLOIS, É. MARZOLF et *al.*, Dossier *Comment la tech peut transformer nos politiques publiques*, in *Acteurs publics actualités : La Revue du management public* juin 2019, n° 139-140, p. 85-184.

K. LATULIPPE et *al.*, *Social Health Inequalities and eHealth : A Literature Review With Qualitative Synthesis of Theoretical and Empirical Studies*, in *J Med Internet Res.* 2017 ;19(4) :e136.

J. LEBLOND, *E-Santé : quel avenir en France ? : ZDNet* 2 juill. 2019.

P. LEMOINE, *La malédiction des données : Esprit* juin 2018, n° 6, p. 131-138.

M. LE ROUZIC, *L'intelligence artificielle en santé : Gestions hospitalières* avr. 2018, n° 575, p. 263-264.

*Les dernières évolutions de la jurisprudence nationale et européenne sur les CCP*, 8 mai 2020.

X. LIANG et *al.*, *Effect of mobile phone intervention for diabetes on glycaemic control : a meta-analysis*, in *Diabet Med* 2011 ;28(4) :455-63.

E. LINCOT, *Les nouvelles routes de la soie du numérique et le défi de l'intelligence artificielle : Nectart* juin 2019, n° 9, p. 146-153.

J. LUCAS, *Les médecins dans le monde de la santé numérique, Enjeux éthiques, réflexions déontologiques et recommandations du Conseil national de l'Ordre des médecins : Les Tribunes de la santé* 2019/1, n° 59, p. 85 à 97.

D. LUPTON, *Health promotion in the digital era : A critical commentary*, in *Health Promotion International* 2014 ; 30(1), 174-183.

J.S. MARCANO BELISARIO et *al.*, *Smartphone and tablet self management apps for asthma (Review) : Cochrane Database of Systematic Review* 2013.

L. MARTIN, Dossier *La télémédecine doit prouver son efficacité : Gazette santé social* févr. 2018, n° 148, p. 15-22.

F. MARTY, *Plateformes numériques, algorithmes et discrimination : Revue de l'OFCE* 2019/4, 164, p. 47 à 86 ; *Le critère du bien-être du consommateur comme objectif exclusif de la politique de concurrence. Une mise en perspective sur la base de l'histoire de l'antitrust américain : RID éco.* 2014, t. XXVIII(4), 471.

A. MATHIEU-FRITZ et G. GAGLIO, *À la recherche des configurations sociotechniques de la télémédecine. Revue de littérature des travaux de sciences sociales : Réseaux* 2018/1, n° 207, p. 27-63.

A. MATURO, *Fatism self-monitoring and the pursuit of healthiness in the time of technological solutionism : Italian Sociological Review* 2014. 4(2), 151-171.

L. MAZEAU, *Intelligence artificielle et responsabilité civile : Le cas des logiciels d'aide à la décision en matière médicale : RPPI* 2018, p. 38-43.

C. MCCABE et *al.*, *Computer and mobile technology interventions for self-management in chronic obstructive pulmonary disease : Cochrane Database of Systematic Review* 2017.

M.G. MELCHIORRE et *al.*, *eHealth in integrated care programs for people with multimorbidity in Europe : Insights from the ICARE4EU project*, in *Health Policy* 122 (2018) : 53-63.

R. MICHEL et A. TRÉBUCQ, *Réformer l'organisation du système de santé : l'exemple de l'Euskadi : Le Concours Médical* sept. 2014, t. 136, n° 7, p. 517-519.

H. MOGHADDASI et *al.*, *E-Health : a global approach with extensive semantic variation*, in *J Med Syst.* 2012, 36(5) : 3173-3176.

L. MORLET-HAÏDARA, *Le système national des données de santé et le nouveau régime d'accès aux données : RD sanit. soc.* févr. 2018, n° 1, p. 91-105 [en ligne] ; *Données de santé : entre exploitation et protection, un numéro d'équilibriste : Dict. perm. Biotechnologies* juin 2018, bull. 293-1, 43 p.

H. MUIR WATT, *La fonction économique du droit international privé : RID éco.* 2010, t. XXIV, 1, (1), 103-121.

C. NOIVILLE, *Séquencer en routine le génome entier des patients ? Une réflexion juridique*, in *Droit, Santé et Societé* avr. 2019, n° 1-2, p. 77-81.

C.D. NORMAN et *al.*, *eHealth Literacy : Essential Skills for Consumer Health in a Networked World*, in *J Med Internet Res.* 2006 ;8(2) :e9.

Z. OBERMEYER, B. POWERS, C. VOGELI et *al.*, *Dissecting racial bias in an algorithm used to manage the health of populations*, in *Science* 2019, vol. 366, n° 6464, p. 447-453.

H. OH et *al.*, *What Is eHealth : A Systematic Review of Published Definitions*, in *J Med Internet Res* 2005 ;7(1) :e1.

V. PAGEOT, *Promotion et prévention de la santé*, in *Cahiers français* févr. 2019, n° 408, p. 52-62.

C. PAGLIARI et *al.*, *What Is eHealth : A Scoping Exercise to Map the Field*, in *J Med Internet Res* 2005 ;7(1) :e9.

D. PEIRIS, J. J. MIRANDA et D. C. MOHR, *Going beyond killer apps : building a better mHealth evidence base : BMJ Global Health* 2018 ;3 :e000676.

V. PEUGEOT, *Données de santé : contours d'une controverse : L'Économie politique* avr. 2018, n° 80, p. 30-41.

PFOSS Auvergne-Rhône Alpes, *Les usages du numérique par les publics fragiles : levier ou frein pour l'accès aux droits ?*, in *Focus de la PFOSS* n° 29, déc. 2018, 22 p.

C. POMMIÈS et J.-F. WILLEMS, *Parallel trade in the pharmaceutical sector : An overview of EU and national case law : e-Competitions* nov. 2016, n° 43745, p. 1 à 23.

D. PON, *Une approche raisonnée et progressive de la transformation numérique*, in *Techniques hospitalières : La revue des technologies de la santé* juin 2019, n° 776 [en ligne].

A.-Y. PORTNOFF et J.-F. SOUPIZET, *Intelligence artificielle : opportunités et risques : Futuribles* 2018/5, n° 426, p. 5 à 26.

N. POSTEL-VINAY et *al.*, *Observance et nouvelles technologies : nouveau regard sur une problématique ancienne*, in *Med Sci* (Paris) 2018 ; 34 :723-729.

N. QUENEL-TUEUX, *Du big data aux objets connectés*, in *Gestions hospitalières* avr. 2018, n° 575, p. 238-246.

L. RACHET JACQUET, L. TOULEMON, V. RAIMOND et A. DEGRASSAT-THÉAS, *Le prix des médicaments en France : Présentation Synthétique des évolutions récentes du système français de fixation des prix, RF aff. soc.* 2018/3, p. 47 à 67.

L. DE LA RAUDIÈRE, *La fabrique de la loi à l'ère du numérique : Enjeux numériques : Annales des mines – Réalités industrielles* sept. 2018, n° 3, p. 73.

V. RIALLE, *Robotique humanitaire versus robotique suicidaire : ou comment ré-enchanter la « silver économie »*, in *Droit, Santé et Societé* 2018, n° 3-4, p. 17-25.

L. ROBINSON et *al.*, *Digital inequalities and why they matter, Information : Communication & Society* 2015, vol. 18, n° 5.

J.-L. ROMANENS, *L'ordonnancement de la loi de santé 2016*, in *Revue Droit et santé. La revue juridique des entreprises de santé* mars 2018, n° 82, p. 197-210.

E. RUSSELL-MINDA et *al.*, *Health technologies for monitoring and managing diabetes : a systematic review*, in *J Diabetes Sci Technol*, 2009.

M. DE SAINT PULGENT, *L'État malade de sa complexité : Le Débat* 2019/4, n° 206, p. 156 à 166.

J. SAISON-DEMARS, F. LENOIR et L. TILMAN, *L'information en droit de la santé dans tous ses états : RGDM* déc. 2018, n° 69, p. 15-151.

L. SARDI et *al.*, *A systematic review of gamification in e-Health*, in *J Biomed Inform* 2017.

B. SCALA, *E-santé : la médecine à l'ère du numérique : Science & Santé* 2016(29) : 33-33, tab., graph., fig.

I. SILVA, *10 years of the French Autorité de la concurrence : looking back and looking ahead. Journal Of Antitrust Enforcement* 2019, (129-136), Retrieved 8 May 2020, from.

P. SIMON, *Télémédecine. Impacts du décret, évolutions, perspectives, enjeux : Revue hospitalière de France* 2011, (539) : 68-74, ill ; *Les pratiques de télémédecine ayant fait leur preuve : ADSP* déc. 2017, n° 101, p. 15-18.

P. SIMON et P. GAYRARD, *Télémédecine, Des pratiques innovantes pour l'accès aux soins : ADSP* déc. 2017, n° 101.

F. STASSE, *Le savoir ne dit rien sur la morale : Les Tribunes de la santé* 2016, n° 52, p. 99.

J. STEPHENS et *al.*, *Mobile phone interventions to increase physical activity and reduce weight : a systematic review*, in *J Cardiovasc Nurs* 2013 ; 28(4) :320-9.

C. SUAREZ, *La télémédecine : quelle légitimité d'une innovation radicale pour les professionnels de santé ? : Revue de l'IRES* 2002, vol. 2, n° 39, p. 157-186.

M. SWAN, *Emerging patient-driven health care models : An examination of health social networks, consumer personalized medicine and quantified self-tracking*, in *International Journal of Environmental Research and PublicHealth* 2009 ; 6(2), 492-525.

E. TAÏEB, *Transhumanisme et santé parfaite : Quaderni* 2020, 99-100, 125-135.

A. VIDAL-NAQUET, *Le citoyen co-législateur : quand, comment, pour quels résultats ?* ; *La e-santé : Gestions hospitalières* 2015 (551), 594-623 ; *Danemark : Le système de santé numérique de demain : Hospital Partenaire* déc. 2012, n° 26, p. 106-110 ; *Germany expanding digitalisation with the new Digital Care Act : Health Europa* 23 juill. 2019.

L. VOGEL, *Concurrence : plaidoyer pour une vraie réforme*, in *Mél. en l'honneur du Professeur B. Teyssié*, LexisNexis, 2019.

Y. WANG et *al.*, *A Systematic Review of Application and Effectiveness of mHealth Interventions for Obesity and Diabetes Treatment and Self-Management*, in *Adv Nutr* 15 May 2017 ;8(3) :449-462.

J.R. WEARING et *al.*, *iPhone app adherence to expert-recommended guidelines for pediatric obesity prevention*, in *Child Obes* 2014 ;10(2) :132-44.

P.-L. WEIL-DUBUC, *Big Data : amélioration technique, dégradation ou transformation du modèle de solidarité ?*, in *Revue d'épidémiologie et de santé publique* févr. 2019, vol. 67, suppl. 1, p. S19-S23.

D. WEISS et *al.*, *Innovative technologies and social inequalities in health : A scoping review of the literature*, in *PLoS ONE* 2018 ; 13(4) : e0195447.

B. WILLEMIN, *Numérisation des données de soin : impact sur l'élaboration et les fonctions du dossier médical*, in *Droit, Santé et Société* 2018, n° 5-6, p. 33-41.

W. ZIRAR, *« Hacking Covid-19 » : cinq projets retenus pour aider les professionnels de santé face à l'épidémie*, TIC Santé, 22 avr. 2020 ; *Comme l'hygiène sanitaire, l'hygiène numérique doit rentrer dans les mœurs des professionnels de santé (Anssi)*, TIC santé, 20 sept. 2019 ; *Covid-19 : le ministère référence les outils numériques à destination des usagers, professionnels et éditeurs*, TIC Santé, 14 avr. 2020 ; *Grand Est : l'e-santé en fer de lance pour lutter contre l'épidémie de Covid-19*, TIC Santé, 15 avr. 2020.

## 3. Publications

C. CARENINI, *Bénéfice de la cartographie des processus en support de la documentation qualité dans l'industrie pharmaceutique*, Sciences pharmaceutiques, 2019.

T. DOUSSON, *Digitalisation en production pharmaceutique : vers l'industrie 4.0*, Sciences pharmaceutiques, 2020 (dumas-02532560).

C. GENÈVE, *État des lieux de la E-santé en 2020, étude d'une application mobile de santé*, *Sciences pharmaceutiques*, 2020.

A. JOUVE, *Les stratégies d'accès au marché des solutions de e-santé*, Sciences pharmaceutiques, 2017.

G. MATTHIEU, *La dématérialisation de la vente de médicaments. Impact économique sur la profession et sur le patient*, Sciences pharmaceutiques, 2016.

A. NGUYEN VAN TY, *Pourquoi l'intégration du digital est nécessaire dans l'industrie pharmaceutique*, Sciences pharmaceutiques, 2018.

F. ROY, *Le numérique au service de la santé*, Sciences pharmaceutiques, 2019.

C. SEUX, *Transformation digitale de l'industrie pharmaceutique : état des lieux, opportunités et challenges*, Sciences pharmaceutiques, 2017.

M. UCCIANI, *Comment les entreprises peuvent-elles stratégiquement utiliser le canal digital pour accompagner la commercialisation d'un médicament ? Cas appliqué à MSD France*, Sciences pharmaceutiques, 2018.

J. VANNI, *Stratégies des laboratoires pharmaceutiques face au GAFAM*, Sciences pharmaceutiques, 2018.

## 4. Livres blancs

L. AUTELITANO et *al.*, *Livre blanc : Réseaux sociaux et Santé : un enjeu pour le suivi des patients et la recherche scientifique*, Healthcare Data Institute, sept. 2018, 31 p.

J.-P. BLUM, *Livre blanc : Contribution des outils numériques à la transformation des organisations de santé, Paroles d'acteurs*, t. 1, 2019.

CONSEIL NATIONAL DE L'ORDRE DES MÉDECINS, Livre blanc, *Santé connectée. De l'e-santé à la santé connectée*, janv. 2015, 36 p.

ENOVACOM, *L'interopérabilité, clé du partage des données et de la coordination des professionnels de santé. Le patient et ses données au cœur du parcours de soins*, Livre blanc, 2018, 64 p.

RENAISSANCE NUMÉRIQUE, Livre blanc, *17 experts/ 36 propositions pour une politique e-santé ambitieuse*, mars 2017.

UMVELT, *Le Livre Blanc des Living Labs*, Montréal, 1re éd., mars 2014, 133 p.

## 5. Dossiers de presse

COMITÉ INTERMINISTÉRIEL DE LA TRANSFORMATION PUBLIQUE, *Action Publique 2022, 100 % des démarches administratives accessibles en ligne d'ici 2022*, Dossier de presse, févr. 2018, 16 p.

CONSEIL NATIONAL DE L'INDUSTRIE, *Signature du CSF Industries et technologies de santé*, Dossier de presse, 4 févr. 2019.

MINISTÈRE DE LA SANTÉ ET DES SPORTS, Dossier de presse du programme de relance du DMP, 9 avr. 2009.

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ, *Ma Santé 2022, un engagement collectif*, Dossier de presse, 18 sept. 2018 ; *Stratégie de transformation du système de santé*, Dossier de presse, 13 févr. 2018.

RÉGION ÎLE-DE-FRANCE, *Smart Région Initiative*, Dossier de presse, 21 nov. 2017, 28 p.

## 6. Études, rapports, avis

AGENCE RÉGIONALE DE SANTÉ ÎLE-DE-FRANCE, Projet régional de santé Île-de-France 2013-2017, Bilan, Synthèse transversale, mai 2017, 100 p.

M. ARRABIT, *L'approvisionnement des pharmacies d'officine : quelles solutions en 2020 ?*, Sciences du Vivant [q-bio], 2020 (dumas-02970014).

ASIP-SANTÉ, *Observatoire des signalements des incidents de sécurité des systèmes d'information pour le secteur santé*. Rapport public sur la 1re année de mise en œuvre du dispositif (oct. 2017-sept. 2018), 24 p.

ASSEMBLÉE NATIONALE, Rapport d'information déposé par la Commission des affaires européennes sur le droit européen de la concurrence face aux enjeux de la mondialisation, n° 2451, 2019.

ASSISTANCE PUBLIQUE-HÔPITAUX DE PARIS (AP-HP), Plan stratégique télémédecine 2017-2022.

AUTORITÉ DE LA CONCURRENCE, déc. n° 17-D-25, 20 déc. 2017, relative à des pratiques mises en œuvre dans le secteur des dispositifs transdermiques de fentanyl ; avis n° 19-A-08, 4 avr. 2019, relatif aux secteurs de la distribution du médicament en ville et de la biologie médicale privée ; *Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques*, 19 févr. 2020.

AUTORITÉ DE LA CONCURRENCE ET BUNDESKARTELLAMT, *Algorithms and Competition*, 2019 ; *Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques*, 2020 ; Rapport annuel 2019, 2020.

M. BÉJEAN et *al.*, *Petit guide d'exploration au pays de la santé numérique*, Rapport d'étude pour la Fondation de l'Avenir et la Mutualité française, 2015, 31 p.

P. BOUET et J.-M. MOURGUES (ss dir.), *Atlas de la démographie médicale en France, Situation au 1er janvier 2018*, Conseil national de l'Ordre des médecins, 2018.

N. BRUN et *al.*, Rapport de la mission « Nouvelles attentes du citoyen, acteur de santé », Paris, Ministère chargé de la santé, Doc. fr., 2011, 46.

BVA, *E-santé : Usages et attentes des Français*, 1er juin 2017 ; *Le numérique : inclusion ou exclusion*, Digital Society Forum, 2018.

L. CADIET, Rapport de la mission d'étude et de préfiguration de l'ouverture au public des décisions de justice, *L'open data des décisions de justice*, remis à la garde des Sceaux, ministre de la Justice, nov. 2017, Recomm. n° 20, p. 25.

CAISSE NATIONALE DE L'ASSURANCE MALADIE (CNAM), Rapport au ministre chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et des produits de l'Assurance maladie au titre de 2018, *Améliorer la qualité du système de santé et maîtriser les dépenses. Propositions de l'Assurance Maladie pour 2018*, juill. 2017, 206 p. ; Rapport au ministre chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et des produits de l'Assurance maladie au titre de 2019, *Améliorer la qualité du système de santé et maîtriser les dépenses. Propositions de l'assurance maladie pour 2019*, juill. 2018, 253 p.

J.-N. CARDOUX et Y. DAUDIGNY, *Accès aux soins : promouvoir l'innovation en santé dans les territoires*, Sénat, Rapport d'information n° 686, juill. 2017, 129 p.

CENTRE DE RECHERCHE POUR L'ÉTUDE ET L'OBSERVATION DES CONDITIONS DE VIE (CREDOC), *Baromètre du numérique 2018*, Document réalisé pour le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGE), l'Autorité de régulation des communications électroniques et des postes (ARCEP) et l'Agence du numérique, 2018 ; *Baromètre du numérique 2019 : ibid.*, 2019.

CIGREF, *Synthec Numérique. Éthique et numérique. Un référentiel pratique pour les acteurs du numérique*, oct. 2018, 18 p.

COLLECTIF IM(PATIENTS CHRONIQUES ET ASSOCIÉS (ICA), *L'impact des nouvelles technologies sur la santé et la qualité de vie des personnes vivant avec une maladie chronique*, Institut Mines Telecom Business School, févr. 2019, 52 p.

COLLECTIF INTERASSOCIATIF SUR LA SANTÉ (CISS), *Le numérique en santé. « Pour un patient acteur de la qualité de son parcours de santé »*, Note de position commune, sept. 2016, 44 p.

COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ (CCNE), avis n° 130, *Données massives et santé : Une nouvelle approche des enjeux éthiques* [en ligne], Paris, CCNE, 2019 ; *Numérique et Santé, quels enjeux éthiques pour quelles régulations ?*, Rapport du groupe de travail commandé par le CCNE avec le concours de la commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene (CERNA), 19 nov. 2018, 100 p.

COMMISSION EUROPÉENNE, *Ententes et abus de position dominante : ASPEN propose de réduire de 73 % les prix de six médicaments anticancéreux dont le brevet est arrivé à expiration afin de dissiper*

*les craintes de la Commission quant à une tarification excessive*, 2020 ; *Inception impact assessment : New Competition Tool*, 2020 ; Rapport d'enquête sur le secteur pharmaceutique, 15 janv. 2008.

CONFÉRENCE NATIONALE DE SANTÉ, *Dialogue citoyen, Applications numériques et objets connectés : comment en faire des outils pour lutter contre les inégalités de santé ? Synthèse des travaux*, Paris, 29 nov. 2017, 22 p.

CONSEIL D'ÉTAT, *Révision de la loi de bioéthique : quelles options pour demain ?*, Étude à la demande du Premier ministre, Section du rapport et des études, 28 juin 2018, 262 p.

CONSEIL NATIONAL DE LA CONSOMMATION, avis, *Objets connectés en santé*, 7 juill. 2017, 7 p.

CONSEIL NATIONAL DE L'INDUSTRIE, *Contrat stratégique de filière Industries et technologies de santé*, 2019.

CONSEIL NATIONAL DE L'ORDRE DES MÉDECINS (CNOM), J. LUCAS et S. UZAN, *Médecins et patients dans le monde des data, des algorithmes et de l'intelligence artificielle : Analyses et recommandations du CNOM* [en ligne], Paris, CNOM, janv. 2018 ; *Éthique du numérique en santé*, J. LUCAS, vice-président du CNOM, 20 juin 2018, 5 p.

CONSEIL NATIONAL DU NUMÉRIQUE (CNNum), *La santé, bien commun de la société numérique : Construire le réseau du soin et du prendre soin*, Rapport remis à la Ministre des Affaires sociales, de la Santé et des Droits des femmes, oct. 2015,128 p. ; *Confiance, innovation, solidarité : pour une vision française du numérique en santé*, 2020 ; *Transformation de l'État : dépasser la norme par la pensée design*, nov. 2019 ; *Citoyens d'une société numérique. Accès, Littératie, Médiations, Pouvoir d'agir : pour une nouvelle politique d'inclusion*, oct. 2013, 380 p ; *L'accessibilité numérique, entre nécessité et opportunité, Une obligation légale vis-à-vis des citoyens. Un levier stratégique pour les acteurs*, 2020 ; *Concurrence et régulation sur l'environnement des plateformes et le numérique. Étude de cas sur l'interopérabilité des réseaux sociaux*, juill. 2020.

CONSEIL SUPÉRIEUR DE L'AUDIOVISUEL (CSA), *L'exclusion numérique des personnes âgées*, Étude réalisée par le CSA pour les Petits Frères des Pauvres, 27 sept. 2018 ; CSA RESEARCH, *Enquête sur « l'illectronisme » en France*, mars 2018, 39 p.

COUR DES COMPTES, *L'avenir de l'assurance maladie. Assurer l'efficience des dépenses, responsabiliser les acteurs*, Rapport public thématique, nov. 2017 ; *Les services publics numériques en santé : des avancées à amplifier, une cohérence à organiser*, Rapport public annuel 2018, févr. 2018 ; *La Sécurité sociale : rapport sur l'application des lois de financement de la Sécurité sociale*, Doc. fr., sept. 2017, 729 p. ; *La sécurité sociale*, sept. 2007 ; *Le coût du dossier médical personnel depuis sa mise en place*, Communication à la commission des finances de l'Assemblée nationale, juill. 2012.

A. COURY et D. PON, *Rapport final « Accélérer le virage numérique », Stratégie de transformation du système de santé*, Ministère des Solidarités et de la Santé, 2018.

M. CUGGIA, D. POLTON, G. WAINRIB et S. COMBES, *Health Data Hub – Mission de préfiguration*, Ministère des solidarités et de la santé, oct. 2018, 110 p.

Y. DAUDIGNY et J.-P. DECOOL, Rapport d'information fait au nom de la mission d'information sur la pénurie de médicaments et de vaccins, Rapp. Sénat n° 737, 27 sept. 2018.

DÉFENSEUR DES DROITS, *Dématérialisation et inégalités d'accès aux services publics*, janv. 2019, 71 p.

C. DE GANAY et D. GILLOT, *Pour une intelligence artificielle maîtrisée, utile et démystifiée*, Les Rapports de l'OPECST, Assemblée nationale, Sénat, 2017, 273 p.

I. DE SILVA, *The future of competition law : time to change or time to adapt?*, Lecture, Fordham Conference, 2019.

DIRECTION DE LA RECHERCHE, DES ÉTUDES, DE L'ÉVALUATION ET DES STATISTIQUES (DREES), *Renoncement aux soins pour raisons financières*, Dossiers solidarité et santé, juill. 2015, n° 66 ; *E-santé : les principaux outils numériques sont utilisés par 80 % des médecins généralistes de moins de 50 ans*, Études et Résultats, janv. 2020, n° 1139.

M. DUBREUIL, *E-santé : décryptage des pratiques et des enjeux*, Observatoire régional de santé Île-de-France, 2019.

H. DUMEZ, L. MARRAULD et E. MINVIELLE, *États des lieux de l'innovation en santé numérique : Working Paper* 2015, 15-CRG-01, 66 p.

N. DURANTON, Rapport d'information fait au nom de la délégation française à l'Assemblée parlementaire du Conseil de l'Europe sur les actes du colloque « Droits de l'Homme et démocratie à l'ère numérique », organisé le 14 novembre 2019, dans le cadre de la présidence française du Comité des ministres du Conseil de l'Europe, 6 déc. 2019.

J.-F. ELIAOU et A. DELMONT-KOROPOULIS, *L'évaluation de l'application de la loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique*, fait au nom de l'OPECST, Rapp. Sénat n° 80, 25 oct. 2018, 128 p.

EUROPEAN COMMISSION, Report from the commission to the Council and the european Parliament, *Competition enforcement in the pharmaceutical sector (2009-2017)*, 2019 ; *eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century*, Brussels, 6 déc. 2012 : Doc. COM (2012), 736 final, 14 p. ; *Provision of a market study on telemedicine*, Final Report, oct. 2018, 132 p.

FONDS D'INTERVENTION RÉGIONAL (FIR), Rapport d'activité 2017, Secrétariat général des ministères chargés des affaires sociales, oct. 2018, 80 p.

FRANCE STRATÉGIE, *Les bénéfices d'une meilleure autonomie numérique*, Rapport au secrétaire d'État chargé du numérique auprès du Premier ministre, juill. 2018, 80 p.

M. GAGNEUX et *al.*, *Pour un dossier patient virtuel et partagé et une stratégie nationale des systèmes d'information de santé*, Mission de relance du projet de Dossier médical personnel, Recommandations à la ministre de la Santé, de la Jeunesse, des Sports et de la Vie associative, 2008.

GROUPE DE TRAVAIL 28 DU COMITÉ STRATÉGIQUE DE FILIÈRES (GT 28 CSF), *Créer les conditions d'un développement vertueux des objets connectés et des applications mobiles en santé*, Ministère des Affaires sociales et de la Santé, Ministère de l'Économie, de l'Industrie et du Numérique, Alliance eHealth France, janv. 2017, 214 p.

P. GRUNY, Rapport d'information sur l'accompagnement de la transition numérique des PME : comment la France peut-elle rattraper son retard ? fait au nom de la délégation aux entreprises, Rapp. Sénat n° 635, 4 juill. 2019.

HAUTE AUTORITÉ DE SANTÉ, *Efficience de la télémédecine : état des lieux de la littérature internationale et cadre d'évaluation*, Rapport d'évaluation médico-économique, juill. 2013 ; *Numérique : quelle (R)évolution ?*, Rapport d'analyse prospective 2019 ; *Guide sur les spécificités d'évaluation clinique d'un dispositif médical connecté (DMC) en vue de son accès au remboursement*, janv. 2019, 20 p. ; Rapport préalable, *Expérimentations relatives à la prise en charge par télémédecine – Article 36 de la LFSS 2014*, sept. 2016, 62 p. ; *Référentiel de bonnes pratiques sur les applications et objets connectés en santé (Mobile Health ou mHealth), Évaluation et amélioration des pratiques*, oct. 2016, 60 p.

HEALTH PRODUCTS REGULATORY AUTORITY (HPRA), *Guide to Good Distribution Practice of Medicinal Products for Human Use*, 9 mars 2021.

INSEE, *Les Tableaux de l'économie française, édition 2011*, 23 févr. 2011.

INSPECTION GÉNÉRALE DES FINANCES (IGF), INSPECTION GÉNÉRALE DES AFFAIRES SOCIALES (IGAS), CONSEIL GÉNÉRAL DES TECHNOLOGIES DE L'INFORMATION (CGTI), Rapport sur le dossier médical personnalisé, 2007.

INSTITUT DE RECHERCHE ET DOCUMENTATION EN ÉCONOMIE DE LA SANTÉ (IRDES), *La e-santé Télésanté, santé numérique ou santé connectée*, Bibliographie thématique, juill. 2019.

INSTITUT MONTAIGNE, *Justice : faites entrer le numérique*, nov. 2017.

INSTITUTE OF MEDICAL SCIENCES (IMS), *Patient Adoption of mHealth. Use, Evidence and Remaining Barriers to Mainstream Acceptance*, IMS Institute for Healthcare Informatics, sept. 2015, 63 p.

IPSOS, *Les médecins à l'ère du numérique*, 31 janv. 2017.

H. ISAAC, *D'un système de santé curatif à un modèle préventif grâce aux outils numériques*, Paris, Renaissance numérique, 2014, p. 108 et 123.

J.-J. JÉGOU, *L'informatisation dans le secteur de la santé : prendre enfin la mesure des enjeux*, Rapport d'information de la commission des finances du Sénat, 3 nov. 2005 ; *Systèmes d'information de santé : le diagnostic est posé, le traitement s'impose*, Rapport d'information de la commission des finances du Sénat, 17 oct. 2007.

K. KIDHOLM et *al.*, *REgioNs of Europe WorkINg toGether for HEALTH*, Final Report Public. *Renewing Health projet*, 25 juin 2014, 72 p.

E. KLEINPETER, *Quatre enjeux éthiques de la « e-santé »*, Institut des sciences de la communication (CNRS, Université Paris Sorbonne, Université Pierre et Marie Curie), France, Paris, Communication, 2015, 5 p.

N. LEMAIRE, Rapport au Parlement sur les expérimentations innovantes en santé (article 51 de la loi de financement pour la sécurité sociale pour 2018), Ministère des Solidarités et de la Santé, 2019.

LES ENTREPRISES DU MÉDICAMENT (LEEM), *La E-santé en chiffres et en images*, 20 avr. 2018.

G. LONGUET, Rapport fait au nom de la commission d'enquête sur la souveraineté numérique, Président M. F. MONTAUGÉ, Rapp. Sénat n° 7, 1er oct. 2019.

G. LONGUET et C. VILLANI, Rapport au nom de l'OPECST sur l'intelligence artificielle et les données de santé, Rapp. Sénat n° 401, compte-rendu de l'audition publique du 21 février 2019.

MACSF ET WITHINGS, *Les professionnels de santé et les objets connectés*, 2016, 36 p.

S. MARINEAU, P. PLANTE et G. DESJARDINS, *Service de conception de jeux numériques pour la santé et le bien-être des aînés : résultats d'une revue de littérature*, Communication présentée à la CIRTA, *Le numérique au-delà de la classe : vers une plus grande hybridation*, Université de Sherbrooke, oct. 2019.

F. MARTY, *Économie des algorithmes et ordre concurrentiel : réflexions sur les abus d'exploitation et les collusions fondés sur des algorithmes de prix [Ebook]*, GREDEG, 2017, mise à jour 8 mai 2020.

MM. H. MAUREY et L.-J. de NICOLAY, *Aménagement du territoire : plus que jamais une nécessité* fait au nom de la commission de l'aménagement du territoire et du développement durable, Rapp. Sénat n° 565 (2016-2017) déposé le 31 mai 2017, 126 p.

A. MAYÈRES, *L'e-santé et la question des inégalités sociales de santé*, in *Les inégalités sociales de santé*, Actes du séminaire de recherche de la DREES, 2015-2016, oct. 2017, 294 p.

M. MERCIER et R.-P. SAVARY, Rapport d'information fait au nom de la délégation sénatoriale à la prospective sur robotisation et emplois de service, Rapp. Sénat n° 162, 28 nov. 2019.

C. MILLION, Rapport fait au nom de la commission des affaires sociales sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, relatif à l'organisation et à la transformation du système de santé, 22 mai 2019.

MINISTÈRE CHARGÉ DE LA SANTÉ, *Stratégie nationale pour le développement de l'e-santé : Le numérique au service de la modernisation et de l'efficience du système de santé*, 2016 ; *Faire en sorte que les applications et objets connectés en santé bénéficient à tous*, avis, 8 févr. 2018, 2 vol. ; *Ma santé 2022 : un engagement collectif*, Paris, 2018 ; *Stratégie de transformation du système de santé*, Paris, 2018 ; *Ma santé 2022 : un engagement collectif, Feuille de route « Accélérer le virage numérique »*, Dossier d'information, Paris, 2019.

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES, *Services publics numériques : Cédric O lance les ateliers d'écoute*, 14 janv. 2020 ; *Industrie du futur : enjeux et perspectives pour la filière industries et technologies de santé*, Prospective, coll. « Études économique », juin 2019, 185 p. ; *Intelligence artificielle – État de l'art et perspectives pour la France*, Prospective, coll. « Études économiques », févr. 2019, 333 p.

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES, SECRÉTARIAT D'ÉTAT AUPRÈS DU MINISTRE DE L'ÉCONOMIE ET DES FINANCES, INSPECTION GÉNÉRALE DES FINANCES, *La politique de la concurrence et les intérêts stratégiques de l'UE*, 2019.

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ, *Stratégie nationale de la Santé, Feuille de route*, 23 sept. 2018 ; *Art. 51 – Innovation en santé. Mise en œuvre du dispositif en 2018*, Rapport au conseil stratégique, 2018, 28 p. ; *Ma Santé 2022, un engagement collectif, À l'hôpital, le numérique est partout. Ensemble,*

*rendons-le plus sûr*, Dossier d'information, Campagne nationale d'information sur la cybersécurité en santé, 28 nov. 2019 ; *Ma Santé 2022, un engagement collectif, Avancement du « virage numérique en santé »*, déc. 2019 ; colloque *Données de Santé et Intelligence Collective*, 18 nov. 2019 ; *Les Français et les objets connectés*, Enquête réalisée par IFOP, juill. 2017, 32 p.

ORDRE NATIONAL DES MÉDECINS, *Éthique dans les usages du numérique en santé*, Journée organisée par le Conseil national de l'Ordre des médecins, 14 nov. 2012.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *La littératie à l'ère de l'information*, Rapport final de l'Enquête internationale sur la littératie des adultes, juin 2000, 208 p. ; *Understanding the Digital Divide*, Paris, OCDE, 2001, 32 p. ; *Adapter la politique de la concurrence à l'ère du numérique*, 2017 ; *Algorithms and Collusion : Competition Policy in the Digital Age*, 2017 ; *Science, technologie et innovation : perspectives de l'OCDE*, 2018, 54 p. ; *Adapter la politique de la concurrence à l'ère du numérique*, 2016.

ORGANISATION MONDIALE DE LA SANTÉ (OMS), Projet de stratégie mondiale pour la santé numérique 2020-2024.

A. PERROT, S. CATOIRE, V. BLONDE, H. MARITON et A. ROPARS, Rapport, *La politique de la concurrence et les intérêts stratégiques de l'UE*, IGF, avr. 2019.

L. PIERON et A. EVENNOU, *La santé à l'heure de l'intelligence artificielle*, Paris, Terra Nova, 2017, 131.

PÔLE INTERMINISTÉRIEL À LA PROSPECTIVE ET À L'ANTICIPATION DES MUTATIONS ÉCONOMIQUES (PIPAME), *E-santé : faire émerger l'offre française en répondant aux besoins présents et futurs des acteurs de santé*, Étude commandée par la Direction générale des entreprises (DGE), 2016, 120 p.

P. PRIBILLE et N. NADET, *Stratégie de transformation du système de santé – Rapport final : Repenser l'organisation territoriale des soins*, Ministère des Solidarités et de la Santé, sept. 2018, 22 p.

PRICEWATERHOUSE COOPERS (PwC), *Socio-economic impact of mHealth : an assessment report for the European Union*, 2013, p. 28.

J. ROSS et *al.*, *Factors that influence the implementation of e-health : a systematic review of systematic reviews (an update)*, 26 oct. 2016.

ROYAL SOCIETY FOR PUBLIC HEALTH (RSPH), *Social media and young people's mental health and wellbeing*, 2017, 32 p.

M.-O. SAFON, *La e-santé : télésanté, santé numérique ou santé connectée, bibliographie thématique*, Centre de documentation de l'Institut de recherche et de documentation en économie de la santé, juill. 2019.

SECRÉTARIAT D'ÉTAT CHARGÉ DU NUMÉRIQUE, *Ensemble pour un numérique inclusif*, Rapport préparé en collaboration avec WeTechCare / Emmaüs Connect, Mission Société Numérique et La MedNum, 2018.

SERVICE NUMÉRIQUE DE SANTÉ (SESAN), Rapport d'activité 2017, 122 p.

TASK FORCE « RÉFORME DU FINANCEMENT DU SYSTÈME DE SANTÉ », *Réforme des modes de financement et de régulation. Vers un modèle de paiement combiné*, Ma Santé 2022, 2019.

A.M. TOTTEN et *al.*, *Telehealth : Mapping the Evidence for Patient Outcomes From Systematic Reviews*, Technical Brief n° 26. AHRQ Publication n° 16-EHC034-EF. Rockville, MD : Agency for Healthcare Research and Quality, juin 2016, 125 p.

G. TURAN-PELLETIER et H. ZEGGAR, Rapport IGAS, *La distribution en gros du médicament en ville*, juin 2014.

C. VILLANI et *al.*, *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, Rapport de la mission parlementaire, mars 2018, 235 p.

WHO, *Guideline : recommendations on digital interventions for health system strengthening*, World Health Organization, 2019.

WHO EUROPE, *From innovation to implementation. eHealth in the WHO European Region*, 2016, 116 p.

## 7. Jurisprudence

Cass. com., 18 oct. 2016, arrêt n° 890, n° 15-10.384.

Cass. com., 11 janv. 2017, arrêt n° 33, n° 15-17.134.

CJCE, 8 juill. 1999, aff. C-49/92, *Anic Partecipazioni SpA*.

CJUE, 11 sept. 2014, aff. C-67/13, *Groupement des cartes bancaires* c/ *Commission*.

## 8. Textes législatifs et réglementaires

### 1) France

Arrêté portant approbation d'un avenant modifiant la convention constitutive du groupement d'intérêt public « Agence nationale des systèmes d'information partagés de santé », 19 déc. 2019, Ministère des Solidarités et de la Santé.

Arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de Covid-19 dans le cadre de l'état d'urgence sanitaire, 21 avr. 2020.

Instruction n° SG/DSSIS/2017/8, 10 janv. 2017, relative à l'organisation à déployer pour la mise en œuvre de la stratégie d'e-santé en région.

L. n° 2004-810, 13 août 2004, relative à l'assurance maladie : *JO* 17 août 2004.

L. n° 2016-1321, 7 oct. 2016 pour une République numérique : *JO* 8 oct. 2016.

L. n° 2016-41, 26 janv. 2016 de modernisation de notre système de santé : *JO* 27 janv. 2016.

L. n° 2017-1836, 30 déc. 2017 de financement de la sécurité sociale pour 2018 : *JO* 31 déc. 2017.

L. n° 2019-774, 24 juill. 2019, relative à l'organisation et à la transformation du système de santé : *JO* 26 juill. 2019.

### 2) Europe

COMMISSION EUROPÉENNE, déc. n° M.8677, 6 févr. 2019, *Siemens/Alstom*.

CONSEIL DES COMMUNAUTÉS EUROPÉENNES, règl. (CE) n° 139/2004, 20 janv. 2004, relatif au contrôle des concentrations entre entreprises.

PARLEMENT EUROPÉEN, Résolution du Parlement européen sur les options de l'Union européenne pour améliorer l'accès aux médicaments (2016/2057[INI]), 2 mars 2017.

PARLEMENT EUROPÉEN ET CONSEIL DE L'UNION EUROPÉENNE, règl. (UE) n° 2016/679, 27 avr. 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).

PARLEMENT EUROPÉEN ET CONSEIL DE L'UNION EUROPÉENNE, règl. (UE) n° 2017/745, 5 avr. 2017, relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

PARLEMENT EUROPÉEN ET CONSEIL DE L'UNION EUROPÉENNE, dir. 2007/47/CE, 5 sept. 2007 modifiant la directive 90/385/CEE du Conseil concernant le rapprochement des législations des États membres relatives aux dispositifs médicaux implantables actifs, la directive 93/42/CEE du Conseil relative aux dispositifs médicaux et la directive 98/8/CE concernant la mise sur le marché des produits biocides.

# Glossaire

***Accountability :*** Obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

**Agence du numérique en santé :** L'Agence agit en coordination étroite avec la délégation ministérielle au numérique en santé, afin de mettre en œuvre les orientations dédiées au secteur de la santé et du médico-social. L'Agence agit sur la construction du cadre de la e-santé en France. Elle s'occupe des questions de sécurité des systèmes d'information ou des messageries de santé, mais aussi de l'interopérabilité des systèmes. Elle intervient sur les enjeux de labels et certifications, comme la certification « Hébergeur en données de santé ».

**Agent intelligent :** Entité autonome capable de percevoir son environnement grâce à des capteurs et d'agir sur celui-ci.

**Aidant :** Personne, le plus souvent bénévole, qui assiste une personne dépendante dans sa vie quotidienne.

**Algocratie :** Néologisme indiquant un pouvoir qui fonde sa légitimité sur une optimisation numérique de la gestion de l'information sociale, et susceptible de concurrencer la démocratie.

**Algorithme :** Un algorithme, notion à la fois mathématique et informatique, est la spécification de la série d'opérations et d'instructions à réaliser pour résoudre un problème ou obtenir un résultat. Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. L'algorithme est traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur.

**Alphabétisation numérique :** Fait de rendre quelqu'un habile dans la navigation entre les flux d'informations. Cela va de pair avec une réduction de la fracture numérique.

**Analyse prédictive :** Ensemble des technologies d'analyse de données et de statistique, destinées à produire des prédictions, ou hypothèses prédictives, et/ou des modèles statistiques sur des événements susceptibles de se produire.

**Anonymisation des données :** Résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification de personne. Elle permet de préserver les avantages de l'exploitation des bases de données, tout en respectant le droit de chacun à la protection de ses données.

**Anthropomorphisme :** Attribution de caractéristiques du comportement humain ou de la morphologie humaine à d'autres entités, comme des choses telles que des robots dotés d'IA, et attribution d'une existence propre inhérente à ces objets en question.

**API :** Programme informatique permettant la communication et l'échanges de données entre applications et systèmes hétérogènes, sans intervention humaine.

**Applications santé (Apps) :** Des pratiques médicales et de santé publique supportées par des appareils mobiles, tels que les téléphones mobiles, les dispositifs de surveillance des patients, les *Personal Digital Assistant* (PDA) et autres appareils sans fil (OMS).

**Apprentissage automatique (ou *machine learning*) :** Branche de l'intelligence artificielle axée sur des processus d'apprentissage permettant à une machine d'évoluer, sans que ses algorithmes soient modifiés. L'algorithme d'apprentissage automatique comporte un modèle dont il modifie les paramètres de valeur initiale en général aléatoire en fonction du résultat constaté. Il existe plusieurs types de *machine learning :* statistique, supervisé (c'est-à-dire dont les règles d'apprentissage sont définies à partir d'une base d'exemples), non supervisé.

**Apprentissage par renforcement :** Processus par lequel l'IA s'améliore à partir de l'expérience sans recours à la programmation humaine. Apprentissage automatique dans lequel un programme extérieur évalue positivement ou négativement, les résultats successifs permettant à l'algorithme d'améliorer ses performances jusqu'à atteindre l'objectif préalablement fixé. Le plus souvent, l'intelligence artificielle aura accès aux données et utilisera celles-ci pour apprendre.

**Apprentissage profond (*deep learning*) :** Méthode de *machine learning* faisant partie du champ de recherche « Apprentissage Automatique » de l'intelligence artificielle. Apprentissage automatique qui utilise un réseau de neurones artificiels composé d'un grand nombre de couches dont chacune correspond à un niveau croissant de complexité dans le traitement et l'interprétation des données.

Le *deep learning* permet un apprentissage non supervisé. Il s'appuie sur l'analyse d'un modèle de données. Il est notamment adapté à la reconnaissance d'images.

**Apprentissage supervisé/non supervisé :** L'apprentissage supervisé et l'apprentissage non supervisé désignent deux méthodes d'éducation de l'IA. La première utilise des jeux de données « étiquetées » par l'homme qui permettent à l'intelligence artificielle d'apprendre à partir des étiquettes et de généraliser ses apprentissages à de nouveaux cas. L'apprentissage non supervisé ne nécessite pas d'étiquettes, et il revient à l'IA d'attribuer une catégorie aux résultats.

• **Apprentissage non supervisé :** Apprentissage automatique dans lequel l'algorithme utilise un jeu de données brutes et obtient un résultat en se fondant sur la détection de similarités entre certaines de ces données.

• **Apprentissage supervisé :** Apprentissage automatique dans lequel un algorithme s'entraîne à une tâche déterminée en utilisant un jeu de données assorties d'une annotation indiquant le résultat attendu.

**Arbre de décision :** Représentation graphique, sous forme d'arbre ou d'arborescence, des règles entrant dans le processus de prise de décision. L'arbre de décision est composé de nœuds de décision et de branches. Utilisé dans la *machine learning*, il permet de calculer différents résultats en fonction de la décision prise, et de faire des prédictions en se basant sur des calculs de probabilités.

**Autoapprentissage :** Apprendre à partir d'une base de données de connaissances interne, sans intervention d'une base de connaissances externe.

**Autonomie numérique :** Aptitude du robot à exécuter des tâches prévues à partir de son état actuel et de sa capacité de détection, sans intervention humaine.

**Autonomisation :** Le regain de pouvoir du patient ; phénomène traduisant la recherche toujours plus approfondie, par les patients, de l'origine de leurs maux et la nature du traitement prodigué. Il peut comprendre l'autodiagnostic par les patients de leur état de santé (*empowerment* du patient).

**Base de connaissances :** Ensemble des informations relatives à un sujet donné. Une base de connaissances comporte l'ensemble du savoir que l'expert d'un domaine doit maîtriser pour pouvoir exercer son expertise.

**Base de données :** Collecte de données organisées selon une structure conceptuelle décrivant les caractéristiques de ces données et les relations entre leurs entités correspondantes, prenant en charge un ou plusieurs domaines d'application.

**BATX :** Acronyme de Baidu, Alibaba, Tencent et Xiaomi, plateformes numériques concurrentielles à l'instar des GAFAM.

***Big data :*** Ensemble très volumineux de données générées et gérées par les nouvelles technologies. Les ensembles de données traités correspondant à la définition du *big data* répondent à trois caractéristiques principales : volume, vélocité et variété. (mégadonnées ou données massives).

**Bioéthique :** Considérée comme l'une des branches de l'éthique, elle étudie les questions et les problèmes moraux et éthiques qui peuvent apparaître à l'occasion de pratiques médicales nouvelles impliquant la manipulation d'êtres vivants ou de recherche en biologie. La bioéthique est une réflexion sur les progrès de la recherche dans les domaines de la biologie, de la médecine et de la santé.

**Bionique :** Science qui a pour objet l'amélioration de la technologie en tirant profit de l'analyse des processus biologiques observés chez les êtres vivants.

**Biovigilance :** Vigilance sanitaire, élément du dispositif de veille sanitaire qui vise à optimiser la sécurité d'emploi des produits sanitaires destinés à l'homme et des produits à finalité cosmétique ou d'hygiène corporelle. Elle a pour objet la surveillance des événements indésirables ou des accidents liés à l'utilisation de ces produits, par un processus continu de recueil, d'enregistrement, d'identification, de traitement, d'évaluation et d'investigation de ces événements ou accidents par une agence de santé (en France l'Agence nationale de sécurité du médicament et des produits de santé [ANSM]).

***Blockchain :*** Technologie de stockage et de transmission d'informations, transparente, sécurisée et fonctionnant sans organe central de contrôle. La *blockchain* se matérialise comme un registre distribué et décentralisé partagé entre différents acteurs.

La chaîne de blocs est un mode d'enregistrement de données produites en continu sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, les blocs et séquences sont protégés contre toute modification. Parmi ses utilisations, la mise en place de contrat intelligent (ou *smart contract*) et l'exécution automatique des conditions du contrat, ainsi que la traçabilité des produits et services notamment de santé et de leurs *datas*, depuis leur fabrication jusqu'à leur livraison ou exécution. La *blockchain* est donc une base de données distribuée (c'est-à-dire répartie sur de nombreux systèmes informatiques) de manière transparente, sécurisée, et fonctionnant sans organe central de contrôle.

***Blog :*** Carnet web sur lequel des personnes morales ou physiques affichent un contenu.

***Botnet :*** Machines zombies, réseaux de machines infectées par un logiciel malveillant permettant le contrôle à distance.

***B to B to C :*** *Business to Business to Consumer*. Service proposé par une entreprise à un distributeur qui le revend à ses clients.

***B to C :*** *Business to Consumer*. Service proposé par une entreprise à des particuliers consommateurs.

**Capteur :** Dispositif permettant de mesurer un phénomène physique, il fournit un signal en relation avec la mesure de ce phénomène.

**CERT (*Computer Emergency Response Team*) :** Centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises et aux administrations.

**Certification de produit ou service :** Activité par laquelle un organisme, distinct du fabricant, de l'importateur, du vendeur, du prestataire de services, de l'utilisateur, ou patient consommateur, atteste qu'un produit, un service ou une combinaison de produits et de services est conforme à des caractéristiques décrites

dans un référentiel de certification. Le référentiel de certification est un document technique définissant les caractéristiques que doit présenter un produit ou un service ou une combinaison de produits et services, et les modalités de contrôle de la conformité à ces caractéristiques. L'élaboration du référentiel de certification incombe à l'organisme certificateur qui recueille le point de vue des parties intéressées (C. consom., art. L. 433-3). Il s'agit de l'organisme notifié pour les dispositifs médicaux (« Procédures de certification de conformité » des dispositifs médicaux : C. santé publ., art. R. 5211-25 à R. 5211-53).

***Chatbot*** (ou agent conversationnel) : Programme d'intelligence artificielle qui imite une conversation humaine interactive par échange vocal ou textuel. À distinguer de « dialogueur ».

**CI-SIS (Cadre d'interopérabilité des systèmes d'information de santé) :** Ce référentiel spécifie les standards (le plus souvent internationaux) à utiliser dans les échanges et lors du partage de données de santé entre systèmes d'information de santé (SIS), et contraint la mise en œuvre de ces standards par des spécifications d'implémentation destinées à faciliter le déploiement de l'interopérabilité entre SIS dans les conditions de sécurité requises.

***Cloud* ou *Cloud computing* :** Modèle qui permet un accès omniprésent, pratique et à la demande à un réseau partagé et à un ensemble de ressources informatiques.

**Consentement :** Dans le cadre médical, toute personne doit être présumée capable *a priori* de recevoir des informations et de donner un consentement « libre et éclairé » à un acte médical qu'on lui propose, à moins qu'il n'ait été établi que cette capacité lui faisait défaut (C. santé publ., art. L. 1114-4 et R. 4127-36, C. déont. méd., art. 34).

Dans le cadre contractuel, le consentement exige que la personne soit saine d'esprit pour consentir à une opération contractuelle. (C. civ., art. 1129 à 1144).

Dans le cadre du traitement des données (RGPD) : « consentement » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

**Cybercriminalité :** Actes contrevenant aux traités internationaux et aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime ou les ayant pour cible. La cybercriminalité est définie par le ministère de l'Intérieur comme l'« ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication de type Internet ».

**Cyberdéfense :** Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'informations jugés essentiels.

**Cyberespace :** Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

**Cyberharcèlement :** Toute forme de harcèlement moral ou sexuel commis au moyen d'un réseau de communication électronique et sanctionné pénalement (C. pén., art. 222-33-2-2).

**Cyberinfrastructure :** Ensemble des nouveaux environnements de recherche qui intègrent des fonctions avancées d'acquisition, de stockage, de gestion, d'intégration, de fouille, de visualisation des données, ou d'autres services de traitement informatique ou informationnel.

**Cyborg :** terme de science-fiction indiquant un humain amélioré ou transformé par la technique.

***Deep learning :*** Sous-domaine du *machine learning* qui traite des modèles de « réseaux de neurones profonds ». L'apprentissage profond est un type d'intelligence artificielle où la machine est capable d'apprendre par elle-même, contrairement à la programmation où elle se limite à exécuter les règles prédéfinies.

**Destinataire des données :** La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

**Dialogueur :** Logiciel spécialisé dans le dialogue en langage naturel avec un humain, qui est capable de répondre à des questions ou de déclencher l'exécution de tâches. Il peut être intégré à un terminal ou à un robot intelligent.

***Digital Health :*** En anglais et « Santé numérique » en français.

**Digitalisation ou transformation numérique :** Ce phénomène va de pair avec l'IA, car il s'agit de produire et d'exploiter des données. Cette action s'opère dans tous les secteurs.

Dans le cadre de l'hôpital, la digitalisation permet de dématérialiser les processus ou les supports de travail comme les dossiers médicaux dont le format papier disparaît peu à peu.

**Dispositif médical :** Dispositif médical (DM) correspondant à tout instrument, appareil, équipement, matière, produit (à l'exception des produits d'origine humaine), y compris les accessoires et logiciels, utilisé seul ou en association, à des fins médicales chez l'homme, et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques, immunologiques ou métaboliques (C. santé publ., art. L. 5211-1).

**Dispositif mobile :** Dispositif numérique, léger et autonome, dont les spécificités techniques assurent potentiellement une connexion permanente

à Internet et permettent le traitement des données sans appareil complémentaire. Classiquement, les dispositifs mobiles désignent les smartphones et les tablettes tactiles.

**Dispositif nomade :** Les dispositifs nomades regroupent l'ensemble des matériels permettant le stockage et/ou l'utilisation des données numériques. Les dispositifs nomades passifs permettent le transport des données mais nécessitent un autre appareil (fixe ou mobile) pour les utiliser. À la différence des dispositifs mobiles, les dispositifs nomades ne sont pas potentiellement autonomes d'un point de vue de la connexion à Internet.

**Données anonymisées :** Données pour lesquelles tout lien avec l'identité directe ou indirecte de la personne est supprimé. Les données n'ont plus de caractère personnel, la personne ne peut plus être identifiée.

**Données biométriques :** Données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

**Données de santé :** Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne. Trois types de données sont recueillies : les informations relatives à une personne physique (collectées lors de l'admission dans un établissement de soin), les informations obtenues lors d'un examen particulier (y compris à partir des données génétiques et biologiques), et les informations concernant une maladie précise.

**Données génétiques :** Données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

**Données personnelles :** Une donnée personnelle est constituée par toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.

L'article 4 du règlement général sur la protection des données (RGPD) définit les « données à caractère personnel » comme toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »), et « est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments

spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

**Données sensibles :** Les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue 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 relatives à la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le règlement européen interdit de recueillir ou d'utiliser ces données.

**Dossier médical partagé (DMP) :** Outil permettant de contribuer à la continuité et à la coordination des soins en ville et à l'hôpital. Carnet de santé numérique qui conserve et sécurise les données. Il permet aux professionnels de santé d'accéder au dossier médical du patient et contribue à la traçabilité de l'évolution de l'état de santé du patient ainsi qu'à la coordination des soins.

**Échange de données de santé :** Communication d'informations à un ou plusieurs destinataires clairement identifiés par un émetteur connu.

**E-inclusion :** Inclusion sociale dans une société et une économie où le numérique joue un rôle essentiel.

**Équipe de soins :** Ensemble des professionnels qui participent directement au profit d'un patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation de handicap, ou de prévention de perte d'autonomie, ou à leur coordination. L'organisation de l'équipe de soins est régie par le Code de la santé publique (C. santé publ., art. L. 1411-11-1).

**Équipe de soins spécialisés :** Ensemble de professionnels de santé constitué autour de spécialistes d'une ou plusieurs spécialités hors médecine générale.

**Équipe primaire de soins :** Ensemble des professionnels de santé constitué autour de médecins généralistes de premier recours.

**E-santé :** Santé numérique en français, et *e-health* en anglais. Désigne l'utilisation intégrée des technologies de l'information et de la communication pour l'organisation, le soutien et la mise en réseau de tous les processus et acteurs du système de santé avec ses équivalents. Beaucoup de termes sont utilisés dans le domaine de l'e-santé qui regroupe de nombreux éléments : de la santé numérique à la santé digitale : télésanté, santé numérique, santé connectée, l'e-santé désigne tous les domaines où les technologies de l'information et de la communication (TIC) sont mises au service de la santé, telle qu'elle a été définie par l'Organisation mondiale

de la santé (OMS) en 1945. Elle désigne une santé qui passe par les évolutions technologiques, numériques et les réseaux sociaux.

Il existe des décalages entre l'e-santé « outil » (produit), mis en avant par les acteurs économiques, et l'e-santé « pratique de soins » (service), promue par la puissance publique. L'e-santé est, en effet, à la fois un marché et une façon de concevoir les politiques publiques pour les autorités sanitaires.

**Espace numérique de santé (ENS) :** Plateforme numérique publique, personnelle et personnalisable, mise à disposition de chaque personne dès sa naissance, lui permettant de gérer ses données de santé et de participer à son parcours de santé.

**Éthique *by design* :** Il s'agit de la phase de conception des outils numériques et de déontologie des concepteurs numériques quels qu'ils soient (développeurs, *designers* numériques, chef de projets, *etc.*).

**Éthique des usages :** Réflexion éthique sur l'usage que fait l'homme des ressources technologiques qu'il a à sa disposition.

**Éthique médicale :** Elle est fondée sur quatre grands principes : autonomie, bienfaisance, non-malfaisance et justice.

**Éthique sociétale :** Elle traite, notamment, de l'acceptabilité des innovations et solutions numériques, de l'économie et du *design* de l'attention, de l'empreinte écologique et énergétique du numérique, de l'inclusion sociale, *etc.*

**Fichier :** Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

**Fracture digitale** ou **fracture numérique :** La fracture digitale ou numérique désigne l'inégalité d'accès et/ou d'usage aux technologies d'information et de communication. Cette fracture peut être économique, sociale ou géographique.

**GAFAM :** Acronyme formé avec les initiales des noms de cinq grandes entreprises américaines, souvent qualifiées de géants du web : G pour Google, F pour Facebook, M pour Microsoft et les deux A pour Apple et Amazon.

**Groupements régionaux d'appui au développement de l'e-santé (GRADeS) :** Groupement qui fédère les acteurs régionaux autour de la stratégie régionale d'e-santé, promeut l'usage des services numériques en santé dans les territoires et apporte son expertise aux acteurs régionaux.

**Hôpital numérique :** La stratégie hôpital numérique définit un plan de développement et de modernisation des systèmes d'information hospitaliers (SIH) et

a pour but de fixer des priorités et des objectifs à six ans, en mobilisant tous les acteurs concernés et en accompagnant les établissements de santé dans leur transformation par les technologies de l'information et de la communication.

**Identité nationale de santé :** L'identité nationale de santé (INS) est l'un des éléments socles de la feuille de route du numérique en santé. L'utilisation de l'INS pour référencer les données de santé est obligatoire depuis le 1er janvier 2021. Chaque personne dispose d'une identité unique et pérenne qui permet de faciliter l'échange et le partage des données de santé entre l'ensemble des acteurs intervenant dans la prise en charge sanitaire et le suivi médico-social de la personne. Cela contribue à la qualité de la prise en charge et à la sécurité des soins.

**Identité numérique :** Lien technologique entre une entité réelle (la personne) et une entité virtuelle (sa ou ses représentations numériques). Elle se construit à partir de plusieurs éléments : les données personnelles associées à son ou ses profils, les informations qu'elle publie sur le web, les informations que d'autres publient à son sujet, les traces qu'elle laisse.

**Illectronisme :** Néologisme apparu récemment pour désigner l'illettrisme numérique et informatique. L'illectronisme fait référence aux difficultés vis-à-vis des outils numériques, qu'il s'agisse de leur manipulation en tant que telle ou de l'incapacité à accéder aux contenus de l'information numérique et à les comprendre.

**Innovation :** « La mise en œuvre d'un produit (bien ou service) ou d'un procédé nouveau ou sensiblement amélioré, d'une nouvelle méthode de commercialisation ou d'une nouvelle méthode organisationnelle dans les pratiques de l'entreprise, l'organisation du travail ou les relations extérieures » (Organisation de coopération et de développement économiques [OCDE], *Manuel d'Oslo*, 2005).

**Innovation adjacente :** Consiste à lancer un produit déjà existant, qu'il soit à son état initial ou qu'il ait subi une innovation incrémentale, en lui attribuant un nouvel usage, cela entraîne la création d'un nouveau marché.

**Innovation continue ou incrémentale :** Consiste à améliorer des produits ou services déjà existants pour en optimiser la production et l'utilisation et répondre aux attentes des utilisateurs.

**Innovation de rupture :** Consiste à lancer un produit ou un service déjà existant à un coût moindre avec une utilisation simplifiée afin qu'il soit accessible au plus grand nombre.

**Innovation inversée :** Conçue dans un pays émergent ou en développement pour le marché local et qui est diffusée dans les pays développés.

**Innovation ouverte :** Processus d'innovation mis en place par une organisation, qui fait appel à divers partenaires extérieurs, en recourant notamment à des pratiques participatives et à l'ouverture des données.

**Innovation radicale :** Consiste à créer un nouveau produit sur un nouveau marché sans lien avec un besoin ou une demande de la société. Le changement engendré par cette nouveauté est radical et généralement risqué.

**Intégrateur :** Toute personne qui conçoit, fabrique ou assemble des systèmes robotisés pour un utilisateur. L'intégrateur assume généralement le statut juridique de fabricant (Dir. 2006/42/CE, relative aux machines).

**Intelligence artificielle :** Ensemble de concepts et technologies visant la résolution de problèmes à forte complexité logique ou algorithmique. Développement de traitements de système de données qui exécutent des fonctions normalement associées à l'intelligence humaine comme le raisonnement critique, l'organisation de la mémoire et l'apprentissage. En médecine, l'IA vise à améliorer les diagnostics médicaux ou les choix thérapeutiques. Certains systèmes d'IA utilisent la logique, c'est-à-dire l'approche dite « symbolique ». Ce sont des systèmes experts d'aide à la décision ou de gestion des connaissances. D'autres utilisent une approche « numérique » qui raisonne sur les données et cherche des régularités dans les données disponibles pour extraire des connaissances, sans modèle préétabli.

**Intelligence artificielle distribuée (IAD) :** Branche de l'intelligence artificielle dont le but est de créer des systèmes décentralisés, généralement multiagents, capables de coopérer et de se coordonner. L'intelligence artificielle distribuée étudie les techniques permettant à des agents autonomes d'interagir, et les moyens de répartir un problème entre ces agents.

**Intelligence artificielle faible :** Fait référence au fonctionnement d'un système qui simule un comportement intelligent dans un domaine restreint.

**Intelligence artificielle forte :** Capacité de résoudre des problèmes complexes dans n'importe quel environnement avec un niveau égal ou supérieur à l'intelligence humaine. Aptitude d'une machine capable non seulement de reproduire les capacités de réflexion et d'interaction intelligentes, mais aussi d'avoir une « conscience », des « sentiments » et la compréhension de ses propres raisonnements.

**Interopérabilité :** Définition de langages communs aux systèmes d'information amenés à les manipuler de manière à éviter la définition de nouveaux langages et donc de nouveaux développements à chaque fois que deux systèmes d'information veulent échanger ou partager des données (Agence du numérique en santé [ANS]).

**Intimité :** Protection contre l'intrusion dans la vie privée ou les affaires d'une personne physique lorsque cette intrusion résulte d'une collecte ou d'une utilisation indue ou illégale des données sur cette personne.

***IoT* (*Internet of Things*) :** En français : Internet des objets. Le terme fait référence aux réseaux d'objets connectés.

**Langage algorithmique :** Langage artificiel pour exprimer des algorithmes.

**Langage artificiel :** Langage dont les règles sont explicitement établies avant son utilisation.

**Littératie en e-santé :** Elle nécessite six compétences fondamentales : alphabétisation traditionnelle, santé, information, science, médias et informatique.

**Littératie numérique :** L'OCDE la définit comme l'aptitude à comprendre et à utiliser le numérique dans la vie courante, à la maison, au travail et dans la collectivité en vue d'atteindre des buts personnels et d'étendre ses compétences et capacité.

***Living Lab* :** Méthode de recherche en innovation ouverte qui vise le développement de nouveaux produits et services. Cette approche promeut un processus de co-création avec les usagers finaux dans des conditions réelles et s'appuie sur un écosystème de partenariats public-privé-citoyen.

**Logiciel :** Ensemble composé d'un ou plusieurs programmes ainsi que des fichiers nécessaires pour les rendre fonctionnels. Un logiciel est conçu pour qu'une machine (par ex. un ordinateur) puisse accomplir certaines tâches.

***Machine learning* :** Appelé en français « apprentissage automatique » ou statistique, il est au centre de l'intelligence artificielle. Il utilise une variété d'algorithmes qui apprennent itérativement à partir de données pour améliorer, décrire les données et prédire les résultats.

**Médiation numérique :** Mise en capacité de comprendre et maîtriser les technologies numériques, leurs enjeux, leurs usages, pour développer une culture numérique de tous, et agir dans la société numérique.

**Medtech :** Entreprises exploitant les technologies de l'information dans le domaine médical afin de proposer des services médicaux innovants.

**Métadonnées :** Données sur des données, ou des éléments de données, y compris éventuellement leurs descriptions, et données sur la propriété des données, les chemins d'accès, les droits d'accès et la volatilité des données.

**M-santé (Mobile-santé) :** Désigne l'ensemble des produits ou services liés à la santé *via* l'utilisation de dispositifs mobiles tels que les smartphones, les systèmes de suivi à distance, les assistants numériques personnels et autres appareils sans fil.

**Nanotechnologies :** Recherche sur les principes et propriétés existant à l'échelle nanométrique, c'est-à-dire au niveauw des atomes et des molécules. L'objectif des nanotechnologies consiste à produire des objets ou matériaux inférieurs à 100 nanomètres qui pourront dans le domaine de la santé intégrer les médicaments, dispositifs médicaux, autres produits et matériaux à usage médical.

**Numérique en santé :** Le numérique en santé constitue un ensemble de processus informatisés dans le domaine de la santé, qu'ils impliquent ou non de l'intelligence artificielle ou de la robotique.

**Objet connecté :** Objet qui capte, stocke, traite et transmet des données, qui peut recevoir et donner des instructions ou accomplir des actions spécifiques en fonction des informations reçues, et qui a pour cela la capacité à se connecter à un réseau d'information.

**Observance :** En anglais : *compliance*. Respect par le patient de son traitement prescrit par le médecin.

***Open data :*** Les données ouvertes ou *open data* sont des données numériques dont l'accès et l'usage sont laissés libres aux usagers. Elles peuvent être d'origine publique ou privée, produites notamment par une collectivité, un service public, un collectif citoyen ou une entreprise.

***Open source :*** La désignation *open source*, ou « code source ouvert » en français, s'applique aux logiciels dont la licence respecte des critères précisément établis par l'organisation *Open Source Initiative*, c'est-à-dire les possibilités de libre redistribution, d'accès au code source et de créer des travaux dérivés.

**Parcours de soins :** Organisation et coordination entre les acteurs des secteurs sanitaires, médico-sociaux, et sociaux en lien avec les usagers, patients, collectivités territoriales afin d'assurer la continuité, l'accessibilité, la qualité, la sécurité et l'efficience de la prise en charge de la population, en tenant compte des spécificités géographiques, démographiques et saisonnières de chaque territoire, afin de concourir à l'équité territoriale (C. santé publ., art. L. 1411-1).

**Partage de données :** Mise à disposition de catégories de professionnels fondés à en connaître des informations respectant les conditions de confidentialité et de sécurité.

***Patient Empowerment :*** Processus de transformation personnelle par lequel les patients renforcent leur capacité à prendre effectivement soin d'eux-mêmes et de leur santé, et pas seulement de leur maladie et de leur traitement comme décrit le plus souvent dans la littérature médicale.

**Professionnels de santé :** Professionnels visés à la quatrième partie du Code de la santé publique. Sont concernés les professions médicales, pharmaceutiques, auxiliaires médicaux.

**Profilage :** Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

**Progrès :** Évolution des sciences, des arts, des études techniques qui participent à l'amélioration de la condition humaine : longévité, confort de vie, santé, éducation, culture et souci des autres (à distinguer de l'innovation).

**Protection de la vie privée :** Dans le secteur du numérique, sont visées toutes les mesures prises pour assurer la confidentialité, par la protection des données, les limitations de la collecte, la combinaison et le traitement des données sur les individus. L'article 9, alinéa 1 du Code civil dispose : « Chacun a droit au respect de sa vie privée ». La jurisprudence considère comme des atteintes à la vie privée toutes les informations faisant intrusion dans l'intimité de la personne.

**Pseudonymisation :** 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. Ces informations supplémentaires doivent être 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.

***Quantified self :*** Littéralement, « mesure de soi ». Ce terme regroupe toute l'analyse de ses propres données personnelles notamment en utilisant tous les outils numériques.

**Randomisation :** Technique d'anonymisation qui consiste à modifier les valeurs réelles pour empêcher que les données anonymisées puissent être mises en relation avec les valeurs originales.

**Réalité augmentée :** Désigne une interface virtuelle, en 2D ou 3D, et vient enrichir la réalité en superposant des informations complémentaires.

**Réalité virtuelle :** Technologie qui permet de plonger une personne dans un monde artificiel créé numériquement. Elle est utilisée dans le domaine médical comme une nouvelle forme de prise en charge du patient.

**Régulation médicale :** Acte médical pratiqué au téléphone par un médecin d'un centre d'appels dédié aux urgences. Le médecin régulateur détermine et déclenche la réponse la mieux adaptée à l'état du patient, puis, si nécessaire, oriente le patient directement vers une unité d'hospitalisation appropriée.

**Réseau neuronal numérique ou artificiel :** Programme composé d'algorithmes reliés à la manière du cerveau humain**.** Ensemble de neurones artificiels interconnectés qui constituent une architecture de calcul.

**Responsable du traitement des données :** La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

**Robot :** Dispositif mécanique, programmable, conçu pour effectuer des tâches de manipulation ou de locomotion sous contrôle automatique.

**Robotique :** Branche de l'IA portant sur la conception et la fabrication de robots. Techniques impliquées dans la conception, la construction, l'utilisation de robots.

**Robotique médicale :** Assistance mécanique robotisée capable d'exécuter et d'accompagner le professionnel de santé dans le cadre d'une réhabilitation médicale, d'une rééducation et/ou d'une chirurgie.

**Science des données :** Extraction des connaissances exploitables à partir de données *via* un processus de découverte, ou d'hypothèse et de test d'hypothèse.

**Sécurité des réseaux et systèmes d'information :** Capacité des réseaux et des systèmes de résister à un niveau de confiance donnée, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

***Serious game* :** Application, d'un jeu qui permet au patient d'apprendre à mieux gérer sa maladie de manière ludique, ou encore à des professionnels en cours de formation de santé de pratiquer la médecine à travers une mise en pratique virtuelle.

**Sous-traitant des données :** La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

**Système national des données de santé :** Système regroupant les principales bases de données de santé publique existantes : données de l'Assurance maladie, activités des établissements de santé, causes des décès, données relatives au handicap et bientôt données provenant des complémentaires santé.

**Systèmes d'information en santé :** Systèmes permettent une meilleure coordination des soins au sein d'un établissement de santé (système d'information hospitalier [SIH], dossier patient informatisé [DPI], *etc.*) ou d'un territoire de soins (système d'information partagé de santé). Ils représentent l'ensemble des ressources utilisées par une structure pour la gestion de l'information, et qui comprend tous les équipements informatiques, les moyens de communication, et les données structurées ou non structurées.

**Technologie de rupture :** Innovation technologique qui porte sur un produit ou un service et qui finit par remplacer une technologie dominante sur un marché.

**Téléassistance :** L'assistance téléphonique, l'assistance en ligne ou encore l'assistance à distance désigne l'action ou le service qui permet d'aider à distance des utilisateurs, d'un système ou d'un produit, à l'aide d'un moyen de télécommunication.

**Téléconsultation :** Technique qui consiste à consulter un médecin à distance, à l'aide de technologies de communication comme l'appel vidéo depuis un smartphone ou un ordinateur. Le patient peut être assisté ou non d'un professionnel de santé comme un infirmier ou un pharmacien.

**Téléexpertise :** Pratique qui consiste à solliciter l'avis d'un professionnel de santé pour une spécialité donnée pour confirmer et/ou établir un diagnostic par une communication numérique.

**Télémédecine :** La télémédecine permet, entre autres, d'effectuer des actes médicaux dans le strict respect des règles de déontologie mais à distance, sous le contrôle et la responsabilité d'un médecin en contact avec le patient par des moyens de communication appropriés à la réalisation de l'acte médical.

**Télésanté :** Technique qui intègre des services de suivi et de prévention des individus dans un objectif principal de bien-être (objets connectés, applications mobiles d'automesure, plateforme web…).

**Télésoin :** Pratique de soins à distance utilisant les technologies de l'information et de la communication mettant en rapport un patient avec un ou plusieurs pharmaciens ou auxiliaires médicaux, infirmiers, orthophonistes, orthoptistes, maïeuticiens ou sages-femmes, masseurs-kinésithérapeutes, podologues et diététiciens.

**Télésuivi :** Technique permettant d'apporter au patient un suivi médical à distance par les technologies de l'information et de la communication.

**Télésurveillance :** Interpréter à distance les données d'utilisation d'un dispositif médical grâce au télésuivi, appelé aussi téléobservance. Le professionnel de santé peut ainsi prendre des décisions à distance sur la prise en charge du patient et le réajustement du traitement.

**Test de Turing :** Inventé par le mathématicien britannique Alan Turing en 1950, il est destiné à évaluer l'intelligence d'une machine ou d'un système.

**Traitement des données :** Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (RGPD, art. 4.2).

**Transhumanisme :** Courant de pensée qui prône l'utilisation de la science et de la technologie moderne pour améliorer les capacités physiques et mentales des êtres humains, *via* notamment un usage avancé des nanotechnologies et biotechnologies.

**Ubérisation :** Néologisme, le terme fait référence aux plateformes Uber en ligne qui réduisent le nombre d'intermédiaires et offrent des services à prix cassés.

**Violation de données à caractère personnel :** Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

# Table des matières

Photocomposition Nord Compo Multimédia
59650 Villeneuve-d'Ascq
Suivi éditorial : Manuella Guillot