Données de santé, dynamiques et enjeux de souveraineté

Erwan Pinilla

Université de Strasbourg

ÉCOLE DOCTORALE ED 101

Centre d'Etudes Internationales et Européennes

THÈSE

présentée par

Erwan PINILLA

soutenue le **23 novembre 2023**

pour obtenir le grade de docteur en droit
de l'université de Strasbourg

Données de santé, dynamiques et enjeux de souveraineté

THÈSE dirigée par :

Monsieur MEGERLIN Francis	Professeur, université de Strasbourg

RAPPORTEURS :

Madame LE GAL FONTES Cécile	Professeur, Université de Montpellier
Madame MULLER Yvonne	Professeur, Université Paris Nanterre

AUTRES MEMBRES DU JURY :

Monsieur NAËGELEN Emmanuel	GBA, Directeur général adjoint, ANSSI
Monsieur PABST Jean-Yves	Professeur, université de Strasbourg

L'Université n'entend donner ni approbation ni improbation

aux opinions émises dans les thèses :

celles-ci doivent être considérées comme propres à leur auteur.

Ce travail reprend parfois *in extenso* des éléments de nos publications sur les points pertinents :

- Pinilla E, Megerlin F, « La donnée de santé « synthétique » en droit européen : un objet virtuel non (encore) identifié », Rev. Gén. Dr. Méd. 2024 (PDP), *à paraître*.
- Megerlin F, Pinilla E, Huriet Cl, « Règlement européen de 2021 sur l'évaluation des technologies de santé : place des données de 'vie réelle' ? » Rev. gén. dr. méd 2023 (PDP), 281-294.
- Megerlin F, Pinilla E, Huriet Cl, « Recueil de données sur les médicaments en accès précoce : quel lien avec la recherche 'impliquant' les personnes humaines ? » Rev. gén. dr. méd 2022 (PDP), 375-388.
- Megerlin F, Pinilla E, Huriet Cl, « Etudes observationnelles et données de santé « par destination » : quelles protections en droit ? » Rev. gén. dr. méd 2021 (PDP), 151-164.
- Pinilla E, Bordas P, Megerlin F, « Le juge européen et les services dématérialisés des professions réglementées : quelle pharmacie à l'aube du Digital Market Act ? » Rev. gén. dr. méd 2021 (PDP), 175-185.
- Pinilla E, Megerlin F, « De la donnée de santé par qualification de la loi, à la donnée de santé par destination », Rev. gén. dr. méd 2018 (PDP), 99-112.

Remerciements

A Monsieur le Professeur Francis Megerlin, ma profonde gratitude pour avoir accepté de diriger un doctorant atypique sur un sujet transverse, ainsi que mon fil rouge dans une optique finalement méthodologique ; pour sa confiance continue, sa vision systémique, son soutien moral, et son appui indéfectible à la finalisation de ce travail dans une période devenue difficile.

A Madame le Professeur Yvonne Muller, qui me fait l'honneur de siéger dans mon jury et qui a accepté de rapporter, pour son expertise en droit pénal notamment, et sa disponibilité malgré ses nombreuses obligations dans une période très dense.

A Madame le Professeur Cécile Le Gal Fontes, qui me fait l'honneur de siéger dans mon jury et qui a accepté de rapporter, pour son expertise en droit de la santé numérique notamment, et sa disponibilité malgré aussi un agenda particulièrement chargé le jour même de cette soutenance.

A Monsieur le Général Emmanuel Naëgelen, qui me fait l'honneur particulier de siéger dans mon jury, pour son expertise nationale en matière de gouvernance et de sécurité des systèmes d'information notamment, et pour sa disponibilité malgré l'ampleur de sa charge.

A Monsieur le Professeur Jean-Yves Pabst, qui me fait l'honneur de siéger dans mon jury, malgré les soucis qu'il a endurés, et pour son accueil avec tous ses collègues auprès du Centre d'Etudes Internationales et européennes de l'université de Strasbourg, lequel me laissera un excellent souvenir.

Ma gratitude également à **Monsieur le Professeur (h) Claude Huriet**, qui m'a honoré de sa confiance, en tant que co-auteur de publications qui furent autant d'étapes dans des questionnements successifs.

A ma famille, à mes amis, pour mes silences ombrageux qu'ils ont souvent du supporter… Cet engagement académique à mon âge sera je l'espère, un encouragement pour tous : comme le disent mon épouse et mes enfants, « oui, nous le pouvons » !

A mes collègues des ministères et agences, françaises et européennes, qui ont pu être étonnés que je me lance ce défi sans enjeu professionnel, pour le sens qu'ils donnent, contre vents et marées, à nos efforts communs.

Liste des acronymes utilisés

Certains acronymes anglo-saxons sont directement employés dans les publications françaises.

AAC : Autorisation d'accès compassionnel
AAP : Autorisation d'accès précoce
AFMIC : Armed Forces for Medical Intelligence Center
AI : IA (« intelligence artificielle »)
AI-SaMD : Artificial Intelligence based Software as Medical Devices
ANS : Agence du numérique en santé
ANSM : Agence nationale de sécurité des médicaments et produits de santé
ANSSI : Agence nationale de la sécurité des systèmes d'information
APT : Advanced Persistant Threat
ATIH : Agence technique de l'information sur l'hospitalisation
CASF : Code de l'Action Sociale et des Familles
CE : Conseil d'Etat
CEDH : Convention européenne des droits de l'homme
CEPD : Contrôleur européen de la protection des données, *ne pas confondre avec le Comité européen de la protection des données (désigné EDPB)*
CFIUS : Comittee on Foreign Investment in the United States
CGCS : Conseil de gestion des crises sanitaires
CIM : Classification Internationale des Maladies
Civ. : Chambre civile de la Cour de cassation
CJCE : Cour de justice des Communautés européennes (a précédé la CJUE)
CJUE : Cour de justice de l'Union européenne
CLOUD Act : Clarifying Lawful Overseas Use of Data Act
CNAM : Caisse Nationale d'Assurance Maladie
CNEDIMTS : Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (voir HAS)
CNIL : Commission nationale Informatique et Libertés
CNOM : Conseil National de l'Ordre des Médecins
CNOP : Conseil National de l'Ordre des Pharmaciens
Cour EDH : Cour européenne des droits de l'homme
CPMS : Clinical Patient Management System
CPP : Comité de protection des personnes se prêtant à la RIPH
Crim : Chambre criminelle de la Cour de cassation
CSIRT (également CERT) : centre de réponse aux incidents de sécurité informatique
CSP : Code de la santé Publique
CSS : Code de la Sécurité Sociale
CT : Commission de la Transparence (voir HAS)
CyCLONe : european CYber Crisis Liaison Organisation NEtwork
DARWIN : Data Analysis and Real World Interrogation Network
DM : Dispositif Médical
DMDIV : Dispositif Médical de Diagnostic *In Vitro*
DME : Dossier Médical Electronique
DMIL : Dispositif médical intégrant du logiciel
DNS : Délégation au Numérique en Santé
ECDC : Centre européen de prévention et de contrôle des maladies
EDPB : Comité européen de la protection des données, *ne pas confondre avec le CEPD (Contrôleur européen de la protection des données)*
EEDS : Espace Européen des Données de Santé

EHDEA : European Health and Digital Executive Agency
EMA : European Medicine Agency
ENISA : European Union Agency for Cybersecurity
ENS : Espace Numérique de Santé
EO : Executive Order
ETF : Emergency Task Force
ETS (HTA) : évaluation des technologies de santé
EUROJUST : Agence de l'Union européenne pour la coopération judiciaire en matière pénale
EUROPOL : l'Agence de l'Union européenne pour la coopération des services répressifs
FDA : Food & Drug Administration
FDC Act : Food Drug & Cosmetic Act
FISA : Foreign Intelligence Surveillance Act
FTC : Federal Trade Commission
GT article 29 : groupe de travail créé par l'article 29 de la directive 95/46 (devenu EDPB)
HAS : Haute Autorité de Santé
HERA : Health Emergency Preparedness and Response
HIPA Act : Health Insurance Portability and Accountability Act
HITECH Act : Health Information Technology for Economic and Clinical Health Act
IDS : Institut des données de santé
INSEE : Institut National de la Statistique et des Etudes Economiques
LFSS : Loi de Financement de la Sécurité Sociale
LIL : Loi Informatique et Libertés
MDIS : Medical Device Integrating Software
MR : Méthodologie de Référence à l'usage de la RIPH, établie par la CNIL
NCMI : National Centre for Medical Intelligence
OCDE : Organisation de Coopération et de Développement Economiques
OMS : Organisation Mondiale de la Santé
OSE : Organismes de Services Essentiels
PATRIOT Act : Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
PESC : Politique étrangère et de sécurité commune
PESD : Politique de sécurité et de défense commune
PGSSI : Politique Générale de Sécurité des Systèmes d'Information de Santé
PHI : Protected Health Information
PMSI : Programme de médicalisation des systèmes d'information
PUT-RD : Protocole d'utilisation thérapeutique - de recueil de données
RER : Réseau Européen de Référence
RGPD : règlement général sur la protection des données
RIPH : recherches Impliquant la personne Humaine
RNIPP : Répertoire national d'identification des personnes physiques
RWD : Real World Data (donnée de vie réelle)
SAFARI : Système Automatisé pour les Fichiers Administratifs et Répertoires des Individus
SAPR : Système d'alerte précoce et de réaction
SGDSN : Secrétaire général de la défense et de la sécurité nationale
SNDS : Système national des données de santé
SNIIRAM : Système National d'Information Inter Régimes d'Assurance Maladie
STAD : Système de Traitement Automatisé des Données
TFUE : Traité de fonctionnement de l'Union européenne
U.S. : Etats-Unis d'Amérique
UE : Union Européenne

Sommaire

Données de santé, dynamiques & enjeux de souveraineté

Introduction

1. **But de la recherche.** Cette recherche a pour but de relever les dynamiques de la « donnée de santé » dans le champ de la souveraineté numérique : qui peut par là décrire, expliquer, prédire des états et tendances en santé, induire des comportements individuels et/ou populationnels, voire étatiques ? **que protéger donc en droit, comment ?**
   Lors de notre inscription en thèse en 2017, l'objectif était la détection dans les interstices du droit et/ou de ses angles morts, de phénomènes transnationaux parfois encore inédits, pour l'aide à la décision publique. Cette recherche, conduite en parallèle de nos activités à temps plein au ministère, nous intéressait pour deux raisons.

   * **sur le fond :** amené à traiter certains de ces aspects à titre professionnel, nous en avons découvert la transversalité, donc le besoin d'approche systémique. Il fallait « naviguer » dans des champs juridiques variés (santé, sécurité sociale, civil, administratif, pénal, disciplinaire, constitutionnel ; droit français, comparé, européen, international), qui s'entrecroisent sans toujours de congruence. Pour autant, les observations qui justifient notre recherche, et les préconisations qu'elles ont pu parfois justifier n'ont, quand elles sont inédites, pas vocation à être publiées. Ma gratitude à mon directeur de thèse, qui a consenti à cette réduction au regard de nos échanges. On ne retrouvera ici **que le fil rouge du raisonnement**.

   * **sur le plan méthodologique :** à ce moment de mon parcours débuté tôt comme officier de marine, j'ai souhaité pouvoir formaliser des réflexions pour mon épanouissement intellectuel, et les potentialiser au service de l'intérêt général. Jusqu'alors, mes raisonnements étaient souvent empiriques et dédiés à une décision rapide ou rapprochée. Cela sans possibilité donc de structuration documentée ni de discussion suivie, du fait de l'alternance des affectations professionnelles. Cette thèse était ainsi l'opportunité d'une formation complémentaire, par le dialogue prolongé de méthodes et de paradigmes propre au monde académique.

Champ de la recherche

2. La « *souveraineté numérique* » dont participe notre sujet, désigne un vaste champ de réflexion et d'actions pour la maîtrise de notre destin national et européen. De conceptualisation récente, elle fait l'objet de nombreux travaux [1]. Notons seulement ici qu'elle est l'objet de politiques nationales et européenne qui visent le développement accéléré en propre, de capacités et de technologies numériques sur notre territoire : moteurs de recherche, logiciels, systèmes d'exploitation, outils d'intelligence artificielle, infrastructures de serveurs « en nuage » *(cloud)* [2], supercalculateurs, semi-conducteurs, mais aussi normes et schémas de certification de cybersécurité etc. et naturellement, protection et maîtrise de nos données.

3. Cela vise certes à éviter de devenir une « *colonie numérique* » [3], mais aussi à disposer de solutions efficientes et compétitives, et, par conséquent, à « *promouvoir l'Union en tant qu'actrice de premier plan dans la définition de normes à l'échelle mondiale dans le domaine de la santé numérique* », pour ce qui nous intéresse ici [4]. Dans ce foisonnement, nous n'approcherons que le lien entre cette souveraineté et les données personnelles de santé.

   * Pour autant, notre thème n'est **pas réductible à l'articulation entre droits de la santé, droits fondamentaux et libertés publiques,** objet de récents travaux magistraux [5]. Nous serons amenés à les citer mais, d'ordre interne et centrés sur notre système national, ils ne constituent pas notre sujet ; ou alors, ils n'intègrent pas cette question de souveraineté [6].

---

[1] Dernièrement, Coll. « Comprendre la souveraineté numérique », *Cahiers français*, n° 415, mai-juin 2020 ; pour une rétrospective de la notion par son initiateur, Bellanger, P. *La souveraineté numérique*, Paris, Stock Ed. 2014 ; Cardot, P. *Cybersouveraineté : mythe ou défi ?* Uppr Ed., 2016 ; Kempf, O. « *La France face au numérique : une souveraineté rénovée ?* », *Rev. Int. Strat*. n° 110, février 2018, p. 109-117.

[2] Nous ne développerons pas cet aspect particulier, intéressant du fait des décisions du Conseil d'Etat en référé, quant aux conditions et au futur de l'implication de la société américaine Microsoft dans l'infrastructure de la Plateforme des données de santé, CE (référés) 13 oct. 2020, n° 444937. Nous l'envisagerons en seconde partie sous l'angle de l'exposition des données au droit du lieu de localisation des serveurs.

[3] Morin-Desailly, C. rapport au Sénat, Rapport d'information n° 443 (2012-2013) ; égal. Rapport de Longuet, G. « Le devoir de souveraineté numérique », fait au nom de la commission d'enquête du Sénat, n° 7 tome I (2019-2020) - 1 octobre 2019. Depuis en 2020, création à l'Assemblée nationale d'une Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne », rapporteur Latombe, Ph. Rapport déposé à l'Assemblée nationale sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne », n° 4299 enregistré le 21 juin 2021.

[4] Introduction à la proposition en mai 2022, d'un espace européen des données de santé (EEDS), non paginé.

[5] Conseil d'Etat, « Santé et protection des données », La documentation française, 2019 ; Conseil d'Etat, « Révision de la loi de bioéthique : quelles options pour demain ? », Rapport à la demande du 1er ministre, rendu juin 2018 ; Cluzel-Metayer, D. « Les données de santé, ou le défi d'un partage sous haute protection », Actes du colloque 40ème anniversaire de l'AFDS, Rev. dr. san. soc. 2022, 149-158.

[6] Teller M., « La régulation des données de santé : entre intérêt général et intérêts particuliers », introduction au cahier spécial, RIDE 2022/3 (t 26), p5 ; Legros P., « L'impératif de sécurité des données de santé, de la nécessité technique à l'obligation juridique », ibid. pp 13-37.

*** L'ouverture des données publiques (*Open Data*) en santé procède aussi d'une réflexion différente** [7], sur l'opportunité de la mise à disposition des données, une fois rendues non personnelles [8]. Le rapport en 2020 de la « mission Bothorel » milite pour une ouverture plus importante des données, notamment quand leur production est financée par l'argent public [9]. Cette dynamique justifie que l'on s'interroge sur les limites d'une doctrine de transparence [10] dans un monde en repolarisation, marqué par des stratégies nationales d'opacification.

* D'autres publications **portent sur le « *business* » des données de santé**, mais souvent sans mise en perspective juridique, *a fortiori* internationale, et parfois dans une confusion affriolante [11]. En droit français, la qualification de « donnée de santé » interdit spécifiquement leur vente lorsqu'elles sont « *identifiantes directement* ***ou indirectement****, y compris avec l'accord de la personne concernée* », sous peine de sanction pénale [12]. Ainsi l'opinion est-elle sensible à un problème qu'elle pressent sans pouvoir le caractériser, et les décideurs publics sous la pression d'écrits volontiers polémiques.

En outre, sur la seule période 2017-2023, nombre d'initiatives nationales et européennes ont été mises en œuvre ou proposées notamment en santé, quant à la régulation des données ; à leurs protection, partage et usages ; à la mutualisation d'évaluations de technologie, la protection des produits, services, process et systèmes. Souvent pensées avant 2017, elles ont parfois été accélérées par la pandémie en 2020, puis par l'invasion de l'Ukraine en 2022.

4. Ces agendas et saccades ont fortement impacté nos activités et enrichi notre recherche. Inédit, le traitement **de la dynamique des données personnelles de santé sous l'angle de la souveraineté numérique** nous semblait ainsi d'une utilité depuis mise en exergue par une vive actualité. C'est pourquoi aussi, nous nous en tenons ici à notre fil rouge.

---

[7] Communiqué de presse préc., « Marisol Touraine lance le débat sur l'open data en santé » 21 nov. 2013.
[8] Dans une bibliographie abondante, voir notamment Lutun, A. « Le Big Data en santé, richesse et conditions d'accès », thèse pour le doctorat en droit, Paris, 2021, qui vaut synthèse actualisée.
[9] A la demande du 1er ministre : Bothorel E, Combes S, Vedel R, « Pour une politique publique de la donnée », décembre 2020, p. 6 et 8.
[10] Au plan intérieur, CE 30 juin 2023, n° 469964, qui valide la décision de la CNIL dans l'affaire « *Palmarès des hôpitaux » : la CNIL précise les raisons de son refus d'autoriser le Point à accéder à la base de données des hôpitaux »*, 10 nov. 2022 (site CNIL). Saisi par la CNIL, qui a suivi son avis, le Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) avait considéré que « *la construction des indicateurs retenus dans le palmarès peut conduire à diffuser une information erronée sur les performances relatives réelles des établissements de santé* ***pouvant induire en erreur les patients et être par conséquent contraire à l'intérêt public*** ». Pour une critique avertie, de Kervasdoué J, « Palmarès des hôpitaux du « Point » : les raisons profondes de la censure » *in* Le Point, 10 juillet 2023.
[11] En France, voir Boulard A, Favier-Baron E, Woillet S, *Le business de nos données médicales – enquête sur un scandale d'Etat* FYP éd. 2021 ; Nabat Y, *in* « Données de santé : entre permissivité juridique, biopolitique et néolibéralisme » (AOC, 2 mars 2021) ; Lemke C, *Ma Santé, mes données*, CPI éd. 2021.
[12] Articles L. 1111-8 – VII, CSP et 226-21 C. pénal.

Esquisse de définitions préalables

Qu'est-ce que « la santé » ?

5. La « santé » connaît nombre de définitions, mais **aucune n'est explicitement consacrée en droit français ni européen**, lesquels exposent nos ambitions collectives [13], énoncent des droits fondamentaux d'accès et leur garantie [14], puis en orchestrent la mise en œuvre nationale ou transfrontière : ils se gardent de définir la « *santé* » en soi, ou un droit « *à la santé* » [15].

   Or, la conception de la « santé » détermine l'ambition des politiques nationales ou régionales, les coûts des systèmes « de santé », les arbitrages (publics en France) quant aux prestations remboursables etc., et surtout, ici, la qualification des activités, technologies et données afférentes. Mais ces dernières **ne sont plus l'apanage des « systèmes de santé », et n'y sont plus encloses sous leur protection**, ce qui renouvelle le jeu des qualifications [16].

6. Trois définitions classiques suffisent pour en caractériser la complexité. Nous esquissons brièvement leur lien avec la production de données, non leur usage en santé publique [17].

   *** La première est négative et lapidaire :** la santé désigne « *l'absence de maladie ou d'infirmité* » [18]. Cette définition n'est pas si éloignée de la formule de monsieur R. Leriche en 1936 : « *La santé, c'est la vie dans le silence des organes* ». Mais son propos élevé est beaucoup plus fécond : il met en exergue le rôle fondamental en santé de la sémiologie [19] : **des signaux faibles peuvent annoncer une rupture d'équilibre / de compensation.**

---

[13] Article 11 du Préambule de la Constitution de 1946 dispose que la Nation « ***garantit à tous,*** *notamment à l'enfant, à la mère et aux vieux travailleurs****, la protection de la santé,*** *la sécurité matérielle, le repos et les loisirs* ». L'article L. 1110-1 CSP dispose que « *Le droit fondamental* ***à la protection de la santé*** *doit être mis en oeuvre par tous moyens disponibles au bénéfice de toute personne* (…) » ; voir les articles 9 et 168 §1du Traité sur le fonctionnement de l'Union européenne (TFUE).

[14] Article 35 de la Charte des droits fondamentaux de l'Union européenne.

[15] Pour une acception qui confond « *droit à la santé* » et droit aux soins, le dossier « Droit à la santé », *in* revue Projet 2008/3 (n°304), pp 35-75, not. Dinechin (de), O. « Les poussées d'un droit à la santé », 37-45.

[16] Pinilla E, Megerlin F, « De la donnée de santé par qualification de la loi, à la donnée de santé « par destination », Rev. gén. dr. méd 2018/1, 99-112 ; depuis, Burroni G., « L'influence de la finalité sur la qualification juridique des données de santé », Rev int. dr. éco 2022/3, pp 63-76.

[17] Pour des développements érudits Lajarge E., Debiève H., Nicollet Z., « Évolution de la définition de la santé publique » Sant. pub. 2013, 13-40 et les ouvrages en bibliographie.

[18] Que l'on corrige parfois par l'aphorisme « *Tout homme bien portant est un malade qui s'ignore* », formule issue de la pièce de théâtre de Jules Romains, « Knock ou le Triomphe de la médecine » (1923).

[19] Le terme aurait été inventé par Hippocrate. La « sémiologie médicale » désigne en médecine l'étude des signes et symptômes, et leur rattachement éventuel à un syndrome pour poser un diagnostic.

Leur perception est donc une fonction majeure des systèmes (automatisés ou non) focalisés sur les variations, parfois infimes, du vivant, des comportements et environnements. Dès lors, la sensibilité de cette perception, l'exhaustivité approchée et/ou la cohérence de leur connaissance, la pertinence de leurs rapprochements et de leurs qualifications évolutives sont cruciales, et une gageure. Ce qui vaut ici pour le corps biologique, vaut pour le corps social.

Dans une humanité du « *corps, nouvel objet connecté* » [20], qui ne cesse par ailleurs de collecter et de croiser des données relatives aux préférences comportementales dans des environnements non médicalisés, la métrologie continue peut fonder un nouveau type de médecine [21], voire de gouvernance… à les supposer socialement acceptables [22]. Dans l'industrie notamment, il en existe déjà une extension maximale : la maintenance anticipée, dite « prédictive », servie par l'intelligence artificielle [23]. La donnée d'intérêt y **est celle qui, selon le cumul continu d'expériences, préfigure finement un état non désirable**, et vise à alerter avant son expression même légère (soit avant le besoin, voire la spirale de soins).

*** La seconde est positive et holiste :** selon l'OMS en 1946, « *la santé est un état de complet bien-être physique, mental et social, et ne consiste pas seulement en une absence de maladie ou d'infirmité* » [24]. Cette définition ambitieuse est à replacer dans le contexte de dévastation physique, psychique et sociale du lendemain de la seconde guerre mondiale, appelant une réflexion systémique pour des actions sur tous ces terrains [25]. Devenue une référence permanente, cette définition de l'OMS réunit ainsi de nombreuses dimensions, imagées dans la « pyramide des besoins » théorisée en 1943 par monsieur A. Maslow [26].

---

[20] Dossier CNIL, *Le corps, nouvel objet connecté*, Cahiers Innovation & Prospective n°02, mai 2014.

[21] Au-delà de la conception originelle de la médecine préventive et prédictive ; voir Sicard D, « Les perspectives de la médecine préventive et prédictive », RFAP 2005/1(n°113), pp 121-125 (elle était alors essentiellement basée sur la connaissance génétique ; la systématisation de la métrologie externe est venue plus tard).

[22] On le voix en Chine communiste avec les « crédits sociaux », aux Etats-Unis avec en matière d'assurance automobile les approches « *Pay as you drive* » (quantitatif), puis « *Pay how you drive* » (qualitatif).

[23] Selon la norme NF EN 13306 X 60-319, « *maintenance conditionnelle exécutée en suivant les prévisions extrapolées de l'analyse et de l'évaluation de paramètres significatifs de la dégradation du bien* ».

[24] *in* Préambule à la Constitution de l'Organisation mondiale de la Santé, tel qu'adoptée par la Conférence internationale sur la Santé en 1946, entrée en vigueur en 1948 (Actes officiels de OMS, n° 2, p. 100).

[25] Notons en 1984 une formule définition encore plus ambitieuse sous l'égide de l'UNICEF, selon laquelle « *la santé n'est pas l'absence de maladie, c'est un sentiment plus profond que le bien-être qui ne dépend pas seulement des services de santé mais du travail, du revenu, de l'éducation, de la culture, des droits et des libertés* ». Depuis, le concept « One Health » entend rapprocher santé humaine, animale et environnementale.

[26] Maslow A., « A Theory of Human Motivation », *Psychological Review*, n° 50, 1943, p.370-396. Signalons que l'auteur ne l'a jamais présentée comme une hiérarchie au sens où il est souvent invoqué : « *Human needs arrange themselves in hierarchies of pre-potency.* ***That is to say, the appearance of one need usually rests on*** *the prior satisfaction of another, more pre-potent need* » (p. 370).

La définition de l'OMS pose cependant pour paradigme philosophique que « santé » et « bien-être » sont consubstantiels [27]. Or, outre l'attente sociale, donc la pression politique induite dans nos systèmes développés, cette approche holiste met en question les catégories du droit (dont les actions, responsabilités), la régulation des marchés des produits et services, la qualification des technologies utilisées et des données produites. **Si toute donnée est ici pertinente « en santé », comment les distinguer et les protéger ?**

*** La troisième est réaliste et opérative**. Selon monsieur R. Dubos dans les années 1970, la santé est un « *état physique et mental relativement exempt de gênes et de souffrances qui permet à l'individu de fonctionner aussi longtemps que possible dans le milieu où le hasard ou le choix l'ont placé* » [28]. Il en résulte, plus pratiquement que dans les définitions précédentes, que **la santé est un état relatif, susceptible d'actions** de prévention, correction, compensation, maintenance : les soins.
Cela n'est-il pas le but *minimal* de nos « systèmes de santé » ? La donnée « de santé » trouve ici son utilité classique : la représentation d'un état et de son évolution circonstanciée, afin d'orienter, déterminer, évaluer et adapter une stratégie thérapeutique et/ou prophylactique, objet des soins et d'autres vecteurs (éducation, habitat, environnement, alimentation etc.).

7. Mais il est désormais notoire que nombre d'informations précitées peuvent être massivement produites à l'extérieur des systèmes de soin, notamment par nos consommations courantes en tous domaines [29], et par tout ce que l'intelligence artificielle peut en inférer [30]. Il en va de même *a fortiori* avec les pratiques croissantes récréatives, sportives etc. de *quantified self* ou « soi quantifié », et de *self analytics* ou « analyse de soi » [31].

8. Ces informations peuvent conférer à ceux qui les agrègent et les croisent, **un potentiel descriptif, explicatif voire prédictif d'états**, cette capacité fût-elle certes grossière sans la médecine. Les conclusions qui peuvent être tirées *a minima*, par exemple de la fréquence, territorialité et vitesse de propagation d'une expression en ligne de besoin par un moteur de recherche [32], sont connues car d'application collective ; mais ce n'est que le premier exemple.

---

[27] Ce qui inclut la recherche technologique pour buts récréatif, de confort, de performance, esthétique etc.
[28] Les sources sont contradictoires quant à la date de ce propos (1970 /71 /73), et mutiques quant à son support.
[29] Alimentation, loisirs, habitat, mobilité, sexualité, lectures, sociabilité, etc.
[30] Marks M, « Emergent Medical Data: Health Information Inferred by Artificial Intelligence » - 11 UC Irvine L. Rev. 995 (2020-2021) 995 et s.
[31] Nombre de pas, durée et qualité du sommeil, poids, tension artérielle, électrocardiogramme, oxymétrie, etc.
[32] Parmi de nombreuses réf : Santillana M, Zhang DW, Althouse BM, Ayers JW, « What can digital disease detection learn from (an external revision to) Google Flu Trends? » Am J Prev Med. 2014 Sep;47(3):341-7 ;

9. Dès ici, on perçoit l'enjeu de la qualification juridique des technologies, et la puissance de **l'assemblage / du croisement de telles données, pour un profilage à l'échelle individuelle voire populationnelle**, au service de la santé publique, de la gouvernance [33], des actuaires [34]… mais aussi des ingérences cybercriminelle et/ou étatique, dans les droits personnels et la souveraineté. Ces ingérences ne visent pas que la capture, la destruction ou la pollution de données, l'attrition des systèmes : ajoutons, pour l'influence et le minage de la confiance, l'organisation et l'exploitation sélectives des sensibilités psychologiques [35]. Ce point lance des défis profonds et durables, notamment pour la communication institutionnelle en santé [36].

   Or, cette ingérence ne nécessite pas en soi l'accès à des bases institutionnelles de « données de santé », lesquelles jusqu'ici **constatent l'entrée des personnes dans un parcours formalisé au sein d'un système**. Dans comme hors de ces contextes et bases dédiées, des données même d'apparence anodine présentent un intérêt désormais exploitable.

Sur la « donnée »

10. La « donnée » n'est juridiquement définie que depuis 2022, comme « *toute* ***représentation numérique*** *d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels* » [37]. Antérieurement, l'implicite suffisait [38]. La donnée sera donc ici **la forme électronique d'une information / d'un signal** individuellement susceptible de traitement automatisé.

Bates M, « Tracking Disease: Digital Epidemiology Offers New Promise in Predicting Outbreaks » IEEE Pulse. 2017 Jan-Feb;8(1):18-22 ; Lippi G, Mattiuzzi C, Cervellin G, « Google search volume predicts the emergence of COVID-19 outbreaks ». Acta Biomed. 2020 Sep 7;91(3):e2020006 ; Rabiolo A, Alladio F, Morales E, McNaught AI et al., « Forecasting the COVID-19 Epidemic by Integrating Symptom Search Behavior Into Predictive Models: Infoveillance Study » J Med Internet Res. 2021 Aug 11;23(8):e28876.

[33] Réf préc. Notons qu'en 2021, Yves Nabat préc. *in* « Données de santé : entre permissivité juridique, biopolitique et néolibéralisme » ne porte de réflexion que sur le contexte des démocraties libérales, évacuant hélas un pan important du sujet : *quid* dans les autres systèmes politiques ?

[34] *« spécialiste de l'application du calcul des probabilités et de la statistique aux questions d'assurance, de prévention, de comptabilité et d'analyse financière associée, et de prévoyance sociale* » (Larousse/wikipedia).

[35] Parmi de nombreuses références, les synthèses de A. Yeung, A. Tosevska, E. Klager, F. Eibensteiner *et al.*, « Medical and Health-Related Misinformation on Social Media: Bibliometric Study of the Scientific Literature. J Med Internet Res. 2022 Jan 25;24(1):e28152 ; V. Suarez-Lledo , J. Alvarez-Galvez, « Prevalence of health misinformation on social media: systematic review », *J Med Internet Res*. 2021;23(1):e17187 ; Y. Wang Y, M. McKee, A. Torbica, D. Stuckler, « Systematic Literature Review on the Spread of Health-related Misinformation on Social Media », Soc Sci Med. 2019 Nov;240:112552 ; Z. Wang, Z. Yin, Y.A. Argyris, « Detecting Medical Misinformation on Social Media Using Multimodal Deep Learning », IEEE J Biomed Health Inform. 2021 Jun;25(6):2193-2203.

[36] D. Schillinger, R.J. Baron « Health Communication Science in the Balance », *Jl Am Med Ass.* Publié en ligne le 31 juillet 2023 (doi:10.1001/jama.2023.14763), impression à venir.

[37] Article 2§1 du Règlement 2022/868 du 30 mai 2022 sur la gouvernance européenne des données ; ce règlement devait définir son objet propre, les « données ».

[38] Cette définition était absente du Règlement général sur la protection des données personnelles (2016), comme de la loi informatiques et libertés en France (1978) définissant les « données personnelles », non les « données ».

Curieusement, une proposition de droit européen (non encore adoptée) porte, en mai 2022, une définition de « *donnée de santé **électronique*** » [39]. **Ce qui pourrait sembler un pléonasme** découle d'une régulation sectorielle : la proposition vise à réunir des définitions tantôt séparées (données de santé, génétiques), tantôt inédites (données relatives à des déterminants de santé, de bien-être) [40], montrant la dynamique en cours des catégories, *infra*.

Sur la donnée « de » santé :

11. Les expressions « *données de »*, « *relatives à* » ou « *concernant »* la santé, trouvent pour équivalent anglais « *health data* » ou « *health-related data* ». Elles peuvent être considérées comme synonymes, n'exprimant pas de grades de sensibilité, et la notion de santé étant à géométrie variable. Mais on constatera que **sous un vocabulaire stable, les définitions vont évoluer par incorporation continue d'éléments nouveaux**.

    En revanche, l'invocation historique dans les droits européens, certes en contexte de dossiers médicaux, du besoin que la donnée de santé présente « *un lien manifeste et étroit avec la santé* » [41] (« *data which have a clear and close link with health* » [42]), **témoigne d'un embarras emblématique,** lorsque l'on analyse la définition complète qui la contient [43].

12. Que peut être un « *lien manifeste et étroit* » avec la notion, si vaste, de santé ? Si une donnée n'a pas de « *lien **étroit** avec* », seulement un « ***lien avec*** », reste-t-elle « de santé » ? le lien peut-il être *étroit **sans être manifeste*** ? *manifeste **sans être étroit*** ? quelle qualification alors, pour des conséquences que l'on peut supposer différenciées (la nuance serait sinon inutile) ? Le droit peut-il pré-qualifier la donnée ? à défaut, cette qualification relève-t-elle de personnels cliniciens, ou administratifs ? est-elle placée sous contrôle juridictionnel, les contextes juridictionnels peuvent-ils varier ? pourrait-il, dès lors, y avoir une contradiction entre des qualifications, selon les juges saisis ? [44]

---

[39] Art. 2§2 a), b) et c), prop. de règlement sur l'espace européen des données de santé, COM(2022) 197 final.
[40] F. Megerlin, « La donnée de santé « électronique » en droit européen : tautologie, pléonasme, levier ? », à paraître RGDM 2024 (1). Nous développerons largement ce point.
[41] Recommandation n° R (97) 5 du Comité des ministres aux Etats membres relative à la protection des données médicales, adoptée le 13 février 1997, lors de la 584e réunion des délégués des ministres ; dans l'Union, issu du GT dit « Article 29 » (*infra*), le « Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques », février 2007, WP 131, point II.2.
[42] Les variantes de traduction entre les deux textes sont infimes, *comp*. Recommendation no. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data (Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies).
[43] *Ibid*. le contexte est (I. Définitions) « *l'expression « données médicales » se réfère à **toutes les données à caractère personnel relatives à la santé** d'une personne. Elle **se réfère également** aux données **ayant un lien manifeste et étroit avec la santé** ainsi qu'aux données génétiques* » (s'ensuit la définition des données génétiques, dont les premières sont donc bien distinctes).
[44] Megerlin F, Fasc 8-10 « Données de santé », n° 21 ; Traité de droit pharmaceutique, JCL LexisNexis (2023).

13. **Il ne s'agit pas là de pirouettes dialectiques** : d'une part, le champ est celui de l'énoncé et de la protection de droits fondamentaux, et appelle donc une rigueur particulière d'attention ; d'autre part, ces questions **ne se posent pas, ici, dans l'environnement homogène et unifié du droit interne** [45]. Dans l'Union Européenne, des écarts d'application peuvent exister [46], certes résorbables par centralisation de l'interprétation devant la Cour européenne de Justice, ou la Cour européenne des droits de l'homme [47]. Mais ailleurs dans le monde existent des divergences fortes de conception[48], rendant le dialogue parfois difficile voire impossible.

14. En outre, le « groupe de travail de l'article 29 » (institué par la directive 95/46 [49] et devenu en 2018 le Comité Européen de la Protection des Données, EDPB), avait publié en février 2015 un avis sur les **critères à considérer pour cerner la notion de « donnée de santé »**, du fait des interférences avec les modes de vie et applications de bien-être [50]. Sur cette base, dans l'optique d'une nouvelle recommandation, il est acté en juin 2015 sous l'égide du Conseil de l'Europe (institution de source et compétence différentes de celle de l'Union), l'abandon de l'expression « *d'information médicale* », au profit de celle de « *donnée de santé* » [51].

15. Ainsi, l'approche du Conseil, dans le sillage de l'Union, s'affiche holiste : tous deux se sont débarrassés des jeux laborieux de qualification de la *netteté*, et de *l'intensité*, de ce lien **avec une notion très vaste (la « santé ») pour une organisation trop précise (le « système »)** [52]. En revanche, en rester *a priori* à la donnée « médicale », de préférence à celle « de santé », permet à juste titre à des auteurs de circonscrire leur recherche [53]. Mais cela ne résout pas le problème, seulement un point de méthode devenu obsolète. **Le paramétrage du « besoin d'en connaître »** reste un enjeu majeur du partage des données protégées.

---

[45] Voir la synthèse sous l'égide du Conseil d'Etat (colloque 2017 préc.), « Santé et protection des données », La documentation française, 2019.
[46] European Commission (Health and Food Safety Directorate-General), Rapport, « Assessment of the EU Member States' rules on health data in the light of the GDPR » (2021), doi:10.2818/546193.
[47] Laquelle a compétence à l'égard des Etats membres, non à l'égard des institutions mêmes de l'Union, *infra*.
[48] Bernier A., Molnàr-Gàbor F., Knoppers B.M., « The international data governance landscape » J Law Biosci. 2022 Apr 4;9(1):lsac005.
[49] Article 29 de la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (actif jusqu'à l'entrée en vigueur le 25 mai 2018, de l'EDPB).
[50] Nous reviendrons sur cet avis, non suivi sur ce point pour l'élaboration du RGPD. Voir la lettre du 5 février 2015 du groupe de travail de l'article 29 sur la protection des données (« Article 29 Data Protection Working Party », voir son « Annex - health data in apps and devices », non traduits).
[51] Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), « Rapport de présentation visant à mettre à jour la Recommandation n° R (97) 5 du Conseil de l'Europe sur la protection des données médicales ».
[52] Fasc 8-10 « Données de santé » n°21 préc., Traité de droit pharmaceutique Litec, JCL Lexis Nexis (2023).
[53] Tirard S (*dir*), Dossier « Données médicales », Rev. Histoire, médecine et santé (11) Hiver 2022. Sous cet énoncé *a priori* restrictif, l'approche historique est intéressante aussi sur la donnée de santé, spéc. Guillemain H et Hanafi N, « Pour une histoire des données médicales - XVIIe-XXIe siècle », pp 31-46.

16. On pourrait étendre le raisonnement aux « *déterminants de santé* » médicaux, comme non médicaux [54]. Dans ce dernier cas, l'information (comportement, environnement, alimentation, addictions etc.) n'est-elle pas aussi « de santé », puisqu'elle la « détermine » [55] ? Si cela n'était pas prévu en 2016, cela est envisagé en 2022, nous venons de le voir [56].

    Le lecteur aura perçu la difficulté : le fait que « *tout (soit) dans tout* » [57] **aiguise le défi de la qualification d'une donnée en vue d'un régime particulier** ; des critères précis sont requis. Néanmoins, nous verrons l'aspiration croissante de telles informations dans la création d'espaces (institutionnel et personnel, national et européen) des « données de santé ».

Sur la « donnée de santé »

17. * En droit français, il n'existe pas de définition en soi de la « donnée de santé ». Mais en matière de protection de l'information, les obligations historiques des acteurs (obligations d'origine hippocratique [58]) et, depuis 2002, les droits formalisés des patients, s'appliquent aux interactions **avec le système de santé tel qu'il est défini par la loi.**

    Ainsi, « *toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins* ***dont les conditions d'exercice ou les activités sont régies par le présent code*** *(…) a droit au respect de sa vie privée* ***et du secret des informations la concernant*** (…). *Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre* ***l'ensemble des informations concernant la personne*** [59] ***venues à la connaissance*** *du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il* ***s'impose à tous les professionnels intervenant dans le système de santé*** » (art. L. 1110-4-I CSP).

18. Dès lors, si l'on quitte la prise en charge « organique » sous couvert de ce droit de la santé, et que la question est posée sous l'empire d'un autre droit interne (hors « système de santé »), ou

---

[54] Alla F, « Les déterminants de la santé », in *Traité de Santé publique* (2016), Lavoisier éd., pp 15-18.
[55] Cette détermination est relative : il ne s'agit souvent que de facteurs prépondérants. En 2022, la proposition EESD (article 2.2.a) vise à y incorporer « *les données se rapportant aux déterminants de la santé* », *infra*.
[56] Article 2§2 a), b) et c) de la proposition de règlement européen EESD, voir note de bas de page n° 39.
[57] La racine « *tout est dans tout* » est attribuée à Anaxagore, la suite « *et réciproquement* » à A. Capus.
[58] « (…) *Quoi que je voie ou entende dans la société pendant, ou même hors de l'exercice de ma profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas* (…) » traduction du serment d'Hippocrate par E. Littré (1839).
[59] Il ne s'agissait que de l'ensemble des « informations médicales », jusqu'à la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, qui en a élargi le champ.

d'un autre droit national (cas du soin transfrontière), le droit invoqué sera plus sûrement le droit des données personnelles, unifié en 2016 par le règlement précité. Qu'en est-il alors ?

19. Depuis son adoption en 1978, la loi française dite « informatique et libertés » plusieurs fois modifiée, ne définit pas plus les « données de santé » [60]. Son actuel article 30 dispose seulement que « *les traitements de données à caractère personnel* ***dans le domaine de la santé*** *sont régis par* (…) » ses articles 64 à 67. Dès lors, ce « *domaine* » ne s'étend *a priori* qu'aux activités limitativement énoncées par la loi. Or, cela fait qu'une donnée personnelle **ne participant pas du « domaine » ainsi défini, semble ne pouvoir être « de santé ».**

20. * En revanche, en droit de l'Union, lequel s'impose en France, une **définition positive des « *données concernant la santé* »,** distincte des données génétiques et biométriques, a été introduite pour la première fois en 2016, par le règlement général de protection des données : « *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* » [61].

Nous l'étudierons à la lumière des considérants plus vastes qui l'introduisent, et de l'avis en 2015 du « groupe de l'article 29 » qu'elle n'a pas suivi à la lettre : **cette définition est de ce fait tautologique, mais c'est pour pouvoir y aspirer ce que l'on veut lui faire protéger**.

21. Or, les textes européens **donnent lieu à des approches toujours plus extensives,** selon qu'ils visent, après l'organisation spécialisée des soins transfrontières (2011), déclinée en services en ligne, et en réseaux de référence, l'énoncé donc d'une protection générale des données personnelles (2016) ; la préfiguration d'un « espace européen des données de santé » (2022), d'une *quasi* qualification autonome d'« application de bien être », l'introduction de catégories prioritaires et minimales etc. Nous verrons aussi en quoi **il serait utile que la notion de « donnée synthétique » de santé**, non évoquée dans les projets de textes sur l'« intelligence artificielle » (2021), soit abordée, même si elle n'est par définition pas « personnelle ».

L'enchaînement de ces approches, leurs interférences et conséquences, seront l'objet de nos développements : ils sont révélateurs de la dynamique que nous allons étudier, montrant **comment l'extension de la notion reflète aussi une transformation des systèmes** [62]**.**

---

[60] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle qu'en vigueur.

[61] Article 4-15 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (abrogeant la directive 95/46/CE), dit « RGPD ».

[62] Fasc 8-10 « Données de santé » n°83, Traité de droit pharmaceutique, JCL LexisNexis (2023) préc.

Sur la « sensibilité » de la donnée de santé

22. Nous venons de citer le droit français et le droit européen ayant pour objet la protection des données personnelles. Dans ce contexte, la « *sensibilité* » des données détermine l'étendue, parfois la nature de leur protection sectorielle [63] ; elle y est souvent associée au caractère « *personnel* », c'est à dire rattaché ou rattachable à une personne physique [64].

    Ainsi, une donnée « *anonymisée* » est qualifiée de « non personnelle », car ce processus est censé rendre la personne non identifiable, de façon irréversible ; en contraste, la donnée « *pseudonymisée* » reste personnelle, et la personne retrouvable par code. Mais nous verrons que ces notions ne sont pas sans ambigüité : elles sont relativisées, quant à l'« irréversibilité », par les progrès exponentiels de la masse d'information et des capacités de calcul.

23. De prime abord, la « sensibilité » d'une donnée « personnelle » s'entend ici **au regard des droits fondamentaux individuels** : le but est de protéger la sphère de l'intime, et proscrire toute conclusion discriminatoire ou infâmante pouvant être tirée de sa connaissance [65].

    Mais il est nécessaire dans une optique ici élargie, de considérer **aussi leur sensibilité à l'échelle populationnelle**. Cette sensibilité peut découler du cumul des données précédentes, ou procéder d'autres pratiques. Aujourd'hui plus encore qu'hier, la connaissance de facteurs de risques spécifiques à une population, d'un état ou d'une dynamique épidémiologique, d'une couverture vaccinale, de capacités physiques/psychiques, de préférences mentales face à différents types de situations/risques, de la confiance en des produits ou services de santé et leur régulation, la qualité du système etc. est un enjeu de gouvernance [66] et de souveraineté.

24. Malgré cela, cette **dimension reste souvent étrangère aux réflexions générales** sur l'usage des données [67], sans doute parce qu'elle relève d'une dimension inhabituelle ? Celle-ci devrait être déspécialisée, en deçà du macro-rapprochement de la santé et de la géopolitique [68]. Michel Foucault avait en 1974 porté l'intéressant néologisme « *biopolitique* », pour désigner **l'exercice du pouvoir sur le vivant**, plutôt que sur des entités rapportées à des territoires [69].

---

[63] Des obligations parfois spéciales de protection sont énoncées par les codes (Défense, Intérieur etc.).
[64] Ainsi par la CNIL (onglet dédié) et le RGPD (consid. 10), mais cette notion n'est pas une catégorie juridique.
[65] Droits du travail, du crédit, du logement, des déplacements ; dignité, réputation, sociabilité, etc.
[66] Voir CE 30 juin 2023, n° 469964, cité note de bas de page n° 10.
[67] Dernièrement, Henrard J-Cl, « Les données de santé et leur utilisation », *Santé Publique*, vol. 34, no. 3, 2022, pp. 333-334, qui présente un dossier de plusieurs articles (et bibliographie), dont cette dimension reste absente.
[68] Sur le lien géopolitique et santé, externe à notre champ de recherche, voir les références en bibliographie.
[69] Collectif (trad. de l'italien), *Lexique de biopolitique. Les pouvoirs sur la vie*, Érès, 2009.

Winston Churchill avait, quant à **l'exercice du pouvoir sur l'esprit**, lumineusement prophétisé que les prochains empires seraient spirituels [70]. Or, les deux sont ici connexes.

25. De fait, l'accès à, et l'usage de la donnée de santé collective voire personnelle, quelle que soit sa précision, sont un **enjeu tactique voire stratégique immémorial** ; cela ne commence-t-il pas dès les alliances matrimoniales et claniques ? La connaissance de la santé des souverains et décideurs politiques (entre autres) est depuis toujours un enjeu majeur, et une information convoitée au-delà des exercices déclaratoires [71]. Depuis peu, la recherche systématique sur la génétique de populations [72] ouvre encore d'autres débats.

26. Si l'on s'en tient à l'utilité moderne de la connaissance de la donnée de santé sans une telle spécialisation [73], notons son institutionnalisation aux Etats-Unis par le *National Center for Medical Intelligence* (NCMI), lequel n'était titré de façon significative avant 2008 que « *Armed Forces Medical Intelligence Center »* (AFMIC), et est depuis 1962 composante de l'Agence du renseignement de défense [74].
Cette connaissance ne se réduit pas à celle des forces en présence : cela potentialise la sécurité et capacité d'action ou de décision (civile autant que militaire), peut en éclairer l'opportunité. Naturellement, les Etats-Unis ne sont pas les seuls à s'y intéresser, d'autres puissances dont les moins démocratiques le pratiquent à mots couverts.

27. En conséquence, le règlement européen de 2022/868 sur la gouvernance des données dispose, quant à leur usage secondaire qu'il vise à réguler [75], que « *des actes législatifs spécifiques de*

---

[70] Churchill W, « Les empires du futur seront spirituels » (citation de 1965, non sourcée).
[71] Par exemple, Accoce P, « Secrets et défense médicale - Chefs d'Etat et dirigeants s'efforcent de tout savoir sur la santé de leurs pairs. Et de ne rien laisser paraître de la leur », *in* L'Express, 23 juin 1998 ; Le Person X., « Usages et discours de la maladie dans l'art de la négociation politique (…) (1585) », *in* Belmas E et Michel MJ (dir.), *Corps, santé, société. Actes du colloque de Paris du 12-13 décembre 2002*, Paris, Nolin, p. 155-172 ; Nevejeans P., « Le corps souffrant et ses enjeux diplomatiques », *in* Bull. Centre de recherches du château de Versailles, 2016; Dossier, *Quel est l'état de santé de nos chefs d'Etat ?* Jeune Afrique (2017) https://www.jeuneafrique.com/dossiers/quel-est-letat-de-sante-de-nos-chefs-detat/
[72] Parmi de nombreuses références, voir en miroir Cyranoski D, « China's massive effort to collect its people's DNA concerns scientists » Nature, 7 juill. 2020 ; Defranoux L, « Fichage génétique en Chine : l'Amérique se réveille » *in* Libération, 22 févr. 2019 ; auparavant Wessel L. « Scientists concerned over US plans to collect DNA data from immigrants », Nature 7 oct. 2019.
[73] Clemente JD, « Medical Intelligence », Jl of U.S. Intelligence Studies, vol 20 n°2, 2013, pp 73-78 ; Wyrd C, Gruson D, « Renseignement et santé », Rev. déf. nat. 2021/7 (n°842), pp 83-89.
[74] Department of Defense Instruction n° 6420.01 de 2009, actualisée le 8 septembre 2020. « *For the purpose of this Instruction,* ***the term "medical intelligence" is defined as*** *the product of collection, evaluation, and all-source analysis of worldwide healththreats and issues, including foreign medical capabilities, infectious disease, environmental health risks, developments in biotechnology and biomedical subjects of national and military importance, and support to force protection* ».
[75] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).

l'Union ***peuvent considérer que certaines catégories de données à caractère non personnel*** *détenues par des organismes du secteur public* ***sont hautement sensibles*** *aux fins du présent article,* ***lorsque leur transfert vers des pays tiers peut mettre en péril des objectifs de politique publique de l'Union****, tels que la sécurité* ***et la santé publique*** *(...)* » (article 5§13). Le refus d'accès pour « *motif d'intérêt public* », à des données de santé non personnelles, vient d'être validé en 2023 en France, pour une application interne contestée [76].

28. En outre, dans l'Union européenne, aucun Etat membre n'est tenu de fournir des renseignements **dont il estimerait la divulgation contraire aux intérêt essentiels de sa sécurité** (TFUE, article 346§1.a). Par exemple, selon le Règlement 2022/123, cela inclut potentiellement la communication de données sur les stocks nationaux de médicaments [77]. Dans le même sens, le Règlement 2022/2372 sur les contre-mesures médicales en cas de crise sanitaire au niveau de l'Union [78] met en exergue des mécanismes de suivi par obligation d'informer la Commission ; la réserve « *sans préjudice des intérêts nationaux en matière de sécurité* » y apparaît de façon prévisible, mais **récurrente donc appuyée** (article 7, §3 et 4).

    Mais nous avons vu que les données que leur combinaison pouvait rendre « hautement sensibles », n'étaient pas l'apanage des bases de données publiques. Si le règlement de 2022/868 est mutique sur ce point, c'est du fait de son champ d'application restreint [79].

29. Dès lors, il est un truisme, peut-être pas inutile, de rappeler que la sensibilité d'une donnée peut être intrinsèque (par exemple stock de contre-mesures médicales, capacité de réponse industrielle, attrition d'effectifs), mais également acquise par le croisement d'informations anodines, lequel les potentialise. Ce point **reste l'angle mort du droit commun,** qui s'attache à la sensibilité intrinsèque des données. Qu'en est-il en matière de « données de santé » ?

    Du fait de la diffusion des traceurs, objets connectés et applications mobiles, le « groupe de l'article 29 » précité avait considéré en 2015 que, pouvaient relever de cette qualification, jusqu'aux « *données* ***permettant de tirer des conclusions à propos de l'état de santé d'un***

[76] Conseil d'État, 30 juin 2023, n° 469964, suite à la décision de la CNIL à l'égard du journal Le Point, préc.
[77] En ce sens, *consid*. 21, Règlement 2022/123 du 25 janv. 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci.
[78] Règlement (UE) 2022/2372 du 24 octobre 2022 relatif à un cadre de mesures visant à garantir la fourniture des contre-mesures médicales nécessaires en cas de crise de santé publique à l'échelle de l'Union.
[79] Article 1er§1 : « *1. Le présent règlement établit: a) les conditions de réutilisation, au sein de l'Union, de certaines catégories de données* ***détenues par des organismes du secteur public;*** (…) ».

individu *(indépendamment du fait que ces conclusions sont exactes ou inexactes,* ***légitimes ou illégitimes,*** *suffisantes ou insuffisantes)* » [80]. Or, cela vaut tout autant pour une population.

Sur le droit comparé de la sensibilité des « données personnelles »

30. Revenons aux données « personnelles » : si depuis 2016, l'Union européenne a adopté une approche protectrice globale par son RGPD, tel n'est pas le cas dans nombre d'autres pays. Leur revue en droit comparé pour les données de santé, a donné lieu en 2022 à un panorama auquel le lecteur se référera utilement [81].

31. Mais nous ne considérerons ici que le dialogue transatlantique : cette dimension est celle du transfert des données **dont l'encadrement formel en droit est le plus poussé**, **et sera de ce fait le plus discuté quant aux ingérences par voie de droit**, *infra*. Ainsi, le premier accord dit « *Safe Harbour »* [82] cadrant ce transfert, était-il en 2000 justifié par le fait que ses principes étaient « *destinés à combler le fossé séparant les régimes américains et européen de protection de la vie privée* » [83] (nous en verrons les avatars). Cette discussion n'a pas lieu, lorsque un tel droit n'existe pas, et/ou que le dialogue est difficilement envisageable.

32. En outre, le paysage reste fragmenté en droit fédéral américain même : à l'inverse de l'approche européenne par un règlement général, les « données sensibles » y sont définies par des règles sectorielles. En santé, les « *Protected Health Information* (PHI) » sont ainsi définies par l'HIPA Act [84]. Or, dans l'*HIPPAA Journal* qui l'explicite, il est noté que « *what is* (PHI) *is a* ***question many sources struggle to answer successfully due to the complicated definitions*** *in the HIPAA Administrative Simplification provisions* » [85]. En parallèle, certains prônent l'extension de l'HIPAA [86], donc l'extension des « *entités couvertes »* par lui [87].

---

[80] Annexe à la lettre du 5 février 2015, développée *infra*.
[81] Bernier A, Molnàr-Gàbor F, Knoppers BM, « The international data governance landscape », *Journal of Law and the Biosciences*, Volume 9, Issue 1, January-June 2022, lsac005
[82] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles (2000/520/EC).
[83] Annexe IV de la décision 2000/520 de la Commission, voir B, rapporté au §10 de la décision précitée.
[84] Health Insurance Portability and Accountability Act, adopté en 1996. Pour une récente synthèse, Rose RV, Kumar A, Kass JS, « Protecting Privacy: Health Insurance Portability and Accountability Act of 1996, Twenty-First Century Cures Act, and Social Media ». Neurol Clin. 2023 Aug;41(3):513-522
[85] What is Protected Health Information? HIPAA Journal, vérifié juillet 2023. L'article de poursuivre « *The HIPAA Administrative Simplification provisions (45 CFR Parts 160,162, and 164)* ***are intentionally ambiguous*** *because they have to relate to the activities of different types of health plans, health care clearinghouses, qualifying healthcare providers (…) and third party service providers to Covered Entities (…)* ».
[86] Theodos K, Sittig S. « Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply ». Perspect Health Inf Manag. 2020 Dec 7;18(Winter):1l. Morley J, Cowls J, Taddeo M, Floridi L, « Public Health in the Information Age: Recognizing the Infosphere as a Social Determinant of Health ». J Med Internet Res. 2020

33. En ce sens, c'est en 2022 l'agence fédérale de protection des consommateurs (FTC) qui s'interroge ainsi : « ***among the most sensitive categories of data*** *collected by connected devices are a person's precise location and* ***information about their health****. Smartphones, connected cars, wearable fitness trackers, "smart home" products, and even the browser you're reading this on are capable of* ***directly observing or deriving sensitive information about users.*** *Standing alone, these data points may pose an* ***incalculable risk to personal privacy****. Now consider* ***the unprecedented intrusion*** *when these connected devices and technology companies collect that data, combine it, and sell or monetize it.* ***This isn't the stuff of dystopian fiction. It's a question consumers are asking right now*** » [88].

34. Certes, le focus n'est ici que celui du consommateur, car telle est la compétence de la FTC. Mais, de fait, elle sensibilise fortement le citoyen autant que le patient, donc la population. En 2021, son interprétation déjà en ce sens des règles sur la divulgation non autorisée de données issues de ces systèmes [89] a toutefois été à l'origine d'une opinion dissidente d'une de ses membres : madame Wilson déplorait en cette interprétation par la FTC, une extension du droit, non sa simple explication, appelant une mise en cohérence [90].

35. Dès lors, la FTC vient de proposer en mai 2023 de renforcer et moderniser les règles [91], et de soumettre un projet en ce sens ; les « *breaches by health apps and other technologies* » **deviendraient des « *health breaches* »** [92]. Or, cela marquerait un changement de statut juridique aux conséquences fortes, sans (encore d') équivalent européen (en gestation).

    D'autres agences n'ont pas attendu, pour réfléchir déjà aux implications géopolitiques d'un constat valable pour toutes autres données sensibles [93].

Aug 3;22(8):e19311 ; S.J. Schweikart, « Should Immigration Status Information Be Considered Protected Health Information ? » AMA J Ethics. 2019 Jan 1;21(1):E32-37.

[87] 2023 UpDate – HIPAA Journal « What is a HIPAA-Covered Entity ? ». Outre les « *Covered Entities* », les règles s'appliquent en cascade à leurs sous-traitants, les « *Business Associates* ».

[88] Cohen K, « Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data », FTC blog, 11 juillet 2022. Depuis, Rozier M, Scroggins S, Loux T, Shacham E, « Personal Location as Health-Related Data: Public Knowledge, Public Concern, and Personal Action », Value Health 2023 May 24:S1098-3015(23)02614-1 ».

[89] FTC Policy Statement on Breaches by Health Apps and Other Connected Devices, 15 sept. 2021.

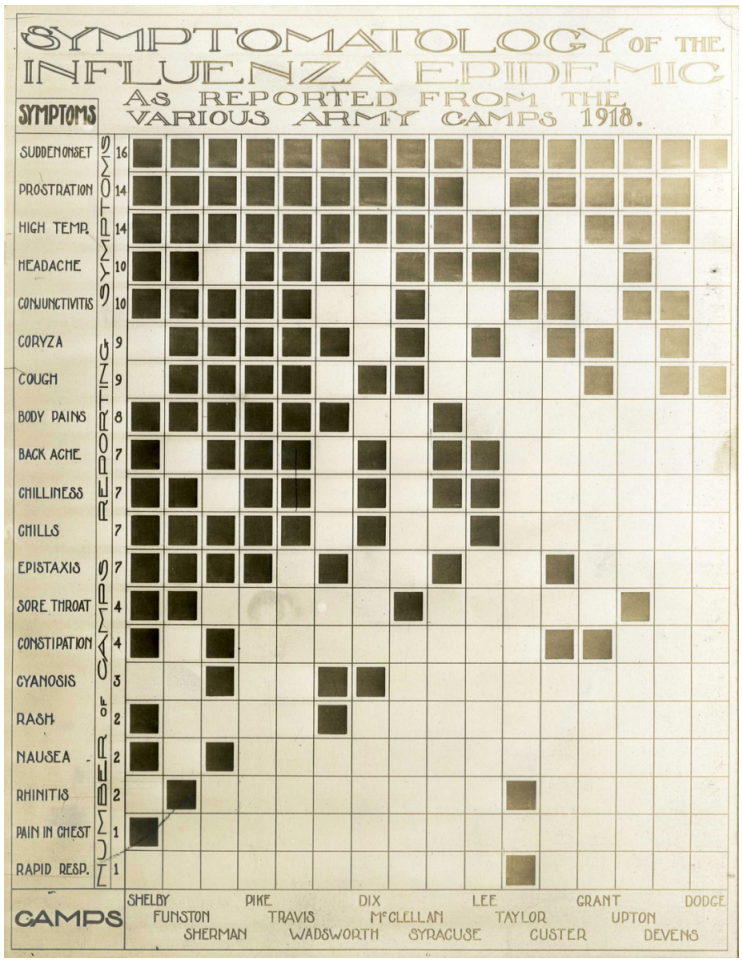
[90] « Dissenting Statement of Commissioner Christine S. Wilson Policy Statement on Breaches by Health Apps and Other Connected Devices », Matter n° P205405, 15 sept. 2021.

[91] FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule, 18 mai 2023.

[92] Référencé P205405, portant sur le « 16 CFR Part 318: Health Breach Notification Rule », 9 juin 2023.

[93] Cf. l'Executive Order, 9 juin 2021, de J. Biden, Président des Etats-Unis : « Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries » (non numéroté, site de la Maison Blanche).

36. Le tableau ci-dessous en est emblématique. Il représente une symptomatologie rapportée (non des états diagnostiqués) associée à la grippe, dans des camps militaires alliés en France durant la première guerre mondiale [94]. Le lecteur **peut imaginer les représentations, certes plus ou moins spéculatives, pouvant résulter des outils numériques** précédemment esquissés. Ils peuvent parfois être appliqués de façon lointaine, continue, à bas coût, de façon globale ou sélective voire ciblée, pour la description, l'explication, la prédiction, voire l'induction de comportements individuels et populationnels, et d'actions publique comme privée.



Ainsi voit-on partout les catégories classiques de raisonnement, **en santé historiquement stables, protégées, et emblématiques en tant qu'elles nous concernent tous**, ébranlées par la technologie, les usages et les convoitises, entre accaparement et instrumentalisation. Elles doivent, parmi d'autres, être spécialement protégées par les Etats au double titre des droits fondamentaux des personnes, et de leur propre souveraineté, c'est-à-dire de la maîtrise de notre destin en tant que communauté politique.

[94] Archives médicales militaires américaines 1918 (https://www.archives.gov/topics/wwi/medicine).

Annonce du plan

37. Pour les raisons qui précèdent, qui tiennent au flou de la notion face à des enjeux critiques, à la transformation des concepts et systèmes par la technologie et les usages, et à la tension géopolitique par des outils renouvelés, nous proposons de restituer le fil rouge de notre recherche en distinguant, **à la lumière de ces enjeux, les dynamiques de la notion de donnée de santé (*Ière partie*), puis des aspects de son accès international (*IInde partie*)**. Notre approche méthodologique est ainsi l'occasion d'une analyse transverse de concepts tantôt établis, tantôt en gestation, dont nous relèverons parfois l'intérêt d'un dépassement.

38. En bibliographie, le lecteur trouvera des ressources non systématiquement rapportées au bas des pages. Tel est le cas, lorsqu'elles ont pu éclairer le contexte de réflexion, mais ne l'ont pas déterminée sur le plan technique ni théorique : dès le début de notre recherche, notre intention était en effet, plutôt qu'une méta-analyse (analyse d'analyses) de littérature, une analyse juridique et un **rapprochement de première main des textes-source** : ceci pour des besoins professionnels en situation, et le maintien de la transversalité du raisonnement ; mais aussi car certaines propositions de normes, encore discutées, n'ont pas donné lieu à publications.

Partie I – Souveraineté et dynamiques de la notion

Titre I – Définition des données de santé : des contours, au contenu
Titre II – Définition des données de santé : du contenu, au contexte

Partie II – Souverainetés et dynamiques du régime

Titre I – Garanties internationales pour un accès licite en santé
Titre II – Garanties internationales contre les ingérences en santé

PARTIE I. SOUVERAINETE ET DYNAMIQUES DE LA NOTION DE DONNEE DE SANTE

Cette première partie rend compte des résultats de notre recherche sur la dynamique de la notion de « donnée de santé », observée au travers de ses manifestations dans les normes, projets de normes et avis, la pratique et les jurisprudences, et parfois les doctrines qui les théorisent pour des objectifs variés. Cela **impose un bref préalable méthodologique** :

* Par « **notion** », on entend l'« *idée générale de la chose qui se présente au travail de l'esprit* »[95]. L'examen d'une notion précède toujours l'établissement d'un concept. Le but peut être que ce concept donne lieu à la création d'une catégorie juridique, à laquelle une entité ou une situation sera rattachée en vue d'effets en droit. Ainsi, **l'extension de la notion peut (et ici va) conduire à modifier les catégories du droit** ; mais cela relève d'un choix politique [96].

* En contraste d'une notion, un « **concept** » suppose un périmètre net et un contenu déterminé de pensée [97]. Il est ou devrait toujours être prédéfini pour être **univoque par convention** (non par l'effet de la loi, sinon il s'agit aussi d'une catégorie juridique). Son invocation permet de convoquer et discuter un contenu complexe, sans devoir systématiquement l'énoncer.
Dès lors, la pensée conceptuelle, ses expressions symboliques ou conventionnelles [98] permettent l'accélération sécurisée des échanges, de la recherche et de la décision, sans imposer la réincorporation continuelle d'éléments explicatifs : **« on sait de quoi on parle ».**

A défaut, le risque est qu'un même mot ne porte pas le même contenu conceptuel, selon le référentiel de l'interlocuteur : ce risque est élevé dans la vie de l'esprit ; il *devrait*, en

---

[95] Ch. Jarrosson, voir le chapitre « La notion de notion » in *La notion d'arbitrage* LGDJ 1987.
[96] Avant tout processus normatif, sachant la possibilité d'une induction jurisprudentielle. Dans ce cas, on pourrait presque dire qu'il s'agit d'un choix politique du juge, dans son office d'interprétation du droit, qui sera ensuite consacrée par l'autorité compétente.
[97] Du latin *con capto,* saisir avec ; ou *conceptus*, « action de contenir, de tenir ensemble, de recevoir ».
[98] Not. en santé les *thesaurus ;* Dénominations Communes Internationales pour les molécules *;* classifications internationales comme la CIM 11 (Classification Internationale des Maladies XIème édition, adoptée en 2019, qui constitue un cadre conceptuel indépendant de la langue et de la culture, lequel intègre la terminologie et la classification) ; ATC, *Anatomical Therapeutic Chemical (ATC) Classification System*, publié en 2016 sous l'égide de l'OMS qui le contrôle (deux autres classifications ont cours en France : le code CIP et la classification UCD) ; hors santé, les INCOTERMS, *INternational COmmercial TERMS,* publiés sous l'égide de la Chambre de commerce international, Paris (dernière version : INCOTERMS 2020), lesquels servent à définir de façon univoque les obligations réciproques des acteurs du commerce international notamment, etc.

principe, être limité dans les sciences et en droit [99] : tel est aussi le but de définitions préliminaires en amont d'actes etc. ou, en droit européen, en aval de considérants parfois ambitieux [100] . Le risque d'équivoque est **maximisé dans la conduite des relations internationales** : au défi de la traduction, s'ajoute parfois la non-coïncidence des concepts [101].

* Enfin, une « **catégorie juridique** » est la désignation, selon un droit déterminé [102], d'une entité ou d'une situation caractérisée : cela pour lui associer des conséquences en droit, dont l'application d'un ensemble de règles, dit « régime juridique ». L'**opération de qualification,** qui conduit à revendiquer ou dénier de telles conséquences, sera *in fine* opérée sous le contrôle du juge compétent [103].

Ainsi, **une erreur de qualification** conduit à ne pas rattacher une entité ou situation à la catégorie correcte, et donc à lui appliquer des règles non appropriées. Ceci de façon généralement involontaire ; **mais parfois aussi par calcul, selon l'effet recherché** sur les obligations légales, contractuelles ou conventionnelles – sachant qu'en matière internationale, les qualifications et/ ou les conséquences peuvent facilement être **en concurrence, voire en conflit**, selon le juge saisi et la loi applicable [104].

Parfois, des acteurs cherchent **à éluder certaines qualifications pour un positionnement plus opportun sur un marché**, pour provoquer le rattachement à un ordre juridique complaisant, et/ou échapper à une surveillance de leurs activités transnationales [105].

Le rappel de ces truismes s'imposait, tant l'abondance des textes et de la production doctrinale, des publications grand public ou spécialisées qui traitent sans les définir des « données de santé » (*health data*), pourrait donner à croire que la notion est cernée dans l'ordre interne, européen et international, à défaut de disposer d'un régime unifié.

---

[99] Sur le fait que les notions scientifiques **ne sauraient recouvrir des concepts différents, donc des catégories juridiques différentes,** en droit de l'Union et en droit national : CA Paris, 11 juill. 2019, pourvoi rejeté par Civ. 1er juin 2022, n°19-20.999, pt. 17 (en matière de médicaments).

[100] En matière de données de santé, nous étudierons spécialement cet écart entre le considérant n° 35 et la définition par l'article 4.15 du RGPD préc.

[101] Pour un récent exemple, *Transcultural dictionnary of Misunderstandings - European and Chinese Horizons*, H. Ping, S. Le Pichon, T. Reichmann, Z. Tingyang, Ed. Cent mille milliards, Paris, 2023 ; plus largement, les travaux de l'Institut International Transcultura, créé en 1988 par H. Ecco et A. Le Pichon.

[102] National ou international; applicable, ou revendiqué comme tel en cas de compétences concurrentes.

[103] Rappelons ici que le contrôle des qualifications est le seul objet de l'examen en cassation devant les juridictions françaises, à l'exclusion donc du contrôle des faits (hors hypothèse de la dénaturation des faits).

[104] B. Audit, *Droit international privé*, Economica, 3ème éd. 2001; en matière de droit international public, D. Carreau, A. Hamann, F. Marella, *Droit international*, Pedone, 13ème éd. 2022.

[105] F. Megerlin, *Ordre public transnational et arbitrage international de droit privé – essai critique sur la méthode*, Thèse pour le doctorat en droit, université Paris II, PU Septentrion, 2000.

Or, comme la notion de « santé » (*supra*), la notion de « donnée de santé » est **susceptible de multiples définitions qui ne se recoupent pas toujours ; elle ne procède pas d'un concept univoque** dont l'invocation suffirait pour se comprendre [106] ; **ni même en droit interne** d'une catégorie juridique stable, puisque son contenu va s'avérer **composite et dynamique** avec des conséquences multiples : celles-ci intéresseront le champ de la protection renforcée des données au profit des personnes (droit des patients, devoirs des professionnels et organisations, des hébergeurs, des fabricants de technologies etc.), mais aussi la dynamique de leur partage national / transfert transfrontière (utilisations secondaires, incluant le traitement par intelligence artificielle et la génération de données de santé « synthétiques ») **à l'heure d'échanges globalisés hautement compétitifs, et d'une géopolitique repolarisée.**

C'est pourquoi nous avons voulu analyser, et restituons ici le dynamisme contemporain de la notion de « donnée de santé ». D'une façon qui apparaît aujourd'hui contre-intuitive – tant la qualification de la « donnée » [107] en soi (c'est-à-dire détachée d'un dossier de santé ou d'une relation de soins) est devenu une évidence, le tracé du contour de la notion **a, en fait et en droit, précédé la détermination de son contenu** (titre I).

Mais celui-ci connaît un développement accéléré, multi-facettes : le contenu de la notion tend en effet à aspirer de son contexte informationnel (notamment des données de « bien être », de « soi quantifié », et de consommation de produits et services hors soins), **lequel tend parfois à s'assimiler juridiquement à lui**, du moins dans certaines bases de données ; ainsi examinerons-nous cette dynamique d'extension-assimilation (titre II).

TITRE I. LA DEFINITION DE LA NOTION DE « DONNES DE SANTE » : DU CONTOUR, AU CONTENU

Ce titre sera surtout descriptif, bien qu'assemblant des éléments rarement réunis faute d'analyses transverses**,** nous l'avons vu en introduction. Si la notion de « donnée de santé » est l'objet de définitions multiples, et recouvre des phénomènes dynamiques, on peut en effet

---

[106] *Comp*. Maisnier-Boché L. « Donnée de santé à caractère personnel » Fasc 945, JCL Communication, et Megerlin F lequel en contraste pointe la tautologie, in Traité de droit pharmaceutique, JCL Fasc 8-10 (2023).

[107] Selon le RGPD en 2016, la donnée est une « information » (article 4-1) ; il faudra attendre le règlement de 2020 pour une définition normative intrinsèque : « « *toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels* » (article 2§1, proposition de règlement sur la gouvernance européenne des données, COM(2020) 767 Final). »

distinguer nettement les termes du débat et son lien avec la souveraineté, selon que la réflexion précède le Règlement européen de 2016 visant la protection des données personnelles en Europe [108], ou lui succède.

Entrée en vigueur en 2018, cette ligne de partage ne tient pas tant ici à l'unification du droit applicable, laquelle s'impose à l'ensemble des Etats membres pour une homogénéisation heureuse des protections des données personnelles selon un standard élevé [109], **qu'à l'explicitation et l'élargissement de la notion** de donnée de santé (Chapitre II) ; ceci **bien au-delà de sa conception antérieure, plutôt implicite et statique** (Chapitre I).

CHAPITRE I. LA DYNAMIQUE DU TRACE DES CONTOURS AVANT LE DROIT EUROPEEN DE 2016

On pourrait imaginer que du fait de son objet, le droit de la santé, lequel régit la relation de soins et encadre les organisations et exercices professionnels en la matière, **soit le premier des droits** à définir la notion de « donnée de santé ». Et ce, au-delà de l'énoncé du principe fondamental de secret, qui depuis le serment d'Hippocrate la protège sans la définir, *infra*.

Mais tel n'est pas le cas. C'est dans une optique de protection des libertés publiques, que la notion a d'abord été abordée, sans non plus être définie, en droit [110]. Voyons donc son appréhension *a minima* par le droit commun historique (section I), avant son développement unifié depuis 2002 par le droit sanitaire (section II), qui n'en pose pas moins nombre de questions, du fait du dynamisme des pratiques, des technologies et de l'organisation des soins.

S1. Une appréhension *a minima* par le droit commun historique

Longtemps, le droit commun n'a pas traité spécifiquement des données « de santé » : celles-ci ne sont qu'une variété non précisément définie, d'un concept plus large, et intuitivement compréhensible : celui on l'a vu *supra*, de « données sensibles ».

---

[108] Règlement général de protection des données (UE) 2016/679 du 27 avril 2016, dit « RGPD ».

[109] Quoique des écarts persistent entre Etats : l'étude de ces écarts a été rapportée 2021 : cf. le rapport (en anglais) pour la commission européenne, DG Health & Food safety : Assessment of the EU Member States' rules on health data in the light of GDPR, Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03.

[110] Conseil d'Etat, Septièmes entretiens du Conseil d'État en droit social « Santé et protection des données » (2017), publié sous le titre *Santé et protection des données*, La documentation française, déc. 2019.

Le droit n'en traite pour autant que ces données soient des données personnelles, **ou d'intérêt critique** pour le fonctionnement de nos institutions et la souveraineté de l'Etat. C'est donc ici en tant que « données sensibles » **au regard d'un intérêt individuel**, que ces données seront appréhendées en droit français (§1) ; puis en droit européen, où la notion de « donnée de santé » apparaît formellement pour la première fois (§2).

§1. L'AUTONOMISATION DE LA DONNEE DE SANTE EN DROIT NATIONAL

En droit français comme dans d'autres droits, l'assujettissement de la notion de « donnée de santé » ou « relative à la santé », au droit commun des « données sensibles » résulte essentiellement d'un droit voué à la protection des libertés publiques.

Soulignons dès ici : **la « donnée sensible » est une notion, non une catégorie juridique**. Même si l'onglet dédié « *donnée sensible* » sur le site de la CNIL en suggère une autonomie juridique [111], c'est par commodité, que la CNIL dénomme ainsi une « *catégorie particulière des données personnelles* ». De même, si le Règlement européen de 2016 utilisera la notion de « *donnée sensible* » (consid. 10) [112], c'est pour éviter la réincorporation dans la rédaction, de la longue dénomination de « *catégories particulières de données à caractère personnel* » (article 9), bien que la « donnée sensible » ne présente que trois occurrences dans tout le texte.

Le terme n'est donc pas à considérer à la rigueur ; on verra dans le même Règlement de 2016 souligné que « *les données à caractère personnel qui sont, par nature, **particulièrement sensibles** du point de vue des libertés et des droits fondamentaux méritent une protection spécifique* » (considérant 51). Il existe bien des grades de sensibilité, et des données sensibles sans être des données personnelles, objet en droit français d'autres protections sectorielles [113].

En matière de données personnelles, la conscience de l'enjeu de « sensibilité » est historiquement née de la crainte **d'un arbitraire de la puissance publique, non de puissances privées,** lesquelles alors ne semblaient pouvoir défier la puissance des Etats sur ce terrain. On esquissera les prémices du débat quant à la « donnée sensible » (A), avant l'avènement en 1978 de la définition de la « donnée personnelle » (B).

---

[111] CNIL, doctrine (pédagogique), https://www.cnil.fr/fr/definition/donnee-sensible

[112] Considérant 10 « *(...) le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées « données sensibles »)* ».

[113] Ainsi par exemple dans le secret de la défense nationale : Brun O, « Secret de la défense nationale », *Dictionnaire du renseignement*, Perrin éd. 2018.

A. PREMICES DE L'APPARITION DE LA NOTION DE « DONNEE SENSIBLE » EN DROIT COMMUN

Absente de la déclaration des droits fondamentaux de 1789 [114], distinctement du droit civil qui protège la vie privée de chacun [115] (et en appelle la protection pénale), du champ déontologique et du droit sanitaire (*infra*), la notion de « donnée sensible » a été **conceptualisée en droit contemporain, même sans être définie comme telle**, lors de l'encadrement légal de la statistique massifiée.

Tel est l'objet de la loi de 1951, bien avant d'être mise en exergue par la dématérialisation des flux et leur traitement informatique (seul critère d'application de la loi de 1978), qui introduit la « donnée personnelle ». Les deux notions sont on vient de le voir, différentes. Voyons donc le premier encadrement moderne en 1951 de la massification statistique (1), avant le rappel de la prévention suscitée par le projet SAFARI (2).

1. L'encadrement de la massification statistique par la loi de 1951

Le maréchal Vauban est à l'origine, au XVIIème siècle, d'un changement de dimension dans le recueil et traitement de la statistique pour l'aide à la décision publique [116]. Il systématise et promeut de façon scientifique une approche immémoriale (objet du renseignement au service de la gouvernance et du commerce, de l'ordre public, de la souveraineté et de l'art de la guerre). En santé, elle s'est fortement développée à compter du XIXème, les progrès médicaux **permettant une harmonisation progressive des outils de classification,** enjeux majeurs pour, entre autres mais ce qui nous intéresse ici, établir des statistiques [117].

---

[114] Qui se limite sur ce point (article 10) à disposer que « *Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi* ».

[115] « *Chacun a droit au respect de sa vie privée* (…) », principe d'une impérativité fondant que « *Les juges (puissent), sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé* » (article 9 du Code civil).

[116] Vauban S, Lettre sur la manière de faire les statistiques (1698) ; Caire G., « Vauban, la Défense et la cohésion de l'économie nationale », Innovations 2008/2 (n°28), pages 149 à 175.

[117] Perrot J-C., « L'âge d'or de la statistique régionale (an IV-1804) », Annales historiques de la Révolution française, 224, 1976, p. 215-276 ; Lalanne Berdouticq A.-M., « La politique des indicateurs : usages politiques et scientifiques des indices d'aptitude militaire (France – Grande-Bretagne, 1914-1923), Histoire, médecine et santé 2022 (11), pp 105-122 ; Moussy H., *Les topographies médicales françaises des années 1770 aux années 1880 : essai d'interprétation d'un genre médical*, thèse de doctorat en histoire, Université Paris 1, 2003 ; Howard-Jones N., « *Les bases scientifiques des conférences sanitaires internationales, 1851-1938* », *Chronique OMS, 28, 1974.*

Mais hors santé, durant les conflits et sous les dictatures, le recueil et tri sélectif de l'information sont aussi devenus un outil de contrôle, de discrimination, d'oppression voire d'extermination d'individus et de populations. Cela explique que la **protection des personnes soit en exergue dès la loi du 7 juin 1951** qui encadre les statistiques par ou pour l'Etat [118].

N'ayant pas pour objet principal la protection des libertés individuelles par un droit général invocable à titre personnel, cette loi « *sur l'obligation, la coordination et le secret en matière de statistiques* » est beaucoup moins connue que la loi de 1978. Mais la notion de « secret statistique » dans son article 6 y concourt, a depuis été élargie et renforcée. On en voit rapidement les principes de base, stables dans le temps, avant d'y relever **l'autonomie postérieure des questions de santé**.

a. principes de base du secret statistique

Dès sa version de 1951, la loi organise le recueil sur base déclarative obligatoire, mais interdit la communication de données individuelle qui en résulteraient ; sont concernées toutes données « *ayant trait à la vie personnelle et familiale, et d'une manière plus générale,* ***aux faits et comportements d'ordre privé*** » (article 6, al 1) **dont la santé participe**. Le texte a depuis été confirmé sous des réserves qui n'intéressent alors pas la santé (infra).

* Ce « secret statistique » [119] est un secret professionnel qui trouve pour corollaire nécessaire une sanction spécifique de sa violation [120]. Depuis, les agents publics en charge du recueil et traitement des données, et les intermédiaires privés légalement sollicités, sont tenus au secret dans le respect des articles 226-13 et -14 du code pénal.

Pour autant, ce secret n'assure qu'une protection théorique externe : il n'est **pas une garantie de légitimité d'usage interne par les services de l'Etat**. Il est significatif que la loi de 1951 prévoie dans son texte original que les « *renseignements individuels d'ordre économique ou financier (...) ne peuvent en aucun cas être utilisés à des fins de contrôle fiscal ou de répression économique* » (article 6 al 2). Les mêmes termes figurent dans le texte en vigueur, quoique le mot « *individuel* » en ait été retiré. Cette protection est censée assurer la loyauté et

[118] Loi n° 51-711, JO 08/06/1951, page 6013.
[119] Le lecteur intéressé voudra bien se référer à l'édition 2023 du Guide du secret statistique.
[120] « *Les agents des services publics et des organisations appelés à servir d'intermédiaires pour les enquêtes sont astreints au secret professionnel sous les sanctions prévues à l'article 378 du code pénal* » (art 6, al 3).

la complétude des réponses. Ainsi, **il s'agit d'un « sur-secret »,** opposable aux demandes de réquisition par toute autorité judiciaire ou administrative (services fiscaux, Douanes, etc.). Il possède son guide permettant dans l'usage de l'information, de limiter les risques d'identification (personnes physiques, mais également morales comme entreprises) [121], et est soumis à la réflexion et protection par un « Comité du secret » [122].

* En droit européen, la notion de « secret statistique » existe aussi, avec l'apparition d'un droit dédié, qui échappe au champ de notre thèse. Notons seulement ici que plusieurs textes encadrent le partage d'éléments statistiques d'intérêt commun [123]. En 2022, la question a été profondément reprise dans le Règlement sur la gouvernance des données **détenues par les Etats et organismes publics**. Ce règlement recouvre notamment les données issues des statistiques d'origine publique, dont il organise la réutilisation conditionnelle (art. 3§1, b) **[124]**.

S'il n'est pas lieu ici d'approfondir les occurrences dans ce règlement, relevons la justification générale par son considérant n° 6 : "*il arrive souvent que certaines catégories de données**, telles que (...) les données couvertes par le secret statistique** (...) figurant dans des bases de données publiques ne soient pas rendues accessibles, même pour des activités de recherche ou d'innovation relevant de l'intérêt public, bien que cette disponibilité soit possible (...). **En raison du caractère sensible** de ces données, certaines exigences procédurales de nature technique et juridique doivent être satisfaites avant leur mise à disposition, en particulier afin (...) de limiter les répercussions négatives **sur les droits fondamentaux, le principe de non-discrimination et la protection des données***".
Certes, ce texte reste mutique sur les « données de santé », mais il n'avait pas vocation à lister les « données sensibles » dont elles participent. Notons qu'il mettra en exergue la sécurité des systèmes comme condition de la protection des droits individuels [125].

[121] INSEE, « Guide du secret statistique » (dernière mise à jour en avril 2023), 13 p.
[122] Articles 6bis, 7bis et 7 ter de la loi de 1951 préc. voir https://www.comite-du-secret.fr/
[123] Règlement (CE) n° 223/2009 du Parlement européen et du Conseil du 11 mars 2009 relatif aux statistiques européennes et abrogeant le règlement (CE, Euratom) n°1101/2008 relatif à la transmission à l'Office statistique des Communautés européennes d'informations statistiques couvertes par le secret, le règlement (CE) no 322/97 du Conseil relatif à la statistique communautaire et la décision 89/382/CEE, Euratom du Conseil instituant un comité du programme statistique des Communautés européennes (JO L 87 du 31.3.2009, p. 164).
[124] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données).
[125] Déjà en ce sens, CNIL, 21e Rapp. activité 2000, p. 191 ; H. Gaumont-Prat, « Aspects éthiques de l'informatisation des données de santé dans la société de l'information », D. 2001, p. 1432.

b. aménagements spécifiques dans le champ de la santé

La santé ne devient un point de focale de la loi de 1951, **qu'avec l'aménagement ultérieur du statut des données afférentes** (dont le traitement sera soumis à la loi de 1978, adoptée entre temps ; en droit européen, la question des données de santé sera traitée de façon autonome, *infra*). Ne retenons ici que les étapes significatives.

*** Précision en 1986 du champ de recueil et droit de cession**. Le législateur adjoint en 1986 un article 7 bis à la loi de 1951. Il prévoit que les informations relatives aux personnes morales et physiques recueillies « *dans le cadre de (la) mission* » (unique contexte de recueil légal donc) peuvent être cédées « *à des fins exclusives d'établissement de statistiques* » à l'INSEE etc (principe de finalité légitime). De façon expresse, le législateur souligne « ***l'exclusion des données relatives à la santé*** *ou à la vie sexuelle* » [126], lesquelles donc alors **échappent au traitement sous cet angle** [127].

*** Extension à des données relatives à la santé en 2004**. L'article 7 bis est complété en 2004, de plusieurs alinéas (2 à 4) [128], sachant qu'entre-temps, le droit sanitaire aura apporté une première définition par inférence de la notion de « donnée de santé ». Le champ de l'analyse statistique est alors substantiellement élargi : il intègre cette fois les « *données à caractère personnel relatives à la santé* » recueillies dans les conditions légales [129].

*** Exclusion de l'identification des personnes, sauf exception légale**. La loi ajoute que, dans ce contexte autonome, « *les modalités de communication* ***des données à caractère personnel relatives à la santé*** *recueillies dans les conditions prévues à l'alinéa précédent ne doivent pas*

[126] Création par la loi n°86-1305.
[127] Le Conseil de l'Europe consacrera la notion de donnée de santé dans la convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *infra*.
[128] Ordonnance n°2004-280 du 25 mars 2004.
[129] Mais elles « *ne peuvent être communiquées, sur demande du ministre chargé de la santé* » (c'est une condition légale), à l'INSEE ou aux services des ministères « *participant à la définition, à la conduite et à l'évaluation de la politique de santé publique* » (la finalité est de gouvernance publique) que « *dans le cadre d'établissement de statistiques sur l'état de santé de la population, les politiques de santé publique ou les dispositifs de prise en charge par les systèmes de santé et de protection sociale en lien avec la morbidité des populations* » ; (le « *en lien avec* » étant, on le verra, **susceptible d'appréciation large dans d'autres contextes**). La loi de souligner que « *Des enquêtes complémentaires, revêtues du visa préalable mentionné à l'article 2, peuvent être réalisées auprès d'échantillons de ces populations* », avec un potentiel de granulométrie fine.

permettre l'identification des personnes ». En outre, le législateur prévoit qu'« *il ne peut être dérogé à cette dernière obligation que* ***lorsque les conditions d'élaboration des statistiques prévues au deuxième alinéa nécessitent de disposer d'éléments d'identification directe ou indirecte des personnes,*** *notamment aux fins d'établissement d'échantillons de personnes et d'appariement de données provenant de diverses sources »* dans le respect de la loi de 1978.

Cette exception est introduite alors que, entre temps, la loi de 1978 puis la convention européenne de 1981 auront posé les droits fondamentaux des individus, et énoncé les exceptions légitimes sur lesquelles nous reviendrons. Ce qui nous intéresse ici, est **le degré d'encadrement de l'activité de l'Etat** en matière de statistique, qui sera à comparer avec le potentiel technologique de recueil et de traitement jusqu'au « profilage » individuel [130] dont disposent les opérateurs privés du numérique fortement concentrés au plan international.

2. La prévention à l'égard de l'identifiant unique porté par le projet SAFARI

Le projet de Système automatisé pour les fichiers administratifs et répertoires des individus (dit SAFARI) est un projet qui n'a pas abouti. La question ayant donné lieu à de nombreuses publications, nous rappelons brièvement en quoi sa dénonciation a aboutit à la loi de 1978.

a. Genèse du projet SAFARI

Le projet SAFARI visait **l'interconnexion des fichiers nominatifs de l'administration** par le numéro dit « INSEE », conçu pour identifier de façon unique chaque personne physique. Cet identifiant **unique historiquement conçu comme immuable**, avait été inventé durant la seconde guerre mondiale par le CGA Carmille, alors directeur du service national des statistiques. Le but aura été de préparer secrètement la remobilisation de l'Armée française qui avait été dissoute en 1940, quoiqu'un doute plane quant à des instructions de 1941 (semble-t-il jamais exécutées) qui lui auraient assigné une autre fonction, ou une fonction additionnelle [131]. Reconstituée après la victoire, l'armée continuera d'utiliser ce code appelé « Carmille » (le n° de matricule militaire s'en est depuis distingué).

---

[130] « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel* ***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* » (RGPD 2016, article 4, §4).

[131] M.-L. Lévy, *Le numéro INSEE : de la mobilisation clandestine (1940) au projet Safari (1974)* », Dossiers & Recherche, Ined, nº 86, septembre 2000, p. 23-34

En 1946, le service national des statistiques devient l'Institut national de la statistique et des études économiques (INSEE) ; le « code Carmille » est **alors adopté par le système de sécurité sociale,** institué en 1945 par les ordonnance du Général de Gaulle. Ce numéro est dit « INSEE », mais l'Institut national de la statistique et des études économiques ne l'attribue pas : l'INSEE n'est que le gestionnaire du répertoire national d'identification des personnes physiques (RNIP), dont procède l'attribution de ce numéro [132].

Le but du projet SAFARI est, **par l'interconnexion des fichiers, d'assurer l'efficience de l'action publique**, par la dissipation d'ambiguïtés, la détection de contradictions et de redondances [133] notamment quant aux obligations des personnes physiques à l'égard de l'Etat, et quant aux prestations servies (débat d'actualité, quant à la fraude aux identités pour le bénéfice indu de prestations sociales, fraude fiscale, etc.). Il en résulte virtuellement une forte efficience de l'action publique, acceptée dans d'autres pays, nordiques notamment, mais **refusée en France du fait de la prégnance de l'inquiétude** quant au « fichage » [134].

b. Dénonciation du projet SAFARI

Le projet aurait été dénoncé par des agents informaticiens du ministère de l'intérieur, auquel on impute le souci de la préservation des libertés individuelles. Impute, car, l'époque étant de guerre froide entre le bloc soviétique et le camp occidental, diverses interprétations circulent quant aux conditions de médiatisation et d'abandon du projet SAFARI, dans le sillage des évènements de mai 1968 et le contexte politique de l'époque.

Quoiqu'il en soit, l'acronyme SAFARI permet en 1974 la publication par Ph. Boulanger d'un article retentissant : « '*Safari' ou la chasse aux français* » [135] : il exprime une inquiétude quant au **recoupement par identifiant unique**, des bases de données administratives visant à la gestion de l'état civil, de la sécurité sociale, des impôts, de l'emploi notamment.

Cet article de presse a l'effet d'ouvrir un débat fondamental sur le recueil et le traitement des « données sensibles », dans des conditions et pour des buts qui pourraient être contraires aux

[132] Décret n°82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques.
[133] J. Desabie « L'INSEE entreprend d'automatiser le rpertoire des personnes, Eco & Stat n°10, 1970.
[134] Dans des sociétés non démocratiques, la centralisation des données pour des traitements policiers ou des « crédits sociaux » (en fait, une application approfondie de police administrative pour la maîtrise de la population selon des critères comportementaux évalués en temps réel) est allée, et peut encore aller très loin.
[135] Ph. Boucher, « *Une division de l'informatique est créée à la chancellerie : « Safari » ou la chasse aux Français* », Le Monde, 21 mars 1974, p. 9.

libertés publiques. Il en résulte l'élaboration puis l'adoption en 1978 de la loi dite « informatiques et libertés » (LIL) [136]. D'emblée, la LIL va dépasser la prévention contre un éventuel arbitraire de la seule puissance publique : le **critère de son application n'est plus l'auteur, mais la technologie du traitement** des informations.

Relevons ici que la multiplication depuis des identifiants personnels (avec la multiplication des traitements informatiques publics comme privés), a conduit, en 2018, **à l'institution d'un « *système national de gestion des identifiants* ».** Il soulage les personnes de la charge mentale et/ou du risque que provoque la dispersion de leurs numéros d'identification, d'affiliation, de rattachement etc. et des codes d'accès afférents [137]. Il a encore été modifié en 2021, pour une meilleure ergonomie du Système national des données de santé (*infra*) [138].

Dans ce contexte, le numéro d'inscription au répertoire (NIR) national d'identification des personnes physiques **devrait il être considéré comme une « donnée de santé » ?** La doctrine de la CNIL retenait un temps que « *le NIR n'est pas une donnée de santé, y compris lorsque celui-ci est utilisé comme identifiant national de santé* » [139]. Puis elle a aligné sa doctrine [140] sur le RGPD de 2016, lequel considère comme donnée de santé, le « *numéro (...) attribué à une personne physique pour l'identifier de manière unique* ***à des fins de santé*** » [141].

Mais ce n'est là que l'expression d'un considérant, sans portée normative. D'ailleurs, l'article 4§15 du RGPD, qui définit la notion de « donnée de santé » **n'intègre pas cet élément.** Pas plus l'onglet sur le site de la CNIL relatif au RNIPP / NIR, qui spécifie seulement que ce numéro « *ne peut être utilisé à des fins de recherche des personnes* » [142].

---

[136] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[137] Décret n° 2018-390 du 24 mai 2018 relatif à un traitement de données à caractère personnel dénommé « système national de gestion des identifiants ».
[138] Décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».
[139] CNIL, « Qu'est-ce qu'une donnée de santé ? » (communiqué non daté, cité par L. Maisnier-Boché fasc 945 n° 14, information non modifiée en avril 2023).
[140] Ibid. CNIL, « Qu'est-ce qu'une donnée de santé ? », site CNIL (nouveau communiqué non daté, vérifié octobre 2022).
[141] Considérant n°35. Participent en effet de cette catégorie « *(...) un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé* ».
[142] CNIL, « RNIPP : Répertoire national d'identification des personnes physiques » (onglet daté 19 juin 2009, vérifié octobre 2022).

B. CONSEQUENCES DE L'APPARITION DE LA NOTION DE « DONNEE SENSIBLE »

Le problème soulevé est certes l'interconnexion des fichiers existants, mais plus encore la **nature et le degré des informations** qu'ils peuvent contenir : ils confèrent déjà un potentiel de description fine par croisement de données, pour une finalité potentielle de discrimination, mais aussi d'explication, d'évaluation et de prédiction [143]. Il n'est pas lieu ici de revenir sur la genèse de la loi Informatiques et libertés (LIL) [144], ni de la commission dédiée (CNIL).

On en rappelle les seuls principes et en tant qu'ils intéressent la santé : la question qui y est initialement traitée de façon lapidaire (1), puis récemment, considérablement développée **sur une base nationale (non seulement sous l'influence, ultérieure, du règlement européen** de 2016 dédié à la protection générale des données personnelles) (2).

1. Place originelle de la santé dans la LIL de 1978

La LIL de 1978 ne contient pas de référence à des données relative à la santé ou concernant la santé. Certes, un rapport qui en 1974 l'a précédée, soulignait qu'il est **«** *des données personnelles qui méritent une protection renforcée ; ce sont* ***en tout cas celles qui sont relatives à la santé mentale et physique*** *des personnes* » [145].

Le « *en tout cas* » mettait alors en exergue leur caractère primordial. Pour autant, elles n'y ont pas donné lieu à une invocation expresse (a), et n'apparaîtront qu'ultérieurement (b).

a. Absence d'invocation expresse des données de santé

En 1980, il est précisé qu'« *il est interdit de mettre ou conserver en mémoire informatisée, sauf accord exprès de l'intéressé, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales (…)* » [146]. **La santé n'apparaît alors toujours pas**.

---

[143] Pour rappel, le profilage est défini comme « « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel* ***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* » (RGPD 2016, article 4, §4). »

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

[145] Rapport Commission Informatique et Libertés 1974, Doc. fr. 1975, p. 58

[146] Article 31 modifié.

En 1994, un Chapitre V bis : *Traitements automatisés de données nominatives ayant pour fin la recherche* ***dans le domaine de la santé*** (Articles 40-2 à 40-1) y est créé par une loi visant spécifiquement la recherche dans le domaine de la santé [147], **mais toujours sans incorporer expressément la notion de donnée de santé** aux données nominatives.

Or, il est remarquable que la même loi dispose déjà (article 40-9, abrogé en 2004) spécifiquement, que **«** *La transmission hors du territoire français de données nominatives* ***non codées*** *faisant l'objet d'un traitement automatisé* ***ayant pour fin la recherche dans le domaine de la santé*** *n'est autorisée, dans les conditions prévues à l'article 40-2,* ***que si la législation de l'Etat destinataire apporte une protection équivalente à la loi française*** » [148].

Enfin, le Conseil constitutionnel **a en 1999 lié les questions** du régime de communication des données de santé, à la sauvegarde du respect de la vie privée des personnes [149].

b. Introduction des « données personnelles de santé »

Plusieurs recommandations de la CNIL ont précédé le complément dédié de la loi, comme en 1997 [150]. En fin juillet 1999, le législateur crée un Chapitre V ter dans la LIL : Traitement des **données personnelles de santé** à des fins d'évaluation ou d'analyse des activités de soins et de prévention (articles 40-11 à 40-15) [151]. Cela correspond à une occurrence spécialisée qui vient **en sus du principe général de protection**.

En 2001, apparaissent les premières préoccupations quant aux sites internet de santé [152]. Mais **c'est sur un autre terrain, que la loi est modifiée** en 2002 : dans le sillage de la loi du 4 mars 2002, le législateur introduit dans la LIL une disposition spécifique quant à l'exercice du droit d'accès lorsqu'il « *s'applique* ***à des données de santé à caractère personnel*** » : celles-ci « *peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet (...)* ». Or, cela n'est qu'une redondance, droit des patients / des personnes (infra).

---

[147] Loi n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[148] On y reviendra avec la dynamique intracommunautaire des soins transfrontières, et avec les décisions de la Cour européenne de justice en 2016 et 2020 quant au transfert de données aux Etats-Unis, Partie II, titre II.

[149] Considérant n°51, Décision n° 99-416 DC du 23 juillet 1999 (contrôle de conformité de la loi portant création d'une couverture maladie universelle).

[150] CNIL, « Recommandation sur le traitement des données de santé à caractère personnel », Délib. n° 97-008, 4 févr. 1997.

[151] Loi n°99-641 du 27 juillet 1999 portant création d'une couverture maladie universelle.

[152] CNIL, « Recommandation sur les sites de santé destinés au public », Délib. n° 01-011, 8 mars 2001.

Dès lors, ce n'est qu'en 2004, qu'apparaît **la première évocation intrinsèque (c'est à dire non rattachée à un régime de recherche, ni d'accès) de la notion de donnée relative à la santé.** Ainsi (article 8 modifié), **«** *I. - Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes,* ***ou qui sont relatives à la santé*** *ou à la vie sexuelle de celles-ci* » [153].

En 2018, les « données relatives à la santé ou à la vie sexuelle » deviennent les « ***données concernant la santé*** *ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* (sic) ». Ce changement n'a aucune conséquence en droit, sinon l'alourdissement de la formulation.

2. Place contemporaine de la « donnée de santé » dans la LIL modifiée

En introduction de notre thèse, nous avons souligné que la LIL n'avait jamais défini en soi la « données de santé ». Son article 30 dispose seulement que « *les traitements de données à caractère personnel* ***dans le domaine de la santé*** *sont régis par* (…) » les articles 64 à 67. Dès lors, ce « domaine de la santé » ne s'étend *a priori* qu'aux activités ainsi limitativement énoncées. Or, cela fait *a priori* qu'une donnée **ne participant pas du « domaine » ainsi défini, semble ne pouvoir être « de santé ».**

a. autonomie du traitement des données « concernant la santé »

La question ici implicitement posée est celle de **l'origine organique de la production**, et le degré de rattachement à la définition de la donnée de santé par le droit sanitaire. Nous verrons que les périmètres ne se supposent pas nécessairement.

Le traitement des données concernant la santé est **autonome à un double titre**. D'une part, en raison de son évocation intrinsèque on l'a dit, qui va ouvrir dans la LIL un régime développé que nous ne ferons ici qu'esquisser, puisque ce régime est hors de notre sujet [154] ; d'autre part, parce que depuis 2018, les données de biométrie et génétique sont traitées

[153] Modifié par la loi n°2004-8001 du 6 août 2004.

[154] Sur ce point, voir L. Maisnier-Boché, Fasc. 945 : Données de santé à caractère personnel. – Régime général, Jurisclasseur communication, Lexis 360 (2023) spéc. n° 31 et s.

distinctement dans la LIL [155] ; et naturellement par le CSP, du fait de leur statut et protection particuliers. Le point d'intérêt ici est le **potentiel de telles données en santé.**

La donnée génétique peut éclairer un état voire posséder un potentiel prédictif – quoiqu'il faille relativiser cette prétention (« *la génétique propose, l'épigénétique dispose* » [156]). **Ces données étaient considérées de façon consubstantielle**, avant la technicisation des textes [157] (elles seront à nouveau réunies dans la notion englobante de « *donnée de santé électronique* » pour un usage spécifique, si la proposition européenne de mai 2022 est adoptée).

De même, l'évolution de caractéristiques biométrique. Pour cela, elles doivent pouvoir être comparées sur des temps longs (c'est un volet de la sémiologie médicale). Par exemple, la Commission européenne a décidé en 2014 de financer directement le projet « *'Wize Mirror' to help you stay healthy* » : cette technologie permet la prévention des maladies cardio-métaboliques dans un miroir intelligent suivant des caractéristiques biométriques [158]. En juin 2023, le 23ème amendement déposé par le Parlement européen quant au considérant n° 7 du projet de règlement sur l'intelligence artificielle, développe spécifiquement ce point [159].

b. développement du régime des « données de santé » dans la LIL modifiée

Il n'est pas lieu ici d'établir un historique, ni une description du régime de ces données, une fois la notion de « *donnée concernant la santé* » introduite [160]. On relèvera simplement que cette notion **est invoquée, mais pas définie** (il faudra chercher la définition ailleurs) ; et que des sections complètes afférentes de la loi, ont été à plusieurs reprises restructurées.

---

[155] Modifié par la loi n°2018-493 du 20 juin 2018.

[156] Pour une approche didactique (2010), https://www.academie-medecine.fr/les-bases-de-lepigenetique/

[157] Rappelons l'article 1 de l'annexe de la recommandation n° R(97)5 du comité des ministres du Conseil de l'Europe : « *l'expression «données médicales» se réfère à toutes les données à caractère personnel relatives à la santé d'une personne. Elle se réfère également aux données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques ; - l'expression «données génétiques» se réfère à toutes les données, quel qu'en soit le type, qui concernent les caractères héréditaires d'un individu ou qui sont en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés* ».

[158] https://digital-strategy.ec.europa.eu/en/news/wize-mirror-help-you-stay-healthy

[159] (adopté le 14 juin 2023). Le nouveau considérant 7ter est ainsi rédigé : « *La notion de catégorisation biométrique, telle qu'employée dans le présent règlement, devrait définir l'affectation de personnes physiques à des catégories spécifiques, ou la déduction de leurs caractéristiques et attributs, tels que le genre, le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou sociale, la santé, les aptitudes mentales, les traits liés au comportement ou à la personnalité, la langue, la religion ou l'appartenance à une minorité nationale ou l'orientation sexuelle ou politique, etc., sur la base de leurs données biométriques et de données fondées sur la biométrie ou qui peuvent être déduites de ces données* ».

[160] V. L. Maisnier-Boché, Fasc. 945 : Données de santé à caractère personnel. – Régime général, préc.

La mise en conformité du droit français avec le Règlement de 2016 dit RGPD (infra) a en effet conduit à développer dans la loi le « *Chapitre IX : Traitements de données à caractère personnel dans le domaine de la santé* (Articles 53 à 65) » ; les traitements relevant de ce chapitre « *ne peuvent être mis en œuvre* ***qu'en considération de la finalité d'intérêt public*** *»* que constitue notamment *« la garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux* ».

Ce chapitre de la LIL réunit une Section 1 « *Dispositions générales* » (articles 53 à 60), et une section 2 : « *Dispositions particulières relatives aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé* » (articles 61 à 65). Ces dernières s'entendent comme celles décrites en droit français. Nous constaterons que le droit distingue **selon que les personnes qui s'y prêtent sont « impliquées », ou « participent ».** Mais cette distinction, par ailleurs source de confusions, n'existe qu'en droit français, *infra*.

§2. L'AUTONOMISATION DE LA DONNEE DE SANTE PARMI LES « DONNEES SENSIBLES » EN DROIT EUROPEEN

Par « droit européen », on entend ici deux catégories de textes de sources différentes : en premier lieu, les textes proclamant des droits fondamentaux des personnes, qui ont une vocation très générale à s'appliquer ; la jurisprudence a alors tracé les contours de la notion, sans véritablement la définir (A).

En second lieu, le premier texte technique européen dédié à la protection des « données personnelles », un peu plus disert. Il était la base du droit en la matière, jusqu'à son abrogation en 2016 (à effet 2018) par le Règlement général de protection des données (B).

A. LES « DONNEES DE SANTE » DANS LES INSTRUMENTS PROTEGEANT LES DROITS FONDAMENTAUX

Nous ne considérons ici que l'environnement juridique européen, nous traiterons de l'environnement juridique américain en seconde partie, sous un autre angle.

Nous examinerons ici la place formelle limitée des « données personnelles » (*a fortiori* « de santé ») dans la Convention européenne des droits de l'homme (1) ; puis dans la Charte européenne des droits fondamentaux, seule norme opposable aux institutions européennes (2).

1. Silence de la Convention européenne des droits de l'homme sur les « données de santé »

Entrée en vigueur en 1953, la Convention européenne des droits de l'homme a été, au plan international, **le premier instrument juridique rendant contraignants certains des droits** proclamés dans la Déclaration Universelle des Droits de l'Homme adoptée en 1948.

Voyons ici ses dispositions pertinentes en matière de protection des données personnelles, avant la jurisprudence qui en résulte et qui s'impose aux Etats partie à cette convention, **mais pas à l'Union européenne** en tant que personne de droit public international (b).

a. Mutisme sur la notion de « données personnelles » dans la CEDH

L'article 8, inchangé depuis le texte d'origine en 1950, pose le principe de la protection des données personnelles en termes très généraux : sous l'intitulé « *Droit au respect de la vie privée et familiale* », il dispose que (8.1) « ***Toute personne a droit au respect de sa vie privée*** *et familiale, de son domicile et de sa correspondance* » et (8.2) qu' « ***il ne peut y avoir ingérence d'une autorité publique*** *dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales,* ***à la protection de la santé*** *ou de la morale, ou à la protection des droits et libertés d'autrui* **».**

Cet article 8 ne **contient aucune référence au traitement automatisé de données**, technique certes balbutiante au moment de l'adoption de la Convention, mais qui n'a jamais donné lieu intrinsèquement à des protocoles additionnels, dont nombre sont survenus depuis [161]. En outre, elle **focalise sur l'ingérence de l'Autorité publique**, qui n'est aujourd'hui plus le seul défi.

Enfin, il n'y est pas précisé selon que l'exception de « protection de la santé », qui doit être prévue par la loi, vaut pour l'individu (ce quoi vers tend la dénomination de droit de l'homme) ou la collectivité.

[161] La Convention a depuis sa formalisation en 1950, donné lieu à ce jour 16 protocoles additionnels à vocation de fond et de procédure.

Or, ce questionnement ne relève pas du sophisme : **il existe des situations dans lesquelles la question de l'arbitrage entre intérêts fondamentaux peut se poser** [162]. Avant même cette jurisprudence, un « *Guide sur l'article 8 de la Convention européenne des droits de l'homme* » a été publié en août 2022 [163]. Il contient plusieurs § dédiés à la protection des données personnelles [164], au droit d'accès [165], au droit à être informé sur son état de santé [166].

b. Apport des textes ultérieurs sous l'égide du Conseil de l'Europe

Si la CEDH est mutique sur ce point précis, d'autres instruments de même source (Conseil de l'Europe) lui sont dédiés.

* Ainsi depuis 1981, la Convention STE (série des Traités européens) n°108 **pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel** a pour objet la protection des droits et libertés fondamentales « *notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés* » [167].

Cette convention a été modifiée par procole en 2018 pour y insérer les données biométriques et génétiques [168] ; la France vient de la ratifier en avril 2023, mais elle est toujours non applicable, 16 autres ratifications étant requises. Son article 6 spécifie les données ne pouvant faire l'objet d'un traitement automatisé sans garanties appropriées. Ainsi en est-il expressément des « *données à caractère personnel* ***relatives à la santé*** ».

* En outre, une recommandation (non génératrice d'obligations) du comité des ministres du Conseil de l'Europe de 1997, vise spécifiquement la **protection des données médicales** [169], dans le sillage d'une recommandation du même comité en 1981 ; cet objet n'apparaissait pas dans l'énoncé, mais dans le texte (4ème considérant ; annexe articles 5, 6 et 8) [170].

---

[162] Ainsi en septembre 2022 dans l'affaire Drelon c. France, *infra.*
[163] Site CEDH, Guide mis à jour le 31 août 2022, « *Préparé au sein du Greffe. Il ne lie pas la Cour* ».
[164] Ibid. (2022), points 206, p 58.
[165] Ibid. (2022), points 207 à 211, p. 58-59.
[166] Ibid. (2022), points 212 à 216, p. 59-61.
[167] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janvier 1981, n° 108.
[168] STCE (Séries des Traités du Conseil de l'Europe) n° 223, Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
[169] Recommandation n° R (97) 5 du Comité des ministres aux Etats membres relative à la protection des données médicales, adoptée par le Comité des ministres le 13 février 1997 (584e réunion des délégués des ministres).
[170] Recommandation n° R (81) 1 du Comité des ministres aux Etats membres relative à la réglementation applicable aux banques de données médicales automatisées (adoptée par le Comité des Ministres le 23 janvier 1981 (328e réunion des Délégués des Ministres).

Or, cette recommandation de 1997, qui dès son 2ème considérant met en exergue la convention n°108, dispose que « *l'expression 'données médicales' se réfère à toutes les données à caractère personnel* ***relatives à la santé d'une personne****. Elle se réfère également aux données* ***ayant un lien manifeste et étroit avec la santé ainsi qu'aux*** *données génétiques* » (annexe, article 1). Nous avons critiqué cette approche dans l'introduction de notre thèse, et relevé la recommandation en 2015, d'abandon d'une telle définition au profit de celle simple de « donnée de santé » [171]. Nous ne nous y attarderons donc pas.

* Enfin, pendant du droit fondamental au respect de la vie privée, un article visant l'interdiction de la discrimination a été adopté en 2005, par voie de protocole additionnel à la Convention [172]. Il porte interdiction générale de la discrimination « *fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance* ***ou toute autre situation*** ». Paradoxalement **la santé n'y figure pas expressément, en contraste** des normes et recommandations antérieures précitées.

Pour autant, un guide dédié a été aussi publié (mis à jour en 2022), qui détaille par revue jurisprudentielle la question de la discrimination [173]. Il traite notamment **de la discrimination « *fondée sur la santé et le handicap* »**, sachant que dans la jurisprudence CEDH, la question du handicap (physique, mental) prédomine sur celle de la santé (statut sérologique) [174].

c. Place de la jurisprudence dans la sanction en santé des « données personnelles »

L'article 8 a donné lieu à de nombreuses décisions de la CEDH, et à l'édition d'une fiche thématique de synthèse de jurisprudences (version décembre 2022). Celle-ci focalise sur la question du traitement des « données personnelles » – la problématique étant intimement liée à l'interprétation du large article 8. Il n'est pas lieu ici de la paraphraser [175].

[171] Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), « Rapport de présentation visant à mettre à jour la Recommandation n° R (97) 5 du Conseil de l'Europe sur la protection des données médicales ».
[172] Protocole n° 12 entré en vigueur en 2005, voir article 14 de la Convention.
[173] Guide sur l'article 14de la Convention européenne des droits de l'homme et l'article 1 du Protocole n°12 à la Convention – interdiction de la discrimination (mise à jour 31 août 2022).
[174] Ibid. (2022), points 169 à 178, p. 43-45.
[175] Fiche thématique – Protection des données personnelles déc. 2022, sur le site de la CEDH. Il est spécifié que cette fiche ne lie pas la Cour et n'est pas exhaustive.

Notons seulement que **la « donnée de santé » n'y est pas définie**. Seule la sanction de la finalité et proportionnalité de l'ingérence en trace les contours, **ce qui requiert une analyse du domaine** : ainsi « *pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu (*un aspect de la vie privée*) (...), **la Cour tiendra dûment compte du contexte particulier** dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés (...)* » [176]. **Il n'y a pas ici de qualification « en soi »**.

Distinctement de cette fiche thématique de 2022, *l'item* titré « *Droit à être informé sur son état de santé* » dans le Guide, également de 2022, désigne curieusement son contenu. En effet, les jurisprudences de la CEDH rapportées **mettent plutôt en exergue le respect du caractère confidentiel des données à caractère plus ou moins médical** dans différents contextes (sérologie positive, obtention de permis de conduire, attestation de capacité professionnelle, contentieux matrimonial, exemption de service militaire, transmission de données à un assureur des soins, divulgation de données à des journalistes, etc.). **L'examen systématique de proportionnalité n'a pas conduit à une conceptualisation intrinsèque des « données de santé », laquelle n'est pas nécessaire** au regard de la lettre de l'article 8.

Enfin, dans une affaire Drelon c. France tranchée en septembre 2022, la Cour européenne des droits de l'homme a jugé la France coupable d'une violation de ce droit au respect de la vie privée et familiale [177]. Le plaignant avait porté plainte **contre l'Etablissement français du sang, en raison de la collecte et conservation par cet établissement de données personnelles** reflétant son orientation sexuelle supposée ; d'autre part, contre les refus opposés à ses candidatures au don du sang, et contre le rejet par le Conseil d'Etat de son recours pour excès de pouvoir contre l'arrêté de 2016 qui modifiait les critères de sélection des candidats à un tel don.

Le cas est intéressant : **ici sont confrontés une responsabilité de santé publique (sécurité transfusionnelle), et un droit personnel protégé au titre de la CEDH**. La Cour sanctionne, d'une part, le caractère spéculatif des données collectées par l'Etablissement français de don du sang [178] ; d'autre part, la durée jugée disproportionnée de conservation des données

[176] CEDH, Grande chambre, 4 déc. 2008, Aff. S. et Marper c. Royaume Uni, req. n°30562/04 et 30566/04.
[177] Arrêt de chambre, CEDH 278 (2022), 8 septembre 2022, req. n° 3153/16 et n° 27758/18.
[178] Qu'il a inférées du refus, par le requérant, de répondre à des questions relatives à sa sexualité lors de l'analyse en colloque singulier, des risques et contre-indications au don.

litigieuses – cette durée rendant possible leur utilisation répétée à l'encontre du requérant, entraînant en l'espèce son exclusion automatique et définitive du don.
On y reviendra ci-dessous.

2. La protection générale au titre de la Charte des droits fondamentaux de l'union européenne

Par le Traité de Lisbonne en 2007, l'Union s'était engagée à adhérer à la « Convention européenne des droits de l'homme » [179]. Si les Etats membres de l'Union en font partie à titre national, tel n'est en effet toujours pas le cas de l'Union européenne en tant que communauté politique, malgré un dialogue ancien en ce sens [180]. **Ainsi, les citoyens européens peuvent déférer leurs Etats, mais non l'Union européenne, devant la juridiction de la CEDH**.

Mais il n'en résulte pas une inopposabilité, à l'Union, de droits fondamentaux des personnes. Depuis 2000, leur définition et opposabilité sont le but de la « Charte des droits fondamentaux de l'Union européenne » [181], qui complète les outils internes du droit européen. Elle **rehausse les droits fondamentaux au-delà de l'énoncé essentiellement technique** des directives et règlements relatifs seulement à la protection des données personnelles, *infra*.

a. Laconisme de la Charte européenne quant aux « données personnelles »

L'article 8 de la Charte **est sobre, mais plus explicite** que son pendant dans la CEDH de 1981, car elle met en exergue des « données » : « *Toute personne a droit à la protection des données à caractère personnel la concernant* » (article 8.1). Le même pose un principe de loyauté de traitement ; une finalité déterminée et consentie, ou un fondement légal légitime ; un droit d'accès et de rectification par l'intéressé (8.2). Il met en exergue la soumission du respect de ces règles, au contrôle d'une autorité indépendante (8.3), laquelle est depuis 2004, le Contrôleur Européen de la Protection des Données (CEPD), *infra*.

---

[179] Depuis l'entrée en vigueur du Traité de Lisbonne (1er décembre 2009) et du Protocole 14 à la CEDH (1er juin 2010), l'adhésion n'est plus simplement un souhait, c'est une obligation juridique.
[180] La CJUE a le18 décembre 2014, rendu son avis 2/13, concluant que l'accord d'adhésion de l'Union européenne à la Convention européenne des droits de l'homme n'est pas compatible avec l'article 6(2) du TUE ou avec le protocole (n° 8) relatif à l'article 6(2) du TUE relatif à l'adhésion de l'Union à la convention européenne des droits de l'homme.
[181] Charte des droits fondamentaux de l'Union européenne, adoptée le 7 déc. 2000, Traité de Nice. Le traité de Lisbonne de 2007 lui confère une valeur contraignante à l'instar du droit originaire.

Notons ici que l'adhésion de l'Union à la CEDH aurait notamment l'effet que l'Union soit intégrée au système de protection de droits fondamentaux de la CEDH ; **avec l'effet d'une application cumulative des textes ?**

Tenue de respecter son droit sanctionné par la CJUE, l'Union aurait alors aussi l'obligation de respecter la Convention sous le contrôle de la Cour européenne des droits de l'homme (**ce que cette dernière perçoit comme une augmentation de cohérence** [182]). Mais cela sans doute se discute-t-il ? S'il est douteux qu'une divergence d'interprétation pointe quant aux droits fondamentaux, cela ne saurait plus être exclu, du fait de leur extension continue. Or, une divergence poserait un problème majeur.

Certes, il est **a priori douteux que de tels problèmes se posent quant à l'interprétation de « données personnelles »**. Mais l'on ne saurait exclure de divergences potentielles dans des domaines intéressant par exemple les données relatives à l'état civil, la question des genres, la mémoire des transitions, l'accès aux traitements correspondants par exemple de mineurs [183], de clandestins, etc. Les causes et conséquences du changement de sexe de naissance, puis d'état civil jusque dans les dossiers médicaux, par exemple, **ne relève pas de l'anecdote, du fait de sa pertinence en santé** pour la protection même des personnes intéressées [184].

En outre, le cas tranché en 2022 par la CEDH contre la France a pointé, à juste titre, un délai excessif de conservation d'information [185]. Mais, par ailleurs, la Cour ne fait-elle prévaloir un droit fondamental de l'individu, sur le droit fondamental de la collectivité en matière de sécurité transfusionnelle ? L'inférence, du silence de la personne, d'une situation à risque, **est certes une donnée spéculative, non factuelle.** Mais constatons ici que le questionnaire est médicalement justifié, et protégé sous secret professionnel ; que le système repose entièrement sur la confiance, et sur une base déclaratoire : cela n'est-il pas raisonnablement respectueux des droits des personnes, **dans l'arbitrage entre des intérêts fondamentaux** ?

b. un improbable (mais possible) potentiel de divergences jurisprudentielles

---

[182] Site CEDH, onglet Adhésion de l'UE à la CEDH, vérifié janvier 2023.

[183] Sur les enjeux juridiques très discutés aux Etats-Unis pour les personnes concernées et pour les praticiens, C. Mallory, MG. Chin, JC. Lee « Legal Penalties for Physicians Providing Gender-Affirming Care ». *JAMA.* Published online May 18, 2023. doi:10.1001/jama.2023.8232

[184] Cl. Junien, N. Priollaud, *C'est votre sexe qui fait la différence*, Plon 2023 ; De façon emblématique, F. Nik-Ahd, A. De Hoedt, C. Butler et al. « Prostate Cancer in Transgender Women in the Veterans Affairs Health System, 2000-2022 ». *JAMA.* Published online April 29, 2023. doi:10.1001/jama.2023.6028.

[185] Arrêt de chambre, CEDH 278 (2022), 8 septembre 2022, req. n° 3153/16 et n° 27758/18.

Plusieurs rapports ont été élaborés qui visent une application effective de la Charte, consistant à promouvoir une culture des droits fondamentaux dans l'Union européenne, y promouvoir l'égalité entre hommes et femmes, aider les citoyens à exercer leurs droits. En 2011, un rapport européen se félicite de ce que, hors du champ d'application de la Charte (aucun citoyen de l'Union d'un Etat membre n'étant en cause), le Conseil constitutionnel en France ait pris le relais pour veiller au respect de droits fondamentaux lors de l'adoption de règles relatives à l'expulsion [186].
Ce rapport en infère une « *confirm(ation) que dans les cas où le droit de l'UE n'est pas applicable, c'est le droit national, notamment par l'intermédiaire des tribunaux, qui prend le relais pour veiller au respect des droits fondamentaux* » [187] ; **en fait sous le contrôle juridictionnel de la CEDH** précitée, pour les Etats partie à la convention.

Il en résulte que, pour une personne non citoyenne de l'Union, la protection des droits fondamentaux à l'égard des traitements informatisés de données personnelles **ne relèverait pas de la Charte européenne des droits fondamentaux, mais de la Convention européenne des droits de l'homme**.

Outre les questions précitées, des conséquences de crise sanitaire ou migratoire, d'urgence de santé publique face à des (risques de) maladies transmissibles affectant des groupes en transit, sont prégnantes. Défi croissant, elles **font partie des exceptions légitimes à l'invocation des droits individuels** quand est en question la « donnée de santé » [188].

La santé notamment, est considérée pour l'évaluation de la vulnérabilité des demandeurs d'asile : en 1998, un titre de séjour pour raison de santé avait été instauré [189], très discuté depuis [190] ; en 2016, un régime juridique dédié a été consacré, lequel par « *étranger malade* », traite essentiellement des personnes en situation irrégulière **ne relevant donc pas de nationalités de l'Union** [191], et suppose le croisement de toutes données correspondantes.

---

[186] Conseil constitutionnel, décision n° 2011-625 DC du 10 mars 2011,
[187] Rapport de la Commission au Parlement au Conseil, au Comité économique et social européen et au comité des régions – Rapport 2011 sur l'application de la charte des droits fondamentaux de l'Union européenne, COM(2012) 169 Final.
[188] Séminaires de la RFAS / Migrations et santé : « Migration et santé : sélection, prévention et soin » (2 février 2023), « Migration et santé **publique** » (20 mars 2023), actes à paraître à la Revue fr. Aff. Soc. 2024.
[189] Loi Debré n°97-396 du 24 avril 1997 en ce qui concerne la protection contre l'éloignement, et la loi n° 98-349 du 12 mai 1998 qui en fait un motif de délivrance de plein droit d'une carte de séjour temporaire *« vie privée et familiale. »*
[190] Y. Charpak, C. Chaix Couturier, M. Danzon, « Demander un titre de séjour pour raisons de santé : que sait-on des systèmes de santé des pays d'origine ? » in Trib. De la Santé 2017/4 n°57, 97-106.
[191] Loi n° 2016-274 du 7 mars 2016 relative au droit des étrangers en France.

Dans ce contexte, la mise en œuvre de l'Aide médicale d'Etat, qui vise à la protection à titre gratuit de la santé de personnes en situation irrégulière, est déclinée en plusieurs programmes [192]. L'accès à ceux-ci suppose de renseigner un formulaire (CERFA 11573*09), lequel permet de distinguer les situations. Ainsi, la collecte des données dans un but d'accès à la couverture de prestations les place à mi-chemin entre une donnée purement administrative et une « donnée de santé », si l'on retient l'acception la plus large proposée.

Or, il est encore relevé en 2022 que « *L'absence d'articulation entre politique de l'immigration et prise en charge des soins délivrés aux étrangers en situation irrégulière* ***met une nouvelle fois en cause la pertinence de l'inclusion de l'AME à la mission « Santé »,*** *son rattachement à la mission « Immigration, asile et intégration » ayant été évoqué à plusieurs reprises dans les débats parlementaires* » [193]. Cela **n'aurait pas pour objet de changer le statut des données,** mais leur portage pour le volet administratif / social [194].

La sensibilité de la ligne de partage entre ces deux missions, les coûts croissants et les tentatives de maîtrise de la dynamique d'engagement de l'AME, comme le potentiel de collision avec des décisions de la CEDH, autorisent à s'interroger quant aux conditions futures d'acquisition et de conservation, **cette fois au statut,** des données correspondantes.

B. LES DONNEES DE SANTE SOUS L'ANGLE DE LA DIRECTIVE DEDIEE AUX DONNEES PERSONNELLES ?

En 1995, avant donc la Charte européenne des droits fondamentaux, le droit européen a, par la directive 95/46/CE (abrogée en 2016 par le RGPD) [195], organisé la protection des données personnelles à l'échelle communautaire (1).

---

[192] V. le Projet de loi de finances pour 2023 – note de présentation mission « Santé » Examen par la commission des finances mercredi 2 novembre 2022 ; Rapporteur spécial, Chr. Klinger (spéc. pp 26 et s).

[193] Projet de loi de finances pour 2023 – note de présentation mission « Santé » Examen par la commission des finances, préc. pp 34 et s.

[194] Le considérant n°35 du RGPD dispose que « *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 (...) au bénéfice de cette personne physique (...)* ».

[195] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Le droit européen a prévu la consultation impérative du Contrôleur européen de protection des données (CEPD) : suite à l'analyse de cette directive, cela va conduire ce dernier **à formuler une doctrine prospective** (2).

1. L'institution d'un droit européen de la protection des données par la Dir. 95/46/CE

La directive n° 95/46 est le **premier texte qui institue un droit commun général de protection des données** à caractère personnel faisant l'objet d'un traitement automatisé [196]. Elle poursuit un double but : fluidifier les échanges intracommunautaire, tout en promouvant la démocratie en se fondant sur les droits fondamentaux reconnus notamment dans la Convention européenne de sauvegarde des droits de l'homme et libertés fondamentales (avant nous l'avons vu, que l'Union ne se dote d'un référentiel propre de droits fondamentaux).

a. La fluidité de la circulation des données par la garantie des droits fondamentaux

Pour réaliser l'objectif de fluidité, cette directive 95/46 met en exergue le besoin d'un « *niveau de protection des droits et libertés des personnes à l'égard du traitement de ces données (…) équivalent dans tous les Etats membres* » [197] : **cela supprime l'invocabilité, par les Etats, d'obstacles à cette circulation, qui seraient tirés d'écarts entre droits fondamentaux**.
Mais la suppression des obstacles à la liberté de circulation **ne vaut que dans les champs couverts par la directive.** Dès lors, cela exclut les questions concernant la sécurité publique, la défense, la sureté de l'Etat, et le volet pénal de la matière judiciaire [198] ; mais cela **recouvre implicitement les soins de santé, quand bien même cette matière** est de compétence essentiellement nationale (art. 186 TFUE) [199].

Pour autant, la Directive de 1995 ne fait que poser de grands principes. Cela, même lorsqu'elle énonce sous couvert de « *catégories particulières de traitement* » (intitulé de la section III), des dispositions relatives aux « *Traitements portant sur des catégories particulières de données* » (intitulé de son article 8). Cet article dispose que les Etats membres interdisent, au rang des autres données dont le traitement est prohibé, « *le traitement **des données relatives à la santé*** » **sous réserve notamment** du consentement explicite de la personne intéressée (article 8.2a), de la défense de ses intérêts vitaux (article 8.2.c), **et d'une finalité médicale**.

---

[196] Transposé en droit français par loi n° 2004-801 du 6 août 2004 modifiée (JO 7 août 2004, p. 14063).
[197] Ibid., consid. n° 8.
[198] Activités alors visées aux titre V et VI du Traité de l'Union, sans préjudice des obligations incombant aux Etats au titre des articles 56§2, 57 et 100A du Traité.
[199] Ce dernier point n'exclut en effet pas, que les principes de liberté d'activités intracommunautaire lui soient applicables (art. 114 TFUE).

L'article 8.3 prévoit expressément l'inapplicabilité de l'article 8.1 « *lorsque le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé* », si ce traitement est opéré par un praticien de la santé autorisé selon le droit national applicable, soumis à une obligation de secret professionnel ou équivalente.
C'est l'unique exception dans l'article 8, qui à nouveau définit la « donnée de santé » par inférence, par l'énoncé d'activités soumises au secret professionnel, ou équivalent [200].

b. une application jurisprudentielle peu éclairante du contenu

La CJUE a été **saisie par voie préjudicielle** de l'interprétation de la Directive 95/46, alors qu'était alléguée une infraction de la législation suédoise relative à la protection des données à caractère personnel, consistant en la publication sur un site Internet privé, de données concernant des personnes travaillant comme bénévoles pour une paroisse locale [201]. Il était alors reproché à l'une d'elles par le ministère public suédois, d'avoir « *traité sans autorisation des données à caractère personnel sensibles, à savoir celles relatives à une blessure au pied et à un congé de maladie partiel* ».

Faits certes reconnus, mais infraction niée par l'intéressée, laquelle se pourvoit en appel devant la juridiction suédoise de renvoi. Celle-ci saisit la Cour européenne notamment **sur la qualification des faits au regard du champ de protection par la directive** [202].

La réponse est lapidaire : **eu égard à l'objet de cette directive, la Cour juge qu'il convient de donner une interprétation large** à l'expression de données « relatives à la santé », « *de sorte qu'elle comprenne des informations* ***concernant tous les aspects,*** *tant physiques que psychiques, de la santé d'une personne* » [203]. Cela est très large, ne définit pas la notion, ni même n'en trace les contours ; **il n'est pas nécessaire qu'une affection soit précisée**.

[200] Nous verrons que cela contrastera fortement avec l'approche du RGPD adopté en 2016.
[201] CJCE 6 nov. 2003, aff. C-101-01 Lindqvist. pt 97 : Rec. CJCE 2003, I, p. 12971 ; Europe 2004, comm. 18, note F. Mariatte ; Rev. Lamy dr. civ. janv. 2004, p. 29, note G. Marraud des Grottes ; D. 2004, p. 1062, obs. Burgogue-Larsen ; Comm. com. électr. 2004, comm. 46, note R. Munoz ; D. 2004, p. 470 ; RSC 2004, p. 712, obs. L. Idot.
[202] Ibid., points n° 15 et 16.
[203] Ibid., point 50.

L'infraction étant constituée, l'article 8.1 de la Directive 95/46 est applicable, les exceptions ne sont pas activées (ni activables). A la différence d'autres questions préjudicielles posées dans la même affaire, **aucune observation n'a ici été soumise à la Cour par des Etats observateurs,** suggérant que nul autre ne voyait là matière à discussion. On en conviendra.

Mais est-ce là dire que la formulation de l'article 8.1 et son interprétation large « *appelée par l'objet de la directive* » résolvent toutes questions à venir ? Dans un contexte différent, **cela n'apparaît pas satisfaisant** au Contrôleur Européen de protection des Données (CEPD).

2. L'interprétation par le CEPD de la notion de « données de sante »

La directive 95/46 va donner lieu à une interprétation **non plus jurisprudentielle, mais doctrinale,** par le CEPD saisi en 2008.

Avant cela même, écartons tout risque de confusion : l'acronyme CEPD désigne tout à la fois le Contrôleur européen pour la protection des données, créé en 2001 [204], institué en 2004 et renforcé en 2018 [205] ; et le Comité européen pour la protection des données [206], entré en vigueur en 2018 (qui remplace le groupe de travail dit « de l'article 29 »), qui a un rôle de conseil auprès des institutions. Afin d'éviter toute confusion, nous recourons aux acronymes CEPD pour le contrôleur, et EDPB (*European Data Protection Board*) pour le Comité.

Les circonstances de la saisine du CEPD sont sa consultation sur la proposition de directive sur les soins transfrontaliers : elle devait faire l'objet d'un avis préalable de sa part (a). Il y **constate et regrette l'absence de définition de la notion de « donnée de santé »** (b).

a. la proposition de directive de 1995, premier texte contrôlé en « domaine de la santé »

C'est pour la première fois en 2008, que le CEPD a l'occasion d'interpréter la Directive 1995/46 relative à la protection des données personnelles **en matière de soins de santé**. Il est

[204] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.
[205] Renforcé par le Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE
[206] Institué par le règlement (UE) 2016/679 (RGPD).

alors est saisi de la proposition de directive qui deviendra la Directive 2011/24 sur les soins transfrontaliers, sur laquelle nous reviendrons en seconde partie de notre thèse.

Or, cela est pour lui **l'occasion assumée de formuler une doctrine ambitieuse :** il se réjouit de cette opportunité d'« *observations (...) de portée très large — elles abordent des questions générales relevant de la protection des données à caractère personnel* ***dans le secteur des soins de santé*** *— et* ***pourraient dès lors valoir aussi pour d'autres instruments législatifs (contraignants ou non) relevant du même domaine*** » [207]. Nous approfondirons ce point dans l'analyse de l'apport du règlement général de protection des données de 2016.

Dès lors, le CEPD relève l'évidence que « *la mise en place d'un système de soins transfrontaliers requiert l'échange (...)* ***de données à caractère personnel pertinentes relatives à la santé des patients****. Considérées comme sensibles, ces données sont soumises aux règles de protection renforcée énoncées à l'article 8 de la directive 95/46/CE, qui traite de catégories particulières de données* » (point 4 du projet d'avis).

b. Le constat de l'absence de définition des « données de santé »

Mais c'est l'occasion pour le CEPD de constater la faiblesse de la proposition de directive sur la question de la protection de ces données. Il passe en revue le projet (nous ne détaillerons pas son avis), pour conclure lapidairement que « *Tout cela donne l'impression* ***qu'une approche globale du respect de la vie privée dans le cadre des soins de santé n'est pas encore clairement définie et que, dans certains cas, elle fait complètement défaut*** » [208].

Dans le considérant n° 24 de la directive n° 2011/24/UE, **la notion n'est ainsi qu'esquissée.** Elle convoque « *par exemple les données figurant dans leurs dossiers médicaux contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement ou intervention entrepris* ». Mais son article 3 ne contient pas de définition des « données relatives à la santé » : **dans cet article, les « données » sont une composante non autonome,** qui n'est citée **qu'en tant que participant des dossiers** [209].

[207] Point 5, du Projet d'avis du contrôleur européen de la protection des données concernant la proposition de directive du Parlement européen et du Conseil relative à l'application des droits des patients en matière de soins de santé transfrontaliers (2009/C 128/03).
[208] Ibid., fin du point 7.
[209] Au côté des évaluations et les informations de toute nature concernant l'état de santé d'un patient et son évolution clinique au cours du traitement), du « dossier médical », seul défini (cf. article 3, m)

Or, cela est amplifié par l'article 14-2 de la même proposition de directive (dédié à la santé en ligne). Cet article indique que les objectifs du réseau « santé en ligne » consistent à notamment à « *b) élaborer des orientations concernant : i)* ***une liste non exhaustive de données à faire figurer dans le dossier des patients et pouvant*** *être partagées par les professionnels de la santé pour permettre la continuité des soins et promouvoir la sécurité des patients par-delà les frontières* ». D**epuis, les données se sont échappées du dossier patient**.

La critique par le CEPD de la proposition de directive qui sera adoptée en 2011, le conduit à proposer une définition fondée sur une norme ISO. Cette suggestion ne sera pas finalement relayée dans la Directive de 2011/24, nous le verrons *infra*.

Peu après, le groupe de travail dit de l'article 29 (qui deviendra le Comité européen pour la protection des données, titré EDPB pour ne pas le confondre avec le Contrôleur) **va émettre un avis très différent quant à la notion de « donnée de santé » [210]**, qui n'a pas non plus été retenu dans l'élaboration du règlement de 2016. Nous l'examinerons *infra*.

En attendant, **une autre dynamique va découler de l'appréhension intrinsèque, par le droit de la santé**, de la notion de « donnée de santé »**.**

SECTION II. L'APPREHENSION INTRINSEQUE DE LA DONNEE DE SANTE PAR LE DROIT DE LA SANTE

Dans notre 1ère section, nous avons vu l'appréhension de la notion de donnée de santé **par le droit non sanitaire** : celui-ci devait traiter, d'une part, du cadre juridique de l'analyse statistique par l'autorité publique ; d'autre part, du cadre juridique de la protection des données personnelles selon leurs usages, sous l'angle des droits fondamentaux.

De ce fait, **l'appréhension intrinsèque de la « donnée de santé » par le droit sanitaire est paradoxalement récente.** Nous voyons ici qu'elle n'était pas en soi définie par le droit qui encadre le secret médical devenu « de santé », lequel énonce une **obligation à la charge des professionnels** impliqués dans les soins, dont on infère une qualification de la donnée (§1).

[210] Article 29 Data Protection Working Party, Lettre du 5 février 2015, voir surtout son « ANNEX - Health Data in Apps and Devices ».

Sa définition progressive ne résulte pas tant d'une modification des conditions d'exercice des professionnels (qui toutefois impactera la géométrie du secret), que de l'énoncé de droits désormais **au profit du patient**, distincts de ceux protégés par la LIL (§2).

§1. LA « DONNEE DE SANTE », INFEREE DU CHAMP MATERIEL DE PROTECTION DU SECRET DE SANTE

Institution fondamentale dans l'intérêt privé et public, le secret « de santé » relève autant (et d'abord !) de la déontologie professionnelle, que du droit. Nous relevons ici une dynamique forte, quant à la qualification de l'information couverte par cette obligation généralisée (A). Depuis toujours, elle relie le secret individuel de santé à des enjeux de souveraineté (B).

A. L'ENONCE LIMITE DU CHAMP MATERIEL DU SECRET DE SANTE

Le « secret médical » et l'évolution de son régime sont l'objet de nombreuses publications. Notons seulement ici qu'en 2002 (*infra*), la loi consacre ce secret comme un **droit, non de protection de l'information, mais de la personne à maîtriser les données la concernant** (expression, à l'échelle individuelle, de la souveraineté – mais au-delà d'une conception qui réduirait le pouvoir conféré aux individus à une finalité de régulation du marché [211]).

Or, ce droit possède une signification distincte du droit d'accès et de rectification organisé par la LIL. En ce sens, la Cour de cassation souligne en 2020 que le secret est instauré dans le seul intérêt du patient afin de garantir la confidentialité **des informations qu'il donne à son médecin** [212], ce qui lui rend loisible d'y renoncer.
Mais quels sont les éléments couverts ? Voyons rapidement ici son champ matériel (1), dont la stratification a évolué avec la **diversification des interactions** professionnelles (2).

1. La « donnée de santé », définie par inférence du champ matériel du secret

Il est un adage médical connu qu'*« il n'y a pas de soins sans confidences, de confidences sans confiance, de confiance sans secret ». Relevons l'unification d'obligations auparavant dispersées (a), avant de voir la consubstantialité de ce secret et de la vie privée (b).*

[211] Nous souscrivons à l'interrogation de E. Netter qui évoque en ce sens le concept imagé de « souveraineté personnelle », in « La portabilité, un droit à inventer ? », Dalloz IP/IT, Dalloz, 2020, pp.352-357.
[212] Crim, 13 octobre 2020, 19-87.341, publié au Bulletin.

a. de la dispersion des obligations à leur unification

En 1985, une jurisprudence porte en ce sens une approche commune explicite : « (attendu que) *si celui qui a reçu la confidence d'un secret a toujours le devoir de le garder, la révélation de cette confidence* ***ne le rend punissable que s'il s'agit d'une confidence liée a l'exercice de certaines professions*** *; Que ce que la loi a voulu garantir c'est la sécurité des confidences qu'un particulier* ***est dans la nécessité de faire a une personne dont l'état ou la profession dans un intérêt général et d'ordre public fait d'elle un confident nécessaire*** » [213].

Or, ces attendus semblent mettre en exergue un critère fondamental : **la nécessité de la confidence – non la découverte incidente, ou la confidence non nécessaire**, qui sont pourtant aussi une manière d'approcher la « donnée de santé » [214].

L'obligation spécifique doit être distinguée de la sanction par le droit pénal commun d'une violation du secret professionnel, lequel **n'est pas l'apanage des professions de santé** [215]. Avant la loi de 2002, qui l'unifie l'obligation dans le Code de la santé publique [216], **c'est de façon dispersée** dans les Codes de déontologie des professions de santé, que l'obligation est définie dans leurs champs respectifs d'intervention. Elle ne l'est pas dans les mêmes termes : **seul le secret médical, est défini dans des termes extensifs**.

* Ainsi, selon l'*a*rticle 4 du Code de déontologie médicale (article R.4127-4 du code de la santé publique) *« Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire* ***non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris*** *».*

C'est dire que l'obligation de secret faite au médecin **ne se limite pas aux informations de santé**, ce que déjà proclamait le serment d'Hippocrate. Dès lors, cela est **l'expression déontologique formelle la plus large du secret exigible, si on la compare** par exemple au secret dans le Code de déontologie des pharmaciens et des infirmiers.

---

[213] Crim, 19 novembre 1985, 83-92.813, publié au Bulletin.
[214] Mais qui apparaît bien réductrice, au regard de l'étendue du serment d'Hippocrate.
[215] B. Py, Le secret professionnel, L'Harmattan éd. 2005. L'auteur y note, en parallèle de la multiplication des catégories de personnes assujetties, la multiplication des exceptions et dérogations.
[216] Quoiqu'apparaissent des occurrences spécifiques, comme pour le conseil en génétique, *infra.*

* Pour les pharmaciens « *le secret professionnel s'impose à tous les pharmaciens dans les conditions établies par la loi » (R. 4235-5 CSP en vigueur à la date de la rédaction).* Le commentaire (2013) du Code de déontologie publié sous l'égide de l'Ordre des pharmaciens [217] dépasse de loin, l'énoncé formel restreint, par le Code, du secret des pharmaciens ; cette doctrine le rapproche de celui du médecin : le **secret couvre les déductions et le recueil incident de toute information privée**, hors de la relation entre patient et pharmacien.

* Dans le Code de déontologie des infirmiers, récent car créé en 2016, puis modifié en 2020 [218], le secret est défini d'une façon similaire (R. 4312-5 CSP) au Code de déontologie des pharmaciens. Mais dans le commentaire publié par l'Ordre des infirmiers, il est aussi très développé [219]. Il n'est pas lieu de développer ces points plus allant.

Tous les codes en effet convergent, **pour aspirer dans le champ matériel du secret exigible, outre les informations relatives à la santé, toutes autres informations privées qui n'en relèvent pas directement** (ce qui n'en ferait *a contrario* pas des données « de santé » [220]). Les commentaires institutionnels des codes étant l'expression d'une doctrine ordinale, ils éclairent l'interprétation probable, devant les juridictions disciplinaires, de l'étendue (large, donc) de l'obligation de secret professionnel à l'égard de toute information « en » santé, non seulement des données « de » santé.

b. Le secret des informations « en » santé, consubstantiel au respect de la vie privée

Distinctement des Codes de déontologie propres aux exercices professionnels, la loi du 4 mars 2002 **a institué un principe général de secret des informations concernant le patient**, intégrant les acquis jurisprudentiels [221] : elle en a tracé un **champ unifié et élargi** à d'autres

[217] Ordre national des pharmaciens, Commentaire du Code de déontologie, mars 2013.
[218] Décret n°2016-1605 du 25 novembre 2016 ; modifié par Décret n° 2020-1660 du 22 décembre 2020 portant modification du code de déontologie des infirmiers et relatif notamment à leur communication professionnelle. Auparavant, existaient des règles professionnelles codifiées (décret du 16 févr. 1993) mais non autonomisées dans un Code de déontologie.
[219] Code de déontologie des infirmiers, version commentée (2020), p. 20 à 27. Site de l'Ordre.
[220] Mais nous verrons que la notion s'est fortement étendue dans les textes européens les plus récents.
[221] Le Code de déontologie médicale commenté, les cahiers de l'ONP (site de l'Ordre), p. 14.

acteurs en santé et d'action médico-sociale ; elle a aussi défini les informations que l'obligation recouvre, **mais toujours sans définir les « données de santé »**.

Ainsi dans sa formulation d'origine en 2002, l'article L. 1110-4 alinéa 1 disposait que « *Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant* » [222]. En 2016, **la loi a effacé la notion « d'information médicale »,** pour évoquer de façon générique les « informations **concernant la personne** » [223].
De façon heureuse, ceci **harmonise le champ du secret légal avec le champ du secret déontologique,** lequel embrasse toute la sphère de l'intimité (*supra*).

En 2020, la Cour de cassation rappelle aussi que « *le médecin, dépositaire du secret médical, doit, **quel que soit son mode d'exercice, personnellement veiller à ce que les personnes qui l'assistent** soient instruites de leurs obligations en matière de secret professionnel et s'y conforment* » [224] ; la même obligation est faite, dans leurs Code de déontologie respectifs, aux autres professions (R. 4235-5 pour les pharmaciens, R. 4312-5) pour les infirmiers, etc.).

La Cour de cassation rappelle que « *l'infraction prévue à l'article 226-13 du code pénal est destinée à protéger la sécurité des confidences qu'un particulier est dans la nécessité de faire à une personne dont l'état ou la profession, dans un intérêt général et d'ordre public, fait d'elle un confident nécessaire* ». **Mais nous avons vu que cela vaut pour toute information acquise de façon incidente même par un personnel non effecteur de soins**, c'est à dire sans lui avoir été spécialement confiée, ni même intéresser son activité professionnelle.

En droit, le fait que les professionnels tenus au secret doivent instruire les personnes qui les assistent de leurs obligations, **conduit à rendre ce secret quant aux données, exigible y compris de personnels non professionnels de santé** (personnels administratifs, comptables, de ménage, etc. qui n'ont pas à en connaître), **sachant pour autant ces personnels non débiteurs d'une obligation de secret professionnel** [225].

---

[222] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.
[223] Modifié par Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.
[224] Préc., Crim, 13 octobre 2020, 19-87.341, publié au Bulletin.
[225] A cet égard, les attendus de Crim. 19 novembre 1985, 83-92.813, préc., sont particulièrement intéressants.

Dès ici, on conçoit le contraste avec le monde numérique de la collecte continue d'informations multiples, non issues de la sphère ou du sillage des soins, mais possédant une signification médicale par agrégation et/ou par inférence.

c. Autonomie de l'information génétique

Dans le Livre du CSP dédié à la protection des personnes en matière de santé, l'examen des caractéristiques génétiques, l'identification par empreintes génétiques et la profession de conseiller en génétique, sont l'objet d'un titre III dédié (articles L. 1131-1 à L. 1133-10). Ne relevons ici que l'autonomie de la consultation (i), et de la transmission de la donnée (ii).

i) Autonomie de la consultation d'information génétique.

La consultation génétique pour un des buts énoncés dans le titre III est soumis à un cadre particulièrement strict par le droit français, sachant que l'examen d'identification génétique **ne possède pas toujours une finalité médicale ou médico-légale**. Dans certains pays, l'identification génétique (voire la généalogie génétique) est l'objet d'un marché peu vigilant, quant à la légitimité des demandes et à la protection des informations collectées.

En France, non seulement ce **régime est très strict**, mais les conseillers et les étudiants se préparant à cette profession sont soumis à l'obligation de secret professionnel **mise en exergue distinctement du droit général** des patients. Ainsi depuis 2004, « *Les conseillers en génétique et les étudiants se préparant à la profession sont tenus au secret professionnel dans les conditions et sous les peines énoncées aux articles 226-13 et – 14 du Code pénal* » [226].

Or, bien que s'applique le principe général posé par l'article L. 1110-4 précité, **l'énoncé autonome de cette obligation n'apparaît pas redondant**. L'optique n'est en effet pas nécessairement celle d'une prise en charge sanitaire (d'un patient), même si une telle hypothèse est la première couverte par l'article L. 1132-1 CSP pour tracer le cadre d'action (« *Le conseiller en génétique, sur prescription médicale et sous la responsabilité d'un médecin qualifié en génétique, participe au sein d'une équipe pluridisciplinaire* »). Par ailleurs, l'analyse génétique **relève de l'activité de laboratoire, ne contient pas de dimension sociale ni clinique**, du moins jusqu'à la consultation médicale même, le prélèvement biologique ne conduisant qu'à une surface limitée d'échanges.

[226] Création par Loi n°2004-806 du 9 août 2004.

ii) Autonomie de la transmission de l'information (donnée) génétique.

En 2021, la loi relative à l'étendue de l'obligation de secret à la charge des professionnels de santé a été précisée dans ce champ. Ainsi, l'article L. 1110-4-V CSP dispose-t-il que « *le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée* ***nécessaires à la prise en charge d'une personne susceptible de faire l'objet d'un examen des caractéristiques génétiques*** *dans les conditions prévues au I de l'article L. 1130-4 soient délivrées au médecin assurant cette prise en charge, sauf volonté contraire exprimée par la personne avant son décès* » (4ème alinéa) [227].

Ce focus vise à régler une situation délicate non expressément couverte par le texte antérieur, lequel n'isolait pas (mais n'incluait pas) ces données pouvant être demandées.

2. Quelle extension du champ matériel par l'obligation professionnelle ?

Nous venons de le relever qu'existait dans le CSP une **dynamique des informations couvertes par le secret professionnel : de la santé, à la non-santé**. Il en résulte une obligation pour les professionnels de santé d'instruire leurs collaborateurs de leurs devoirs en matière d'information « en » santé, **les données « de » santé n'étant pas encore individualisées, mais implicitement recouvertes**.

Ces devoirs valent quand bien même ces personnels opérant dans la santé ou en périphérie ne seraient pas eux-mêmes soumis à un secret unifié par le CSP comme droit fondamental du patient, ni spécialement sanctionné au titre de devoir professionnel par le Code pénal.

a. La distinction des « Professions de santé » et des « professionnels de santé »

Existe-t-il en santé **une dynamique des acteurs concernés, de façon principale ou incidente,** par l'évolution de la notion d'information à caractère privé (au delà des la transformation de l'organisation des soins et des modes d'exercice, que nous verrons *infra*) ?

Le Code de la santé publique définit les « Professions de santé » dans la IVème partie : ce droit vise à déterminer leurs champ d'intervention, établir les qualifications requises, les conditions de formation initiale et continue, etc. sachant que les formes autorisées d'exercice

[227] Modifié par la loi n°2021-1017 du 2 août 2021, article 14.

professionnel (droit spécifique des sociétés) sont parfois définies hors de la IVème partie [228]. A juste titre, madame Moquet-Anger a récemment relevé que **les notions de « Professions de santé » et de « professionnels de santé » ne se recoupaient pas parfaitement** [229].

Ainsi, nombre d'activités ne sont pas définies dans la IVème partie du Code : ostéopathes, chiropraticiens, psychologues, sophrologues, etc. Cela n'exclut pas que leurs prestations, non remboursées par l'assureur obligatoire des soins (Code de la sécurité sociale), puissent être **prises en charge par des organismes dits « complémentaires santé »,** disposant d'une liberté de référencement compétitif de leurs prestations.

En outre, on observe en droit certains mouvements, qui rendent les catégories d'intervention professionnelle poreuses [230] : ainsi depuis la LFSS 2022, la prise en charge de consultations par la sécurité sociale de psychologues.
Elle est motivée par l'impact psycho-social des confinements suite à la pandémie de Covid19, et leurs effets potentiels sur l'équilibre mental [231]. Mais il n'en résulte pas que le psychologue, lequel n'est pas psychiatre (i.e. pas médecin), soit en conséquence reçu dans la IVème partie « professions de santé » du Code.

La question n'est pas anodine. Le concept à géométrie très variable de « santé » (de l'absence de maladie et d'infirmité, à l'état de complet bien être physique, psychique et social », cf. introduction) pourrait avoir un **effet d'attraction dans le champ des activités de santé donc du CSP et dans le champ des « données de santé »,** tout ce qui y contribue.
Or cela est impossible.

i) cas non ambigus

Certains auteurs comme madame Moquet-Anger évoquent une réticence des pouvoirs publics à consacrer, dans le livre « Professions de santé », des activités qui ne donnent pas lieu à un remboursement selon les critères du Code de la sécurité sociale [232].

---

[228] Ainsi notamment pour les pharmaciens, les formes juridiques des sociétés d'exercice professionnel ne sont pas définies dans dans cette IVème partie, mais dans la Vème partie « Produits de santé », etc.
[229] M.-L. Moquet-Anger, « Professions et professionnels de santé », in Actes du Colloque de l'AFDS, n° spécial hors série Revue de droit sanitaire et social 2022, pages 99-108.
[230] Si l'on voit aussi apparaître des professions de santé « intermédiaires », celles-ci toutefois participent de catégories légales préexistantes ; ainsi depuis 2016, les infirmiers de pratique avancée Loi n° 2016-41 du 26 janv. 2016 de modernisation de notre système de santé.
[231] LFSS n° 2021-1754 du 23 déc. 2021 ; décret n° 2022-195 du 17 février 2022/
[232] En ce sens, M.-L. Moquet-Anger, préc., 99.

Mais force est ici de relever que l'absence de production des services par des « Professions de santé » au titre formel du CSP, comme de prise en charge de la prestation par les assureurs obligatoires des soins au titre du CSS, n'a **aucune incidence sur la qualification du but poursuivi, et donc sur la qualification de la donnée générée**. La question deviendra plus complexe, lorsque la donnée « de santé » est générée sans même poursuivre un tel but, ce qui est un des aspects majeurs de notre recherche.

L'article 226-13 du Code pénal prévoit que l'on est soumis au secret professionnel **par « *état ou par profession, par fonction ou mission temporaire* ».** Les professions de santé telles que définies en IVème partie du CSP sont elles seules redevables de l'obligation de secret énoncé à l'article L. 1110-4 CSP ? Sont-elles les seules, à devoir sensibiliser/former les autres personnes qui les assistent (ce qui ne signifie pas entre eux partage du secret, infra) ? Il existe d'autres **cas d'obligation expresse**, pour une activité hors CSP, mais relevant du Code de l'action sociale et des familles (L. 411-3 CASF) : ainsi pour les assistants sociaux [233].

ii) cas ambigus

Il existe des cas ambigus, comme celui porté par l'article L. 2213-1 CSP, modifié en 2021, lequel traite de l'interruption volontaire de grossesse : il dispose que dans l'équipe pluridisciplinaire qui doit accompagner la femme que la poursuite de sa grossesse mettrait en péril grave, doivent figurer outre les « professionnels de santé » (tels que définis donc dans la IVème partie du CSP), « *une personne qualifiée tenue au secret professionnel, qui peut être un assistant social ou un psychologue* ».

Or, le psychologue n'est pas une profession que la loi astreint au secret professionnel [234], à la différence des assistants sociaux préc. **C'est donc une mission ou fonction spécifique, qui, le faisant dépositaire de données de santé, l'y assujettit** [235].

---

[233] « *Les assistants de service social et les étudiants des écoles se préparant à l'exercice de cette profession sont tenus au secret professionnel dans les conditions et sous les réserves énoncées aux articles 226-13 et 226-14 du code pénal. La communication par ces personnes à l'autorité judiciaire ou aux services administratifs chargés de la protection de l'enfance, en vue de ladite protection, d'indications concernant des mineurs dont la santé, la sécurité, la moralité ou l'éducation sont compromises n'expose pas, de ce fait, les intéressés aux peines fixées par l'article 226-13 du code pénal*. »

[234] La loi n° 85-772 du 25 juillet 1985 portant diverses dispositions d'ordre social, qui a régulé l'usage du titre de psychologue, ne mentionne pas le respect du secret professionnel parmi leurs obligations légales.

[235] Voir l'analyse complète de B. Bruyère, Les psychologues et le secret professionnel, Ed. Armand Colin 2011, p 31 et 32.

Ainsi, on ne peut inférer d'une jurisprudence de 2001, l'assujettissement *per se* du psychologue à une obligation de secret professionnel [236] : **c'est une erreur d'interprétation** [237]. Certes, les syndicats de psychologues se sont spontanément dotés d'un Code de déontologie qui énonce une obligation de secret, mais celui-ci ne possède pas de force contraignante [238]. Cela ne retire rien à la force d'un engagement unilatéral visant la confiance. **Qui pourtant douterait qu'ils traitent de « données de santé »,** même sans être médecins.

En 2022, une question parlementaire soulève à nouveau ce point devant le Sénat [239].
En 2023, la réponse du ministère de la santé et de la prévention confirme le constat précédant, que les deux ne sont pas nécessairement liés : « *le secret professionnel* ***constitue une obligation et peut également constituer une infraction pénale****, en cas de violation de cette obligation, ainsi que le dispose l'article 226-13 du code pénal* » ; « *En conséquence, en dehors des cas où la loi impose ou autorise la révélation du secret et des cas énumérés à l'article 226-14 du code pénal, l'obligation de respecter le secret professionnel, au sens de l'article 226-13 du code pénal, s'applique aux psychologues, non en raison de leur titre, mais par profession, ou en raison d'une fonction ou d'une mission temporaire* » [240] – ce qui apparaît discutable quant à l'élément « profession » : l'ambiguïté n'est elle pas réintroduite ?

Pour notre champ de recherche, cela pose par exemple la question de jeux vidéos en ligne co-élaborés par des psychologues, dans lesquels peuvent être **encapsulés des scores de psychologie de type MBTI [241] visant à établir des préférences comportementales** de joueurs (de tous âges etc.) dans des environnements variés et renouvelés, avec un potentiel d'usage à finalité prédictive de réactions dans des situations futures « réelles » voire critiques.

b. La clarification de la notion de « professionnel » habilité à connaître du secret

---

[236] Crim. 26 juin 2001, 01-80.456, Inédit. La Cour rapporte entre guillemets, une considération ***qui n'est pas la sienne***, selon laquelle « *si un psychologue n'a pas la qualité de médecin, cette profession est elle aussi soumise au secret professionnel établi par l'article 226-13 du Code pénal* ».
[237] Voir la démonstration de E. Barthe, Les arrêts de la Cour de cassation : y faire référence, les analyser, les interpréter sans erreur ; V. l'onglet « OpenData juridique », sur le site https://www.precisement.org/blog/Les-arrets-de-la-Cour-de-cassation-y-faire-reference-les-analyser-les
[238] C'est même son article 1, dont les limites sont exposées dans un article 19.
[239] J.-P. Sueur, Question écrite n° 01818, JO Sénat du 28/07/2022 - page 3986.
[240] Réponse à QE n° 01818, Rép. Ministère de la santé et de la prévention , JO Sénat du 12/01/2023 - page 209.
[241] Myers Briggs Type Indicator (souvent dit « test MBTI »), outil d'évaluation psychologique mis au point en 1962, établissant de façon fine des préférences comportementales parmi 16 types psychologiques différents. Son usage est, en principe (et par licence commerciale) subordonné à l'exercice d'une fonction ou mission sous secret professionnel exprès. Il a des applications civilo-militaires. Il existe d'autres types de scores/tests beaucoup plus développés.

La loi a depuis **clarifié les notions « d'échanges » et de « partage » des données**, et a organisé leurs régimes (*infra*). Notons seulement ici qu'un décret d'application en 2016 pose une catégorie réglementaire (c'est-à-dire non légale) de personnes considérées comme « professionnels », pour les habiliter à partager des informations avec les « professionnels de santé » au sens du CSP. Le libellé du décret est parfaitement explicite [242].

Les Professions de santé au sens de la IVème partie du CSP sont concernées, identifiés au titre d'une première catégorie d'acteurs (R. 1110-2-1°), **mais également tous les personnels relevant de « sous-catégories » de la catégorie définie par le 2°.** Il en résulte un nombre importants d'acteurs concernés, y compris des non professionnels de santé [243], ce qu'expliquera l'apport de la loi de 2016 de modernisation du système de santé au profit notamment de son décloisonnement.

La condition est naturellement leur association à la prise en charge, sous réserve de l'accord du patient ; cela détermine une « mission » ou une « fonction », qui les attire *ipso facto* dans l'orbite du secret professionnel pénalement sanctionné (*supra*), car les **faisant dépositaires à degrés variables, de données de santé**.

B. ENJEU DE SOUVERAINETE LIE AUX DONNEES DE SANTE PROTEGEES PAR LE SECRET

Le principe général de protection de l'information personnelle est posé en frontispice du Code de la santé publique (1110-4 CSP). Pour autant, il ne s'applique qu'aux circonstances, organisations, actions et professionnels que le CSP définit, et ne couvre donc à l'évidence pas la totalité des cas de génération de données « concernant la santé ». Dès ici, **la donnée de santé ne peut plus être réduite à la production organique du système décrit par l'application combinée** ou non, des codes (CSP, CASF et CSS) [244].

[242] Décret n°2016-994 du 20 juill. 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico social et l'accès aux informations de santé à caractère personnel.
[243] Ibid. « *Art. R. 1110-2.-Les professionnels susceptibles d'échanger ou de partager des informations relatives à la même personne prise en charge appartiennent aux deux catégories suivantes : 1° Les professionnels de santé mentionnés à la quatrième partie du présent code, quel que soit leur mode d'exercice ; 2° Les professionnels relevant des sous-catégories suivantes* » (s'ensuit une liste détaillée de professions rattachées à 9 catégories).
[244] Pinilla E, Megerlin F, De la donnée de santé par qualification de la loi, à la donnée de santé « par destination », RGDM 2018(1), 99-112.

Dans ce contexte, nous voyons rapidement ce qu'il en est de la **souveraineté des individus sur leurs données « de santé »,** du fait des conséquences de cette qualification (1). Nous ne traiterons pas ici de la question de la souveraineté liée à l'information relative aux personnes physiques dirigeantes, évoquée en introduction [245]. Nous verrons déjà ici en quoi la maîtrise (refus d'obtention par un Etat tiers) de telles données **à l'échelle populationnelle, pourtant cédées par les personnes concernées**, est affaire de souveraineté (2).

1. « Souveraineté » des bénéficiaires du secret professionnel, à quel point ?

La loi du 4 mars 2002 a consacré un principe général de secret des informations médicales, c'est-à-dire des données de santé. Mais ce secret a été étendu nous l'avons vu aux informations concernant le patient par la suppression en 2016 du qualificatif « *information médicale* » en 2016, avec l'effet d'élargir le champ des données de santé. Nous n'entrerons pas dans le détail du droit des personnes en la matière, qui a fait l'objet sur le site du service public de fiches explicatives claires, qu'il n'est pas lieu de paraphraser [246].

Toutefois il y manque un *item*, relatif à la **renonciation globale ou sélective par le bénéficiaire même de son vivant, au secret relatif à sa santé ou plus largement relatif à sa vie privé [247]**.
En effet, les deux sont consubstantiels, d'un point de vue déontologique et désormais légal (supra). Esquissons ici le fondement du secret des données de santé (a), qui conduit à se demander de quel ordre public cette règle relève (b).

a. Le secret des « données de santé » : d'intérêt public, autant que d'intérêt privé

En juin 2022, l'Ordre national des médecins a diffusé un nouveau Commentaire du Code de déontologie médicale. Ce commentaire (doctrine de pédagogie et d'interprétation, opposable aux professionnels et à l'Ordre même) souligne que le secret professionnel du médecin ou

[245] Accoce P, « Secrets et défense médicale - Chefs d'Etat et dirigeants s'efforcent de tout savoir sur la santé de leurs pairs. Et de ne rien laisser paraître de la leur », *in* L'Express, 23 juin 1998 ; Le Person X., « Usages et discours de la maladie dans l'art de la négociation politique (…) (1585) », *in* Belmas E et Michel MJ (dir.), *Corps, santé, société. Actes du colloque de Paris du 12-13 décembre 2002*, Paris, Nolin, p. 155-172 ; Nevejeans P., « Le corps souffrant et ses enjeux diplomatiques », *in* Bull. Centre de recherches du château de Versailles, 2016; Dossier, *Quel est l'état de santé de nos chefs d'Etat ?* Jeune Afrique (2017) https://www.jeuneafrique.com/dossiers/quel-est-letat-de-sante-de-nos-chefs-detat/
[246] https://www.service-public.fr/particuliers/vosdroits/F34302
[247] On trouvera une réflexion sur ce point précis de Netter E. qui évoque l'idée de « souveraineté individuelle », *in* « La portabilité, un droit à inventer? », Dalloz IP/IT, Dalloz, 2020, pp.352-357

secret médical « ***est à la fois d'intérêt privé et d'intérêt public*** ». Le régime du secret, mis en perspectives selon les circonstances et droits applicables, y est particulièrement détaillé [248].

Pour synthétiser, le secret est d'intérêt privé en tant qu'il protège l'intimité et la dignité de la personne, et que sa garantie est une condition de la confiance nécessaire à l'acte médical. Il est d'intérêt public (notamment d'un point de vue de santé publique), **afin que nul,** quel que soit sa condition sociale (situation marginale, irrégulière, interné, précaire, etc.), **ne soit dissuadé de demander un soin** par crainte d'être dénoncé.

On peut rapprocher ici, naturellement dans la sphère très différente couverte par le secret statistique au titre de la loi de 1951, *supra*. **Ce secret dans l'intérêt privé interdit également, dans l'intérêt public, la communication à des services étatiques**, afin de ne pas provoquer un biais comportemental dans le recueil des données vouées à un tableau de bord pour une **mission de gouvernance : celle-ci a priorité explicite sur la détection et répression de certaines infractions** que les données pourraient révéler.

Il n'est pas lieu d'entrer plus allant dans ce régime en santé, lequel n'est pas l'objet de notre thèse. On notera toutefois, que si les dérogations ne concernent pas de la même façon les autres professions de santé [249], le principe peut être considéré comme les liant également.

En effet, le mutisme des autres Codes de déontologie ou commentaires des codes sur la question de l'« intérêt public » est explicable par la technicité et les circonstances propres à ces exercices. Cela **n'implique aucunement que les considérations développées dans le commentaire du Code de déontologie médicale ne leur soient pas toutes applicables**.

Nous considérons que d'un point de vue déontologique, et sans que cette déontologie soit nécessairement codifiée, ces considérations s'appliquent [250]. Pour chacune des « Professions » du IVème livre CSP, mais aussi pour tous les professionnels qui n'y sont pas inscrits, cette double vocation du secret nous semble pertinente [251], et recouvre toutes les données : en

[248] CNOP, « Nouveau Commentaire du Code de déontologie médicale » (2020), v. p 25 à 43.
[249] Les dérogations aux règles d'exercice professionnel au profit d'acteurs CSP ou non relèvent de cas légaux exprès, lesquels caractérisent les situations et identifient strictement les professionnels débiteurs de l'obligation de signalement ou de transmission etc. d'informations intéressant la santé.
[250] N'est-ce pas là du bon sens, que l'on pourrait même qualifier de civique ?
[251] Ce n'est pas le cas dans tous les pays : Plaiasu M, Alexandru D, Nanu C, « Physicians' legal knowledge of informed consent and confidentiality. A cross-sectional study » ; Sankar P ; Mora S., Mers J.F. Jones N.L. « Patient perspectives of medical confidentiality: a review of the literature », J Gen Intern Med 2003 Aug;18(8):659-69 ; Lambert K., Barry P., Stokes G, « Risk management and legal issues with the use of social media in the healthcare setting », J Healthc Risk Manag 2012;31(4):41-7.

quelque sorte, **ce n'est ici pas la « donnée de santé » qui aimante le secret : c'est le secret qui aimante la donnée,** avec l'effet de la qualifier comme telle.

b. Les données de santé relèvent-elles d'un ordre public « de protection » ?

Le secret médical est source d'abondants travaux, du fait de la diversification continue des dérogations légales strictement encadrées [252]. Il **ne peut pas être rapproché d'un concept d'ordre public de protection.** En effet, ce dernier **postule la possibilité de renoncer à des droits qui seraient disponibles,** lorsque son bénéficiaire estime pouvoir se passer de la protection de la loi, une fois connu l'événement et ses conséquences, désirables ou non.

Quand donc le droit au secret des données est-il ici constitué ; à quel point, ou dans quelles conditions, le patient peut-il y renoncer (car il ne saurait y renoncer *avant* sa constitution) ?

La constitution du droit au secret sur les données de santé au sens large [253] naît de la seule relation de soins. Cela inclut ses précurseurs (dialogue à visée préventive, mise en œuvre de tests ou de scores de dépistages, etc.), indépendamment de son aboutissement qui pourrait être une orientation diagnostique, une stratégie thérapeutique etc. Mais sans qu'il s'agisse de secret au sens médical, ce secret ne naît il pas dès la prise de rendez-vous ? En soi, la sollicitation d'une consultation auprès d'un professionnel de santé [254] est déjà l'expression d'un besoin (justifié ou non : cela **est en soi déjà une information sensible,** tout comme la trace de passage laissée par des internautes sur des sites dédiés aux questions de santé ?

En mai 2023, la CNIL a prononcé une forte condamnation contre une **plateforme de prise en ligne de rendez-vous médicaux**, laquelle par ailleurs « *propose des articles, tests, quiz et forums de discussion en lien avec la santé et le bien-être, à destination du grand public* ». Cette condamnation a été prononcée pour défaut de conformité, notamment pour ne pas avoir recueilli le consentement d'utilisateurs au recueil de données de santé, ni respecté la règle relative aux *cookies* en dépit de leur refus par les utilisateurs, etc [255].

---

[252] Commentaire du Code de déontologie des médecins (2022) préc. pages 29 et 30 ; également 44 à 54, avec l'annexe dédiées aux dérogations au secret professionnel.
[253] Nous verrons dans le titre II, la justification de l'inclusion dans le concept de donnée de santé, de ce qui relève du champ de secret au titre d'informations d'environnement.
[254] Et même, qui ne serait pas « professionnel de santé » au sens du livre IV CSP, nous l'avons vu.
[255] CNIL (communiqué, 17 mai 2023) Données de santé et utilisation des cookies : DOCTISSIMO sanctionné par une amende de 380 000 euros.

Si toute personne est certes libre de révéler à qui elle le souhaite, son propre état de santé ou des données relatives à sa santé, le patient ou toute personne même enquêteur (réquisition à témoignage en contexte judiciaire etc.) **ne peut délier le médecin de son obligation de secret à l'égard des données de santé, lesquelles ne s'y trouvent pas pour autant précisées,** puisqu'il s'agit en fait et en droit de toute information couverte par le secret [256].

Plusieurs décisions judiciaires et administratives sont explicites sur ce point : le patient ne peut affranchir le médecin du secret [257] ; le patient ne peut y renoncer que pour lui-même, **c'est-à-dire en dehors d'un contexte médical qui impliquerait un débiteur de l'obligation de secret** [258], ou hors d'un contexte de demande de prise en charge sociale. En outre, cette dernière n'implique en soi aucun acquiescement implicite à la levée du secret [259]. **Enfin, le patient ne peut y renoncer à titre onéreux** (*infra*).

Mais le réseau social ou forum sur lequel un patient s'épanche, les sites internet qu'il consulte en y laissant des traces, les requêtes qu'il active par des moteurs de recherche, etc., sont **autant de circonstances externes au système de soin, dans lequel il peut disséminer** des informations possédant une signification intrinsèque, ou par recoupement/inférence.
En 2020, la généralisation durant la pandémie de la télémédecine a d'ailleurs conduit à s'inquiéter quant à l'émergence d'une « zone grise » du secret médical : « *alors qu'elles ne sont pour beaucoup, techniquement, que de simples plateformes d'échanges en «* tchat video *», les* startups *de télémédecine lèvent des millions d'euros, souvent auprès de mutuelles, sans que cela n'interroge ni ne choque plus personne. Malgré des données médicales anonymisées,*

[256] L'environnement social, professionnel, des considérations non sanitaires etc. en sortent progressivement.
[257] Crim. 8 avr. 1998, n° 97-83.656 : « L'obligation au secret professionnel, établie par l'article 226-13 du Code pénal pour assurer la confiance nécessaire à l'exercice de certaines professions, s'impose aux médecins, hormis les cas où la loi en dispose autrement, comme un devoir de leur état ; sous cette seule réserve, elle est générale et absolue et il n'appartient à personne de les en affranchir, pas même au patient » ;
[258] CE 28 mai 1999, n° 189057, Rec. Lebon : « *La diffusion, dans un organe de presse qui procède à une enquête sur l'hypnose, de la photographie d'une patiente prise dans le cabinet du praticien,* ***même avec le consentement de l'intéressée, est de nature*** *à dévoiler l'identité de cette patiente qui est partie intégrante des informations couvertes par le secret médical; par suite, en regardant le comportement du praticien, qui a autorisé et organisé la réalisation de la photographie dans son cabinet, comme constitutif d'une violation du secret médical et comme un manquement à l'honneur professionnel privant le requérant du bénéfice de l'amnistie, la section disciplinaire du Conseil national de l'Ordre des médecins* ***n'a pas commis d'erreur de droit ni entaché sa décision d'une erreur de qualification juridique*** *des faits* ».
[259] Civ. 2ème, 13 nov. 2008, 07-13.153 : La simple sollicitation de prestations sociales ne saurait impliquer, à elle seule, ni l'accord du demandeur, ni son absence d'opposition à la levée du secret médical, lequel continue de s'imposer aux médecins conseils des caisses ainsi qu'au juge.

il semblerait que les investisseurs voient en ce big data *médical une mine d'or qui un jour où l'autre pourra être exploitée à profit* » [260].

Hors de ce contexte, le fait pour une personne d'exprimer son consentement à son « suivi » sur un site internet (paramétrages de sécurité), est un mode de sollicitation qui s'étend. Le patient n'a pas nécessairement conscience du risque lié à la diffusion potentielle de telles informations, **selon le droit national applicable**. Sur ce plan, nous avons vu le droit européen très protecteur, tout donnée personnelle étant assujettie au RGPD ; mais les données sont elles éligibles à une protection renforcée au titre de « données de santé » ?

En outre, il existe un cas emblématique d'attitude inversée.

2. Le cas du partage altruiste par le patient de ses données de santé

Nous avons vu que le CSP interdisait la vente de données de santé « *identifiantes directement ou indirectement,* ***y compris avec l'accord de la personne concernée*** » (article L. 1111-8 – VII) [261], ce mettant en exergue la question de ce qui est « indirectement identifiant ».

Or, ceci caractérise un **ordre public de direction** : selon le CSP, une telle vente constituerait en effet un « ***détournement de finalité*** », laquelle finalité ne peut être énoncée que par l'autorité compétente. Illégale, la pratique de cession de « données de santé » (mais quelle extension de la notion dans ce contexte pénal, du fait de l'étendue très vaste du « secret de santé » ?) est susceptible de sanction pénale (article 226-21 CP), de seul droit commun. Ce qui peut apparaître antinomique d'une protection renforcée des données « de santé » [262].

L'accord de la personne concernée est sans incidence sur la qualification pénale. Mais depuis 2018, le débat est croissant, quant à la pertinence d'une vente de leurs « données de

[260] Des médecins alertent sur la « zone grise » du secret médical en télémédecine, Rev. sc. gestion. 5 août 2020.
[261] Modifié par Ord. n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel.
[262] « *Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement,* ***de détourner ces informations de leur finalité*** *telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.* »

santé » par les patients, ou de leur intéressement à une telle vente [263]. Certains auteurs volontiers polémistes reprochent même à l'Etat une complaisance voire complicité à l'égard du « business » des données de santé et invitent « *à rétablir la souveraineté de nos données* », tout en dénonçant une « *logique ultralibérale* » … dans leur centralisation étatique [264].

Toute autre est la notion de « partage altruiste » par le patient de ses données de santé. Elle **n'est pas conceptualisée dans le Code.** On pourrait vouloir l'autoriser par interprétation *a contrario* de l'article L. 1111-8 CSP (hypothèse de cession **à titre non onéreux**) ; mais cela ne règle pas le problème **du contexte** de renonciation par le patient à ses données, *supra*. Cette hypothèse fait l'objet d'une réflexion portée en 2020 par la mission Bothorel [265], sans encore d'applications en droit français.

Or, l'hypothèse apparaît dans le Règlement (UE) 2022/868 sur la gouvernance des données [266], lequel en traite comme une **pratique facultative** (i.e. à la discrétion des Etats membres), mais devant, le cas échéant, relever d'un **régime obligatoire,** lequel est le cas échéant unifié par le chapitre IV « *altruisme en matière de données* ».

S'il ne traite pas spécifiquement des données de santé, lesquelles sont l'objet d'un droit sectoriel **proposé presque simultanément en 2022, mais non encore adopté,** *infra,* cela n'empêche pas qu'elles en soient un point de focale.

Ainsi, par « *altruisme en matière de données* », ce règlement portant droit commun entend « *le partage volontaire de données fondé sur le consentement donné par les personnes concernées* ***au traitement de données à caractère personnel les concernant*** *(…) sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données, pour des objectifs d'intérêt général prévus par le droit national****, le cas échéant, par exemple les soins de santé*** » (article 2, point 16). On esquissera l'approche dans la proposition de règlement européen de 2022 relatif aux données de santé quant à la compétence juridictionnelle (a), avant de relever une expérience américaine qui illustre une tension croissante en géopolitique repolarisée (b).

---

[263] G. Koenig, Génération Libre, Rapport « Mes data sont à moi » (24 janvier 2018) ; du même, Rapport « Aux data, citoyens ! » (12 sept. 2019) ; dans un sens convergeant, N. Benyahia « Cinq ans après le RGPD, quelles protections pour les données de santé ? », Espace expressions, Institut Montaigne (24 mai 2023).
[264] A. Boulard, D. Favier-Baron, S. Woillet, *Le business de nos données médicales – enquête sur un scandale d'Etat*, FYP editions (2021).
[265] Préc., spéc. p 181.
[266] Règlement (UE) 2022/868 du parlement européen et du conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données). Nous le retrouverons *infra* en Partie II.

a. L'appréhension européenne de l'altruisme : quelle protection juridictionnelle ?

Conceptualisé en droit européen [267], mais non en droit français, l' « *altruisme en matière de données* » ne signifie pas pour le patient se défaire de ses droits : son consentement ne peut en effet relever que d'une finalité précise, et d'une temporalité limitée. **En conséquence, il n'y a pas de perte de qualité de la « donnée de santé »** par renonciation irréversible à sa protection, donc à sa qualification (cette qualification ne sert, en effet, qu'à sa protection [268]).

Nous avons vu que, bien que portant un droit commun, le Règlement (UE) 2022/868 met en exergue, dans sa définition, l'exemple des *« soins de santé »* (article 2, point 16). Si les **données couvertes par le secret de santé sont ainsi potentiellement concernées**, le règlement n'en traite pas spécifiquement, mais traite de la réutilisation de données **détenues par les Etats ou organismes publics**.

Or, parmi ces données, figureront notamment les données de santé **produites [269] ou réunies [270] par des organismes public.** Cela est typiquement le cas en France avec le Système National des Données de Santé (SNDS) institué en 2016, et l'accès par la plateforme des données de santé, *infra.* C'est ce double critère de rattachement au SNDS, qui avait conduit le Conseil d'Etat a distinguer en 2017 les données « privées », des données « publiques », au seul sens ici de leur mode d'hébergement et de leurs règles d'accès centralisé.

Dans le contexte non spécifique du règlement sur la gouvernance des données, il est **loisible aux Etats d'élaborer des « *politiques nationales* *dans le domaine de l'altruisme en matière de données* »** : elles « *peuvent notamment aider les personnes concernées à mettre à disposition volontairement, à des fins d'altruisme en matière de données,* ***des données à caractère personnel les concernant détenues par des organismes du secteur public****, et déterminer les informations nécessaires qui doivent être fournies aux personnes concernées en ce qui concerne la réutilisation de leurs données dans l'intérêt général* » (article 16).

Si ces politiques nationales sont facultatives, leur cadre est obligatoirement unifié, non sans une certaine autonomie étatique : institution de registre des organisations altruistes en

[267] Voir à titre préparatoire, « Avis du CEPD sur la stratégie européenne pour les données – Avis 3/2020 », spéc. 5§3 titré «Altruisme en matière de données» (pts 68 et 69).
[268] Mais le partage avec une personne ou organisation identifiée, ne signifie pas pour autant partage « universel » ; la qualification demeurerait donc, à l'égard de tout tiers au contrat de cession à titre gratuit.
[269] Dans le cas de soins reçus en établissements publics.
[270] Dans le cas de soins remboursés par l'assureur obligatoire.

matière de données reconnues (article 17) ; de conditions générales pour leur enregistrement (article 18), de transparence quant à la réutilisation sur ce fondement (article 20, spéc. §2b) etc. – et surtout, pour ce qui nous concerne ici, des « *exigences spécifiques* ***visant à préserver les droits et intérêts des personnes concernées*** *(…) quant à leurs données* » (article 21).

Ainsi, l'organisation altruiste doit informer les personnes concernées **préalablement à tout traitement de leurs données** (article 21§1) ; elles doivent pouvoir retirer facilement leur consentement (article 21§3). Si cette information porte sur les objectifs d'intérêt général, lesquels devraient s'exprimer en termes de « *finalité déterminée, explicite et légitime* » (article 21§1a), l'information doit aussi porter **sur la localisation géographique du traitement**. La question est explicitement soulevée **si le traitement est opéré dans un Etat tiers,** dans la seule mesure, en principe, des objectifs d'intérêt général consentis (article 21§1b).

Mais sous quelle compétence juridictionnelle ? on notera que « *Lorsque l'organisation altruiste en matière de données reconnue facilite le traitement de données par des tiers, y compris en fournissant des outils permettant d'obtenir le consentement de personnes concernées (...), elle précise, le cas échéant****, la juridiction du pays tiers où l'utilisation des données est prévue*** » (article 21§6). L'article 21§6 nous semble applicable quel que soit le pays (en comme hors UE) où le traitement pourrait être opéré.

Or, ce point est frappant : il suggère que la protection des droits des personnes ressortissants européens ayant consenti de façon altruiste à la réutilisation de leurs données personnelles pour une finalité explicite, peut ne pas bénéficier d'une **compétence *juridictionnelle* européenne ; n'eût-elle pu être le corollaire de la compétence *normative* européenne ?** La compétence de l'Etat siège du tiers utilisateur se conçoit (juridiction du siège du défendeur) [271], mais le droit international privé autorise les clauses attributives de juridiction.

N'était-ce pas là un apport potentiel du chapitre IV du règlement (pourquoi pas la juridiction de résidence de la personne « altruiste » ?), tant il apparaît peu envisageable (complexité, coûts) qu'un particulier ayant consenti à cette réutilisation pour un but altruiste, cherche à faire valoir ses droits devant la juridiction d'un pays tiers à l'UE [272], dans

[271] Règlement (UE) n° 1215/2012 du Parlement européen et du Conseil du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (refonte).
[272] Si dans l'UE, une clause attributive de juridiction rédigée en langue anglaise au profit d'une juridiction allemande et opposée à une personne physique non commerçante domiciliée en France est valable (Civ. 1ère 23 janv. 2008, n°06-21.898), hors UE, la Cour d'appel de Paris a écarté la clause attributive de juridiction qui donnait compétence au juge californien dans un litige opposant Facebook à un de ses utilisateurs, CA *Paris, 12 février 2016, n° 15/08624.*

l'hypothèse où cet Etat pourrait s'avérer (ou être simplement suspecté) ignorer ces droits ?

Quoiqu'il en soit, **cette approche contraste fortement avec l'approche américaine**, qu'explique sans doute la faiblesse du droit fédéral sur ce point, et le durcissement géopolitique sino-américain.

b. l'appréhension américaine : l'enjeu de souveraineté sur les « données de santé »

En droit américain, le contexte est très différent, du fait que le statut des données de santé fait l'objet d'une définition spécifique [273], et que la vente de données de santé n'y est pas interdite.

Le **Health Insurance Portability and Accountability Act** (**« HIPAA »**) a été adopté en 1996 par le Congrès des Etats Unis, puis modifié en 2009 par le **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** [274]. Son but essentiel est garantir leur confidentialité, non sans permettre à des entités spécialement définies (« *Covered entities* ») d'adopter des technologies notamment numériques, pour améliorer les soins [275].

* Ainsi, l'HIPAA couvre les données de santé dites **« *Protected Health Information* » (PHI)**, **volet à protection spécialement renforcée** des **« *Personally Identifiable Information* » (PII) protégées depuis 1974 par le Privacy Act** [276]**. Encore ces notions fédérales connaissent-elles parfois des déclinaisons particulières dans le droit des Etats fédérés** [277]**.** Dans ce contexte hautement fragmenté (il existe de multiples réglementations sectorielles selon les types de données, et des conceptions variées entre les Etats fédérés), les Etats-Unis s'interrogent sur une réforme pouvant se rapprocher d'une approche unifiée type RGDP à l'européenne [278].

L'HIPAA s'applique essentiellement aux **fournisseurs et assureurs des soins, centres d'information sur les soins, et par extension à leurs partenaires et sous-traitants** qualifiés

[273] Voir site du US Department of Health and Human services : https://www.hhs.gov/programs/hipaa/index.html
[274] Ibid. : https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
[275] Voir le livre blanc prospectif de M-M. Goldstein, A-L. Rein, « Consumer consent options for electronic health information exchange: policy considerations and analysis » 23 mars 2010, https://www.healthit.gov/sites/default/files/choicemodelfinal032610.pdf
[276] Pour une mise en contexte du Privacy Act en 2020, OPCL, US department of justice « « Overview of The Privacy Act of 1974 (2020 Edition) », https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition
[277] Pour un site de droit comparé, https://www.dlapiperdataprotection.com/index.html?t=definitions&c=US
[278] Council of Foreign relations, « Reforming the U.S. Approach to Data Protection and Privacy (Digital and cyberspace Policy Program) », 30 janv. 2018. https://www.cfr.org/report/reforming-us-approach-data-protection

« *Business Associates* » (ainsi, en cascade, qu'aux sous-traitants de ces sous-traitants, etc.) [279]. Notons seulement ici que les « *covered entities* » ne sont autorisées à divulguer les PHI à leurs « *business associates* » qu'à la condition que ces derniers ne les utilisent qu'aux fins contractées, les protègent contre tout détournement, et aident les « *covered entities* » à respecter leurs obligations au regard du HIPAA, déclarent les cas de violation, etc. [280].

Si les données personnelles doivent être ainsi protégées, cela n'exclut pas une activité très lucrative de **vente de données de santé (non interdite aux Etats-Unis) une fois anonymisées [281].** Telle est l'activité des « *Data Brokers* ».
Certes, ces derniers sont censés expurger les PHI des données identifiantes ; mais parfois il les associent à un numéro (quasi pseudonymisation, donc) permettant de réunir *ex post* des informations qui auront été dispersées, accroissant ainsi leur valeur par recoupement potentiel [282]. Cette activité est florissante et compétitive : il existe des entreprises commerciales **spécialisées dans la comparaison qualitative des fournisseurs de données de santé,** à l'échelle non seulement nationale (fédérale américaine), mais internationale [283].

Ces données sont en effet très convoitées par les laboratoires, (développement de médicaments, dispositifs médicaux), les entreprises opérant en santé (évaluation et développement de modèles de prise en charge), les actuaires (ajustement de produits d'assurance sur un marché compétitif), mais aussi récupérées par des opérateurs du numérique pour le développement de leurs offres en intelligence artificielle, etc. [284].

En conséquence, la tentation est grande pour certains, de **vendre les données en dehors du cadre légal qui l'autorise**. En 2018, une étude aux Etats-Unis par le cabinet Accenture a rapporté que 18% des employés sondés, appartenant à des organisations de prestation ou de liquidation de paiement de soins, seraient **disposés à vendre des données de santé confidentielles à des parties non autorisées** [285]. En 2020, une alternative est explorée,

---

[279] Fournisseurs de fichiers médicaux électroniques, d'infrastructures informatique en nuage (« cloud »), développeurs d'applications pour terminaux mobiles, consultants et fournisseurs de services informatiques en mode SaaS (« Software As A Service »).
[280] Sur les obligations résultant de ces statuts, voir la présentation didactique https://www.transatlantic-lawyer.com/fr/hipaa-les-startups-francaises-sont-aussi-concernees/
[281] Sur la notion d'anonymisation, et la relativité croissante de son irréversibilité postulée, *infra*.
[282] https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/
[283] https://datarade.ai/data-categories/healthcare-data/providers
[284] T. Feathers, S. Fondrite-Teitler, A. Waller, S. Mattu, « Facebook Is Receiving Sensitive Medical Information from Hospital Websites, Pixel Hunt, 16 juin 2022.
[285] Accenture, « Losing the Cyber Culture War in Healthcare: Accenture 2018 Healthcare Workforce Survey on Cybersecurity », https://www.slideshare.net/secret/2bnzxgIzzSTxD4 (contrôlé nov. 2022).

consistant en le traitement *in situ* des données de santé, sans transfert numérique [286].

* Des modèles de partage altruiste existent aussi aux Etats-Unis, en dehors d'une dialectique commerciale ; ce n'est d'ailleurs pas sans soulever de questions depuis des années, quand le partage au sein de communauté de patients **les conduit à avoir accès aux données les uns des autres** [287]. C'est le cas d'organisation de type « *Patients Like Me* », qui certes vise l'information réciproque, mais est d'abord un réseau en ligne d'information, de soutien solidaire personnalisé, et de recrutement de patients en vue d'essais [288]. Comptant plus de 850.000 membres, il œuvre aussi avec la FDA, l'agence fédérale des médicaments [289].

Or, en 2017, une société chinoise de données de santé et de génomique, iCarbonX, fortement capitalisée par le conglomérat Tencent, en est devenu actionnaire majoritaire, par apport de 100 millions de dollars. De la récupération des base de données de population américaine mises à disposition par les patients, résultait **un gain significatif pour le développement d'intelligence artificielle en Chine, prétendant à l'amélioration des soins** [290].

En 2019 sous l'administration Trump, le Comité sur les investissements étrangers aux Etats Unis (*Comittee on Foreign Investment in the United States, CFIUS*) **a préconisé, et a forcé le départ du capital** d'iCarbonX. « *A spokesperson for the Treasury Department declined to comment, writing in a statement that "information filed with CFIUS may not be disclosed by CFIUS to the public." A representative from iCarbonX also declined to comment* » [291].

Le consentement au **partage altruiste des données de santé ne peut donc avoir qu'une portée relative**, car d'une part, les personnes concernées conservent la protection de leurs données (selon leur volonté) ; d'autre part, l'Etat peut s'opposer au transfert de données renseignant sur les caractéristiques (entre autres génétiques) de sa population, quand bien même les données de santé ne seraient plus « personnelles », et ne relèveraient donc plus du secret « de santé ». **L'enjeu devient de souveraineté.**

---

[286] O. Beyan, A. Choudhury, J van Soest et al. « Distributed Analytics on Sensitive Medical Data: The Personal Health Train ». *Data Intelligence* 2020; 2 (1-2): 96–107.
[287] J-H Frost, M-P. Massagli, « Social Uses of Personal Health Information Within PatientsLikeMe, an Online Patient Community: What Can Happen When Patients Have Access to One Another's Data », J Med Internet Res. 2008 Jul-Sep; 10(3): e15. Doi: 12.2196/jmir.1053.
[288] https://www.patientslikeme.com/
[289] J. Comstock, « PatientsLikeMe, FDA explore how patient-generated data could help event reporting », HIMSS 23 août 2018, https://www.mobihealthnews.com/content/patientslikeme-fda-explore-how-patient-generated-data-could-help-event-reporting
[290] H. Mack, « PatientsLikeMe secures $100M, partners with health data company iCarbonX », HIMSS 5 janv. 2017.
[291] C. Farr, A. Levy, « The Trump administration is forcing this health start-up that took Chinese money into a fire sale », CNBC News, 4 avril 2019.

§2. LE CHAMP EXPLICITE DE PROTECTION DES DONNEES DEFINI PAR LE « SECRET DE SANTE » ?

Revenons au contexte français, dans la tentative de cerner toujours la notion aux contours encore fuyants. Nous avons vu comment **un champ de « données de santé » avait d'abord été inféré des obligations** des membres des « Professions de santé » (relevant de la IVe partie du CSP, ou du CASF notamment [292]), parfois d'autres professionnels ; et pourquoi ces derniers ne devaient pas en être véritablement distingués, quant aux « données de santé ».

La loi du 4 mars 2002 a donné à cette question une résonnance nouvelle. En effet, son point de focale **n'est plus tant les obligations des professionnels, que les droits des patients** (A). En outre, les débiteurs de l'obligation à son égard (et corrélativement, le champ des « données de santé » produites dans les missions d'accompagnement des soins) se sont élargis (B).

A. « DONNEE DE SANTE » : INFERENCE PAR L'INTRODUCTION D'UN DROIT DU PATIENT ?

La loi du 4 mars 2002 est une loi fondamentale dédiée aux « *droits des malades et à la qualité du système de santé* » [293]. Ce qui nous intéresse ici, est qu'elle institue un principe général de protection des données, lequel défragmente les obligations des « Professions de santé » en la matière (1). Puis nous relèverons la façon dont l'article L. 1110-4 **donne, pour la première fois, une définition directe (et non plus par inférence), du champ du secret,** sans pour autant définir les « données de santé » qu'il recouvre, autrement qu'implicitement (2).

1. Défragmentation du champ de l'information par la loi du 4 mars 2002

Cette loi est composée de plusieurs titres, dont seul le titre II « Démocratie sanitaire » nous intéresse : il est divisé en deux chapitres, le chapitre I (articles 3 à 10) est relatif aux « droits de la personne », le II (articles 11 à 19) relatif aux « droits et responsabilités des usagers ». Ce faisant, la loi objective des droits fondamentaux, dont la particularité innovante en 2002 est d'être **indifférents aux motifs et circonstances de recours au système de santé par la personne (malade ou non) mais** à la condition qu'elle fasse recours **« au système de santé »**.

[292] On peut y adjoindre les activités de praticien conseil et de contrôle médical définis dans le CSS, etc.
[293] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé.

a. L'unification des droits protégeant la personne en tant qu'« usager » du « système de santé »

Par « usager » au sens du Chapitre II, **le législateur n'a pas entendu désigner la seule situation d'une personne qui recourt au service public (**sens classique en droit administratif [294]). Par ce terme, d'acception donc élargie par le législateur en santé, la loi désigne **toute personne qui a recours au système de santé, en toutes ses composantes** fonctionnelles, quel que soit leur statut (publique, social, libéral), pour quelque motif que ce soit (patient, ou sujet *a priori* bien portant, pour des actions de prévention etc).

L'ensemble de ces droits et responsabilités s'applique par essence au système de santé tel qu'il est **institué, organisé et régulé par le Code de la santé publique**. L'enjeu est donc ici la qualification des périmètres d'action, dont va résulter la qualification des données. L'offre de « santé » qui ne serait pas une production organique du « système de santé » institué par le CSP, **échappe-t-elle par définition au champ de la loi de 2002 ?**

Cela n'est pas non plus une pirouette dialectique : nous avons vu la différence entre les « Professions de santé » au sens du CSP, et les professionnels de santé qui n'en relèvent pas [295], bien que leurs activités ou prétentions s'inscrivent dans l'approche holiste, portée par l'OMS, de la « santé ». Est-ce là dire que leurs offres en marge du système, qui prétendent offrir des prestations hors des catégories du CSP, sans pour autant les violer ces catégories [296], **ne seraient pas incluses dans ce champ, et ne produiraient pas de « données de santé »** (la question de leur assujettissement au secret professionnel est distincte) ?

Nous avons vu que des « non-Professions de santé » au sens du CSP, pouvaient être sollicitées par des Professions et établissements au sens du CSP, dont dérivait le fait que, sinon par « état », ils étaient tenu au secret par leur « mission » ou « fonction », celle-ci fût-elle ponctuelle.

Or, la situation existe et même se développe, avec l'introduction par exemple en milieu hospitalier public à titre de médecines « complémentaires », de la sophrologie, de l'hypnose, de l'acupuncture, du toucher relationnel [297]. Mais dans ce cas, les professionnels sont, pour

---

[294] Un « usager du service public » est légalement en situation statutaire, ce que n'est pas le patient en secteur ambulatoire privé libéral ou social, où sa situation est contractuelle.

[295] M.-L. Moquet-Anger, Professions et professionnels de santé, RDSS 2022 préc.

[296] Ce qui serait passible de sanction pénale sur chef d'exercice illégal de la médecine, de la pharmacie, de la biologie, des actes infirmiers, etc.

[297] Dans le silence de la loi, la question est affaire de doctrine d'établissement. L'AP-HP par exemple, a adopté 17 recommandations en la matière, dont que « *n°1 - La pratique des médecines complémentaires à l'AP-HP est réservée aux professionnels de santé* », et « *n° 3 - Les professionnels de santé exerçant les médecines complémentaires doivent être titulaires d'un diplôme devant faire l'objet d'une procédure d'agrément interne*

cette « *fonction* » ou « *mission* », attraits dans le champ du CSP, sans pour autant participer du système de santé au sens organique défini par la loi, *infra*.
En contraste, **il est des cas où les actions ne sont pas combinées** (c'est-à-dire ne sont pas réalisées en équipe de soins ; sur sollicitation en secteur hospitalier ou libéral, au titre d'appui ou d'accompagnement) ; elles ne sont donc pas attirées dans le champ du CSP.

De façon emblématique de la confusion, mais sans pour autant violation de la loi, on a vu en 2022 un site internet marchand (*Doctossimo*) **associer sur un pied d'égalité les pratiques « conventionnelles »** (seules définies dans le CSP)**, « complémentaires »** (acceptées autour du CSP) **voire « alternatives »** (non acceptées au regard du CSP), organiser le référencement centralisé de tous ces professionnels, et faciliter la prise des rendez-vous sur une même plate-forme.
Ce point suscitant l'ire des professionnels de santé (CSP) a été dénoncé par eux, et cette pratique arrêtée [298] : elle avait l'effet d'induire une confusion quant à la nature des qualifications et des responsabilités, et d'accréditer en quelque sorte, des activités « alternatives », non sans risques pour la santé.

b. Portée des droits protégeant la personne (et qualification des données afférentes) ?

La philosophie de la loi de 2002 étant de protéger la personne, les droits qu'elle institue **sont, sur le point qui nous intéresse, indifférents à sa position** (patient ou pas, français ou non, assuré ou non assuré, situation régulière ou irrégulière), **comme à l'égard du statut des opérateurs** (Professions du CSP ou non ; en équipe de soins, en mission/ fonction, ou pas).

Du fait de leur nature, ces droits fondamentaux pourraient-il être considérés indifféremment **quant à leur contexte national d'invocation ?**

En cas de soins extraterritoriaux, la saisine d'une juridiction non française dans l'Union, ou hors Union européenne, pourrait selon le droit national applicable changer la donne ; cela pourrait susciter un intéressant débat quant au **rattachement de l'essence de ces droits à la CEDH**, dont le contenu serait alors à préciser, *infra*. A notre connaissance, il n'existe pas de contentieux sur ce point.

---

par un comité hospitalo-universitaire » in « L'AP-HP et les médecines complémentaires à l'hôpital : un engagement hospitalo-universitaire » (11 juin 2012), voir le site de l'AP-HP.
[298] R. Porcher, « Grand ménage de printemps chez Doctolib », Rev. dr. santé janv. 2023 (111), 10-11.

De façon incidente, on relèvera que si les professionnels qui ne relèvent pas du CSP, ne sont pas inclus dans des équipes de soins définies par le CSP, ni impliqués au titre d'une « fonction » ou « mission » individuelle qui leur serait assignée dans le cadre du CSP, **ils ne sont** pas liés par l'article L. 1111-3 CSP. En matière d'information sur les prix des prestations et garanties associées, cela implique d'ailleurs le renvoi au droit de la consommation quant à la protection du « citoyen-consommateur » (non du « patient-usager »).

Pas plus, ces professionnels non définis par le CSP ne sont en effet liés par le secret des informations mis en exergue par l'article L. 1110-4 CSP. Mais il nous semble difficile de soutenir que **leur extériorité au cadre organique régulé par le CSP, prive les données qu'ils traitent de la qualification de « données de santé »,** et cela, quelle que soit la façon dont ils les traitent.

Selon nous, la qualification de donnée de santé est à la fois subjective (s'il s'agit de données personnelles), et objective : **qu'importent l'opérateur et le cadre d'opérations dans lequel ces données sont produites**. Nous retrouverons les causes et conséquences de ce point *infra*.

2. Dynamique de l'article L. 1110-4 CSP quant au champ du secret de l'information

Le Code de déontologie des médecins contient l'énoncé le plus large du champ du devoir de secret. Mais il est l'héritier direct du serment d'Hippocrate, et de la période durant laquelle les riches étaient soignés à domicile, les pauvres à l'hospice. Cela conduit naturellement à ce que **la nature et l'ampleur des interactions par accès à l'intimité n'étaient pas les mêmes**. On voit ici la conception unifiée des devoirs professionnels, puis de leur champ d'application.

a. une conception unifiée des devoirs à l'égard du secret de l'information

Nous avons précédemment souligné que pour la première fois en 2002, le législateur défragmentait les obligations de secret quant aux données de santé et par extension toute autre information acquise de façon incidente (même non-santé). Le patient, ses ayants-droit ou avocats, **n'ont plus à consulter les régimes respectifs d'exercice des professions de santé impliquées dans le soin, pour déterminer ses droits en tant que personne**. Les énoncés légaux, déontologiques et réglementaires restent naturellement différenciés ; mais ils sont désormais essentiellement l'énoncé d'obligations à la charge des professionnels.

Ainsi, la loi de 2002 présente en miroir de ces devoirs du point de vue des professionnels, une **conception unifiée, et autrement intelligible, des droits du point de vue du patient**. Nous citerons ici l'article complet L. 1110-4 CSP en ses alinéas 1 et 2, qui posent les notions et principes de méthode nous intéressant seuls ici (tous aussi fondamentaux ; mais les autres alinéas soulèvent des questions de régime, étrangères à l'objet de notre étude).

b. une conception unifiée du champ des devoirs en matière de secret de l'information

L'alinéa 1 dispose que toute personne (indifféremment donc quant à son statut, etc.) « *prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit* ***au respect de sa vie privée et du secret des informations la concernant*** ». Le secret des informations est autonomisé à l'égard du respect de la vie privée, sachant les deux consubstantiels.

Ce qui nous intéresse ici est dans l'alinéa 2 d'origine, **la définition du champ du secret, qui est nouvelle du fait de son approche unifiée** : « *Excepté dans les cas de dérogation, expressément prévus par la loi, ce secret* ***couvre l'ensemble des informations concernant la personne venues à la connaissance*** *du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé* ».

Ce secret est donc vaste : il ne se limite pas aux « données de santé », puisque est couvert « *l'ensemble des données venues à la connaissance* », **quels que soient donc la nature des données, et le mode de connaissance.** Mais nous verrons que depuis 2022, des données d'environnement (socio-éducatif, alimentation, habitat) sont spécialement prises en compte au titre des déterminants de santé, et peuvent rejoindre le champ des « données » ainsi élargi.

Naturellement, il sera intéressant de balancer ces obligations professionnelles particulières unifiées par le principe général par l'article L. 1110-4 CSP, **avec l'ère de la production massive de données par les personnes elles–mêmes**.

B. ELARGISSEMENT DES DEBITEURS DE L'OBLIGATION DE SECRET SUR LES DONNEES DE SANTE

En instituant un principe général de secret comme droit fondamental du patient (L. 1110-4 CSP), le législateur en 2002 a également du traiter, de façon simultanée, des hypothèses de prise en charge **qui transcendaient nécessairement les catégories d'acteurs** définis par le CSP, et leurs obligations individuelles de secret.

Le besoin du partage du secret est ancien ; il a été constaté par des jurisprudences, avant d'être consacré par la loi. Mais la dynamique inhérente aux évolutions technologiques et fonctionnelles dans la production des soins a abouti à une diversification dans l'organisation des soins, parfois à une **multiplication des points de collectes et modes de dissémination de l'information**. Ce point a spécifiquement fait l'objet, dans une autre optique (celle de l'information médicale), de récentes réflexions sous l'égide du Conseil d'Etat [299].

1. Paramétrage des droits : de l'échange au partage des données de santé

Comme souligné par Madame Fombeur, le secret institué dans l'intérêt du patient, ne devait pas se « *retourner contre lui* ». Surtout, du fait de l'évolution des modes de production des soins, la dialectique est rapidement passée **de l'échange des données** (dimension ponctuelle, vers destinataires personnellement identifiés), **au partage de données** (dimension permanente, vers tous destinataires habilités), sachant que cette distinction a été le fait en 2016 d'un simple arrêté [300]. Nous en présentons et nuançons rapidement ici la dynamique.

a. L'échange de données « de santé » : vers des destinataires identifiés

Dès le premier Code de déontologie médicale (1947), il est prévu que sauf opposition du patient, des données de santé pertinentes pour la prise en charge soient échangées, ou au moins rapportées, en cas de consultations concomitantes (généralistes/spécialises) ou successives (substitution de professionnels en cas d'indisponibilité) [301].

La jurisprudence a également statué sur les hypothèses de prise en charge non **par des personnels dispersés** – cas alors dominant en secteur ambulatoire, mais **par des personnels**

[299] P. Fombeur, Le secret médical partagé, in Actes du Colloque du Conseil d'Etat 2017, préc., 107-110
[300] Arrêté du 25 nov. 2016 fixant le cahier des charges de définition de l'équipe de soins visées à l'article L. 1110-12, 3° CSP. Ce texte était imposé par la loi, mais c'est lui qui a procédé à la distinction.
[301] Articles 43 et 57 du Code de déontologie de 1947, créé par le décret n°47-1169 du 27 juin 1947.

regroupés – cas dominant à l'hôpital [302] ou en centres de santé mutualistes [303] : dans ce cas, il a été jugé que, c'est « ***nécessairement à l'ensemble du personnel médical*** *de cet organisme que, sauf prescription particulière de la part de ce malade, le secret médical est confié* » [304].

La loi du 4 mars 2002 préc. consacre ces jurisprudences **en la forme unifiée de « droits des personnes »**. Dans la première hypothèse, l'article L. 1110-4 dispose que deux ou plusieurs professionnels peuvent, sous réserve de la volonté du patient, « ***échanger des informations*** *(...) afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge possible* ». Dans la seconde hypothèse, a contrario de prise en charge dans un établissement de santé par une équipe de soins (**unité de lieu et de temps**), « *les informations (...) sont réputées confiée par le malade à l'ensemble de l'équipe* ».

Dans les deux cas, on note que tous ces professionnels **ne sont pas nécessairement des médecins.** Cela ne pose plus de problèmes, dès lors que leur statut les rattache aux Professions consacrées dans le CSP, et au secret correspondant ; ou que leur mission ou fonction les soumet à l'obligation unifiée d'un secret pénalement sanctionné, *infra*.

Mais force est depuis de constater **l'accélération de nouveaux modes de prise en charge des soins** (concepts, et technologies – dont l'apport du numérique).

Les soins marqués par une spécialisation et technicisation croissantes, sont parfois fragmentés et dispersés dans le temps et l'espace (selon les qualifications, infrastructures, technologie). La recherche de qualité, fluidité, d'efficience des soins, comme de confort du patient, conduit au **développement de réseaux de prise en charge multi-opérateurs et d'autres organisations** pluridisciplinaires, qu'il n'est pas lieu de détailler ici.

b. **Le partage de données « de santé » : avec des destinataires habilités**

Au-delà de l'échange ponctuel d'informations, la loi du 4 mars 2002 a intégré l'hypothèse plus large du partage des données. Celui-ci suggère une dimension permanente, laquelle n'exclut pas la graduation des droits d'accès. La **dynamique est la même hors du champ de la santé** (i.e. des activités couvertes par le CSP).

---

[302] Civ. 1ère, 12 févr. 1963, pourvoi n° 98 ; 26 mai 1964, pourvoi n° 276.
[303] CE 11 févr. 1972, Sieur Crochette, n° 76799, rec. P. 138.
[304] CE 11 févr. 1972, préc.

Ainsi en 2004, le « dossier médical personnel » (champ aussi du CSS) est institué [305] ; en de même en 2007, le partage de l'information en équipe pluridisciplinaires vouées à la protection de l'enfance (champ du CASF) [306] , et en 2009 les nouvelles coopérations dans le champ de la santé [307]. **A défaut de textes dédiés (CSP, CSS, CSAF), le droit commun de la LIL de 1978 s'applique** : ce fût le cas jusqu'en 2016 dans le secteur médico-social [308].

En effet, en 2016, la loi a permis le décloisonnement des activités aux profit d'une meilleure coordination des professionnels en charge des personnes (prise en charge médicale, médico-sociale, sociale). A cette fin, elle a modifié l'article L. 1110-4 CSP en introduisant un nouveau cadre, et de nouveaux outils de communication fluidifiée, dont la dynamique des motifs et de la mise en œuvre technique a fait l'objet de travaux auquel le lecteur voudra bien se référer [309]. Cette loi a également **substantiellement élargi les acteurs professionnels « *susceptibles d'échanger ou de partager* »** des informations (Professions de santé de la IVème partie du Code, et autres professionnels, qu'ils soient ou non « de santé ») [310].

De façon emblématique, le « dossier médical personnel » [311], est alors devenu le « dossier médical partagé » (L. 1110-14 CSP), et devenu depuis janvier 2022 accessible aux patients au titre su service « **Mon espace santé** » : cet espace de stockage sécurisé de ses données de santé, lui permet de partager des documents avec les professionnels de son choix.

Les avatars de l'acronyme DMP conduisent à ce qu'il soit encore actuellement (janvier 2023) utilisé pour plusieurs significations, selon l'optique des organismes le citant dans leur doctrine : sur les sites de la CNIL (dossier médical **Personnel**) [312], de l'assurance maladie (dossier médical **Partagé**) [313], de la Haute Autorité de Santé (dossier médical du **Patient**) [314].

---

[305] Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie.
[306] Loi n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance.
[307] Loi n°2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.
[308] Voir l'analyse de Mme Fombeur, préc., p. 111.
[309] S. Dodeh, « Du dossier médical personnel au dossier partagé - Vers un dispositif de médiation documentaire », les Cahiers du numérique 2016 1/2 pp 31-50.
[310] Tel est l'apport de son décret d'application, devenu R. 1110-2 CSP.
[311] Institué en 2004, son essor a été rapidement enrayé par le fait que l'autorisation de sa consultation par des praticiens déterminerait, selon la loi, le niveau de prise en charge des soins par l'assurance maladie.
[312] https://www.cnil.fr/fr/cnil-direct/question/dmp-dossier-medical-personnel-et-dossier-medical-quelle-difference
[313] https://www.ameli.fr/medecin/sante-prevention/dossier-medical-partage
[314] https://www.has-sante.fr/jcms/c_438115/fr/dossier-du-patient

2. La caractérisation du besoin d'en connaître : le critère de la « stricte nécessité »

Que l'optique soit d'« échange » (transmission à des destinataires identifiés), ou de « partage » (accessibilité à des personnes habilitées), **se pose la question des données éligibles**, sachant en tout état de cause que les personnes habilitées ne sont que « *susceptibles d'échanger ou de partager des informations relatives à la même personne* » [315]. Ces actions restent subordonnées à son consentement, même en établissement de santé où ce consentement pourrait, en théorie, être sélectif, selon les membres impliqués des équipes.

a. l'édiction jurisprudentielle du critère de la stricte nécessité

La question a été posée de façon positive dans le contexte particulier de la santé en milieu carcéral, lequel **relève pour partie d'un droit autonome** (on le reverra en droit européen : pour le traitement des données de santé dans ce milieu spécifique, ce n'est pas le RGDP qui s'applique, mais une directive dédiée, adoptée le même jour, *infra*).

En l'occurrence, une circulaire interministérielle adoptée en 2012 entendait établir un cadre de « *partage d'informations opérationnelles entre professionnels de santé et ceux de l'administration pénitentiaire et de la protection judiciaire de la jeunesse* » [316]. Elle a fait l'objet d'un recours pour excès de pouvoir : occasion pour le juge administratif de contrôler **la nécessité pour l'administration pénitentiaire, de disposer de certaines informations intéressant la santé** des détenus [317], sachant cette administration devoir respecter le droit au secret médical des personnes détenues, ainsi que le secret de la consultation [318].

En premier lieu, ce jugement s'intéresse à la nature des actes pouvant être accomplis par les professionnels de santé en milieu carcéral, pour relever que par cette circulaire attaquée, « *le pouvoir réglementaire n'a pas prévu que pourrait être demandé aux médecins et aux*

[315] *Supra*, et pour rappel, R. 1110-2 CSP, qui liste les catégories « susceptibles de » : au titre du CSP, la catégorie des Professions de santé (1°), au titre de ce texte d'application de la loi de 2016, la catégorie non Professions de santé (2°) et ses sous-catégories préc.

[316] Circulaire interministérielle N°DGS/MC1/DGOS/R4/DAP/DPJJ/2012/94 du 21 juin 2012 relative aux recommandations nationales concernant la participation des professionnels de santé exerçant en milieu carcéral à la commission pluridisciplinaire unique (CPU)prévue par l'article D90 du code de procédure pénale ou à la réunion de l'équipe pluridisciplinaire prévue par l'article D514 du même code et au partage d'informations opérationnelles entre professionnels de santé et ceux de l'administration pénitentiaire et de la protection judiciaire de la jeunesse.

[317] CE 22 oct. 2014, Section française de l'observatoire international des prisons, n°362681 (inédit Rec. Lebon).

[318] Article 45 de la loi du 24 novembre 2009 pénitentiaire : " L'administration pénitentiaire respecte le droit au secret médical des personnes détenues ainsi que le secret de la consultation, dans le respect des troisième et quatrième alinéas de l'article L. 6141-5 du code de la santé publique "

personnels soignants intervenant en milieu carcéral ***un acte dénué de lien avec les soins ou avec la préservation de la santé des personnes détenues ou une expertise médicale*** *».*

En second lieu, les considérants 6, 7, 8 et 9 consistent en l'analyse approfondie **de la finalité et proportionnalité des partages de données** : protection effective de l'intégrité physique ; problème psychiatrique ou somatique ; risque suicidaire etc. Pour conclure, *in fine*, en l'absence d'illégalité de la circulaire administrative.

A titre anecdotique, la même question de la nécessité d'accès, cette fois évidente, a conduit à une correction en janvier 2017, de la loi de 2016 : suite à une erreur matérielle de rédaction, les établissements de santé, laboratoires de biologie médicale, hôpitaux des armées avaient été exclus du partage/échange de secret médical ! **La nécessité étant ici caractérisée d'office**, ces établissements ont été réincorporés dans l'article L. 1110-4 CSP (Art 5-1°).

Signalons, sur un terrain conceptuel certes autre mais significatif, que, par la même ordonnance de 2017, dans l'article L. 1115-1 CSP, les mots : « *auprès de professionnels ou d'établissements de santé* » sont remplacés par : « *auprès de personnes physiques ou morales* ***à l'origine de la production ou du recueil de ces données*** » (Art. 5-2°) [319].

Cela n'élargit-il pas le champ des « producteurs » au-delà des catégories légales du CSP ?

b. la consécration législative du critère de la stricte nécessité

Ce critère est consacré par la loi, avec quelques nuances qui nous semblent relever de l'erreur matérielle, plus que d'une intention de différencier des contextes de mise en œuvre.

i. en matière civile

Dans l'article L. 1110-4 CSP en vigueur, figurent 3 occurrences du critère « **strictement nécessaire** ». On y retrouve la distinction de l'échange (L. 1110-4 II) et du partage (L. 1110-4 III). Dans les deux cas la condition est, dans des termes quasi identiques, que ces « *informations* ***soient strictement nécessaires*** *à la coordination ou à la continuité des soins, à*

[319] Article 5, Ord. n° 2017-31 du 12 janvier 2017 de mise en cohérence des textes au regard des dispositions de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

la prévention ou à son suivi médico-social et social » (seul le II, contient le mot « prévention »).

On pourra s'étonner ce que l'alinéa 2 du II n'évoque que « *le partage, entre des professionnels ne faisant pas partie de la même équipe de soins,* ***d'informations nécessaires*** *à la prise en charge* », et non pas « ***strictement nécessaires*** ». Mais cela nous semble relever d'une erreur matérielle, qui n'altérerait probablement pas un raisonnement juridictionnel.

En outre, l'article 92 de la loi du 26 janvier 2016 autorisait, à titre expérimental, pour une durée de cinq ans suivant sa promulgation, des « *projets d'accompagnement sanitaire, social et administratif des personnes souffrant d'une maladie chronique ou étant particulièrement exposées au risque d'une telle maladie ainsi que des personnes handicapées* ». Il est alors précisé que « *Pour l'application du présent article,* ***les informations strictement nécessaires*** *au projet d'accompagnement et relatives à l'état de santé de la personne, à sa situation sociale et à son autonomie peuvent être échangées et partagées dans les conditions fixées à l'article L. 1110-4 »* (CSP). **On retrouve ici le critère de la stricte nécessité.**

ii. en matière militaire

En 2018, le critère « strictement nécessaire » a aussi été retenu pour l'introduction de l'application de l'article 1110-4 CSP en matière militaire, « *au sein du service de santé des armées ou dans le cadre d'une contribution au soutien sanitaire des forces armées prévue à l'article L. 6147-10, ou un professionnel du secteur médico-social ou social relevant du ministre de la défense* »). Mais ici, il ne s'agit que d'échange à **finalité d'accompagnement**, et **des conditions supplémentaires doivent être fixées par décret en Conseil d'Etat pour cela**. Dans le III bis qui vise spécialement ce cas, il s'agit en effet des « *informations (...) strictement nécessaires* ***à son accompagnement*** »[320].

Curieusement, en matière militaire toujours, l'article L. 1110-4 VI dispose que « *Les conditions et les modalités de mise en œuvre du présent article pour ce qui concerne l'échange et le* ***partage d'informations*** *entre professionnels de santé, non-professionnels de santé du champ social et médico-social et personnes ayant pour mission exclusive d'aider ou d'accompagner les militaires et anciens militaires blessés sont définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés* ».

[320] Ajout par art. 2, ord. n° 2018-20 du 17 janvier 2018.

Or, ce VI est étonnant : n'apparaît-il redondant avec le III bis, car il porte la même finalité (mission exclusive d'accompagnement) et la même condition (décret en Conseil d'Etat) ; contradictoire, car il étend le champ d'application du texte (de « échange » dans le III bis, à « échange et partage » dans le VI), tout en atténuant, en apparence, les conditions quant à l'information (« information strictement nécessaire » dans le III bis, « partage d'information » dans le VI) ; presque emphatique, ordonnant le recueil de l'avis de la CNIL en préalable du Décret (VI), tandis que la procédure de décret (III bis) ne le prévoit pas ?
La seule différence tient à la qualité des personnels indiqués : dans le VI, « professionnels de santé, non-professionnels de santé du champ social et médico-social et personnes ayant pour mission exclusive » etc. *ne relevant implicitement pas du ministre de la défense (ou de sa tutelle)*. Mais cela justifie-t-il toutes les différences relevées ?

iii. conséquences

Ici, le texte régit des professionnels et des non-professionnels de santé **qui n'exercent pas dans le contexte visé par le III bis**. **Mais cela peut-il justifier ces écarts entre le III bis et le VI** [321] ? cela ne serait-il une atteinte au droit introduit en 2002 qui, du fait de son but, doit relever d'une appréciation objective (l'information à protéger, qui que soit la personne) ?

Le même critère des « informations strictement nécessaires » s'appliquant à tous les subdivisions pertinentes (I à III bis, sachant de notre point de vue accidentelle, son omission à l'alinéa 2 du II et au VI), **n'eût il pas été plus efficient de le mettre en exergue simplement au titre du principe général dans le I, applicable à toutes les subdivisions de l'article L. 1110-4 CSP ?**

Cela pour une question d'intelligibilité, mais aussi pour éviter l'inflation continue des textes.

Quoiqu'il en soit, nous constatons ici que si l'on parle dans l'article L. 1110-4 CSP de « *secret professionnel* », de « *secret des informations* », de « *respect de la vie privée* », « d'informations strictement nécessaires », et si la loi dispose que « *ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes.* » (I al. 2), **nulle part la « donné de santé » n'est en soi définie**.

[321] A moins de considérer que la jurisprudence du Conseil d'Etat préc. en 2012 quant au partage d'information en milieu carcéral, ait été une source d'inspiration par analogie.

3. L'impact des nouvelles technologies sur le partage « habilité » de données

Nous voyons ici deux cas récents déterminés toujours par le dynamisme technologique : le cas du professionnel de santé « concerné » par l'usage de l'intelligence artificielle (a), et le cas des applications habilitées à accéder à de l'espace numérique de santé (b).

a. Le professionnel de santé « concerné » par l'usage de l'IA, un cas flou ?

En 2021, le législateur a institué un cadre légal d'emploi de l'intelligence artificielle en santé, pour des fins de prévention, diagnostic ou de soin [322]. Dans la 4ème partie CSP (Professions de Santé), la loi a créé un article L. 4001-3, lequel traite des conditions d'emploi, par un professionnel de santé, d'un dispositif médical « *comportant un traitement de données algorithmique dont l'apprentissage a été réalisé à partir de données massives* » (L. 4001-3-I) : cela distingue ici l'IA d'autres types de logiciels qualifiés de « dispositifs médicaux » – on le reverra en partie II de notre thèse quant au régime d'accès et de supervision des données [323].

Outre le fait que le patient doive, selon la loi, être informé du recours à un tel outil, et même « *averti* » (sic) de l'interprétation qui en résulte (étonnamment on trouve ce point en partie IV dans L. 4001-3, non dans la partie I du livre I CSP), il est spécifié que les « *professionnels de santé concernés sont informés du recours à ce traitement de données. **Les données du patient utilisées dans ce traitement et les résultats qui en sont issus leur sont accessibles*** ». Ce point n'a pas plus retenu l'attention de la doctrine : auteur d'une belle synthèse à chaud, madame Crichton n'y traite pas des causes/conséquences de cette information interprofessionnelle [324].

Or, si l'on peut inférer du contexte, que les « professionnels de santé concernés » **sont nécessairement ceux ayant à connaître de l'action de leur confrère**, force est de constater que la question ne se pose pas explicitement dans le cadre d'un « échange », ni d'un « partage » de données au sein d'une équipe de soins, pour un projet de soins déterminé (*supra*) : elle **peut lui être postérieure, voire hétérogène** (autre contexte de soin, qui impliquerait ou mobiliserait des données liés à des constats et actions antérieurs).

---

[322] Loi n°2021-1017 du 2 août 2021 relative à la bioéthique.

[323] On notera qu'à l'origine, l'article 11 du projet de loi n'évoquait qu'un « traitement algorithmique de données massives », ce qui ne peut caractériser l'IA. Assemble nationale, projet de loi n° 2187 du 24 juill. 2019). Sur les débats parlementaires qui en ont résulté : B. Bévière-Boyer, « Droit, intelligence artificielle et système de santé », in M. Bouteille-Brigant [dir.], *La personne face à l'intelligence artificielle*, IFJD, 2021, p 152 et s.

[324] C. Crichton, « L'intelligence artificielle dans la révision de la loi bioéthique », Actualité Dalloz, IP/IT et communication, 16 sept. 2021.

Selon la loi, le seul compte rendu d'un acte motivé par l'IA, et l'interprétation/conclusion formalisées du professionnel, **ne sont pas suffisants** : il semble que la loi veuille donner aux intervenants subséquents ou ultérieurs (cas de complications, récidives, autres), **la possibilité d'une réassurance quant à la pertinence de l'interprétation/conclusion, sans que le « professionnel concerné » soit nécessairement strictement homologue de l'utilisateur initial** (par exemple, de radiologue à radiologue, en matière d'imagerie médicale). Cela rend bien compte des difficultés de gestation de la loi, et du caractère non clos du débat.

Ainsi, si le but de L. 4001-3-II est la réassurance intellectuelle en contexte d'usage encore balbutiant de l'IA, le professionnel utilisateur décidera-t-il seul des professionnels « concernés » qu'il doit informer ? Un professionnel de santé qui *ex post* s'estime « concerné » peut-il demander **l'accès aux données « brutes » qui précédaient le résultat et l'ont déterminé** ? pourrait-on reprocher à un professionnel, que la juridiction estimerait raisonnablement « concerné », **sans que la loi n'ait expressément défini ce critère,** de ne pas avoir demandé de telles données, à défaut d'avoir été pressenti par leur collecteur et utilisateur initial ? L'acte sera-t-il déposé dans le dossier avec mention expresse de l'usage de l'IA, ouvrant la possibilité pour des professionnels soucieux ou curieux, de s'estimer « concernés » *ex post* ? Que se passerait-il, en cas de divergence d'interprétation quant au résultat sur la base de mêmes données, mais avec une IA différente (ou sans IA), au titre de procédure de second avis ? [325]

Certes, beaucoup pourrait dépendre de l'attitude du patient. Ce dernier doit être « averti » de l'interprétation [326] ; ceci sans être explicitement destinataire des données et des résultats de la mise en œuvre de l'IA (L. 4003-I), lesquels toutefois, ne sauraient sans doute lui être refusés s'il les demandait (droit d'accès). En revanche, son consentement à l'usage de l'IA n'est pas requis : il doit en être informé, sans que cela en soit un préalable nécessaire [327].

[325] Echanges entre MM. Megerlin F et Villani C, TR in Colloque sur l'intelligence artificielle en matière d'imagerie médicale IABM 2023, Ecole des Mines Paris Tech – Institut Curie, Paris 31 mars 2023.
[326] Ce qui postule un risque, en contraste du verbe « informer » habituellement utilisé ; on ne peut imaginer – mais ne saurait exclure ! – que l'emploi du verbe « avertir » ait ici été justifié par le seul désir d'éviter la répétition dans la même phrase, du verbe « informer », ibid. préc.
[327] En 2018, l'avis 129 du Comité consultatif national d'éthique (CCNE) relatif à la révision de la loi de bioéthique exprimait le souhait qu'un principe d'information préalable du recours à un algorithme fût consacré dans la loi (p. 103, § 6.3). **Cela n'a donc pas été le cas.**

L'unique point certain ici, est que seuls des professionnels de santé (implicitement, ceux définis au quatrième livre dans le CSP) peuvent être « concernés ». Comme pour toutes autres données de santé, mais tout spécialement, cela **ouvre la question du traitement à distance potentiellement transfrontière**, si le système d'IA le requiert (Partie II).

b. Le « besoin d'en connaître » par les outils numériques / services connectés à l'ENS

En 2019, le législateur a institué l'espace numérique de santé (ENS), qui désigne un guichet centralisé d'accès par tout assuré social français (et par tout bénéficiaire de l'Aide médicale d'Etat), à l'ensemble de ses données de santé enregistrées dans les supports (dossier médical personnel, dossier pharmaceutique, dossier de remboursement, etc.), **auparavant autonomes et surtout non directement accessibles à l'intéressé** [328]. Le décret d'application a été publié en 2021, et est à l'origine d'une section 4 « Espace numérique de santé » (articles R. 11111-26 à -39 dans la partie réglementaire du CSP [329]. Nous en traiterons *infra* [330].

Notons seulement ici que, créé en 2019, l'article L. 1111-13-1, qui détermine les conditions d'ouverture, le contenu et les modalités d'accès de l'ENS, prévoit que **des outils et services numériques peuvent l'abonder distinctement de l'implication d'acteurs ou d'établissements de santé,** sociaux ou médicaux sociaux (*ibid.* II, 3° et 6°).

Or, son III, qui détermine les conditions d'intégration de ces outils et services numériques dans l'ENS (laquelle intégration suppose un référencement des technologies [331]), **prévoit la possibilité d'accès transverse de ces outils et services numériques à des données** contenues dans les composantes réunies par l'ENS.

*** cette prévision est négative dans la loi :** « *Les services et outils numériques référencés ne peuvent accéder aux données de* (l'ENS) *du titulaire* ***qu'avec l'accord exprès*** *de celui-ci, dûment informé des finalités et des modalités de cet accès lors de l'installation de ces services et outils,* ***et qu'à des fins*** *de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour une durée de conservation strictement proportionnée à ces finalités* »;

---

[328] Article 45 II de la loi n° 2019-774 du 24 juillet 2019.
[329] Décret n° 2021-1048 du 4 août 2021 relatif à la mise en œuvre de l'espace numérique de santé NOR : SSAD2112391D
[330] Sous un autre angle, not. Morlet-Haïdara, « L'*empowerment* du patient et l'Espace Numérique de Santé « Mon espace santé », JDASM 2023/1 (n°36), pp 33-44.
[331] Arrêté du 23 juin 2022 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé - NOR : SPRD2214799A, JO 5 juillet 2022.

*** cette prévision est positive dans le décret d'application** : « *Le titulaire peut autoriser les services et outils numériques en santé référencés dans l'espace numérique de santé* ***à accéder à certaines données de son dossier*** *dans les conditions (...)* » (R. 1111-32 4ème alinéa). L'accès des outils et services numériques (applications et objets connectés, III 3° et 6° préc.) aux données ne dépendra-t-il que de la volonté du patient ? **Que signifie la phrase « certaines données » ?**

L'arrêté de juin 2022 relatif aux critères de référencement de ces outils et services dispose que « *Les services conformes à ces seuls* ***critères ne peuvent pas encore proposer à leurs utilisateurs d'échanger des données*** *avec Mon espace santé* » [332] ; cela suggère qu'une disposition technique complémentaire et/ou un arrêté additionnel seront peut-être requis **pour déterminer le « besoin d'en connaître »** [333] : cela ne pourrait il éviter une approche invasive, par aspiration de données de santé au-delà de la finalité consentie, qui pourrait découler d'une conscience imparfaite des enjeux de leur partage pour les titulaires de l'ENS ?

SYNTHESE P1T1C1

Ce premier chapitre du **Titre I « définition de la donnée de santé, du contour au contenu »** était le cadre de restitution de nos recherches, dans ce titre plutôt descriptif mais occasion de relever des points inexplorés, de la dynamique de la notion de « donnée de santé » avant l'adoption du droit européen en 2016, qui portera à maturité la ligne de partage conceptuel.

***** Dans une première section, nous avons constaté la première définition *a minima* de la notion par le droit commun. L'autonomie de la notion en droit français, a été précédée par l'apparition de la notion de « donnée sensible », dans le champ statistique puis informatique. Longtemps, la « donnée sensible » n'a pas intégré de façon explicite la « donnée de santé » :

[332] Ibid préc. article 1.

[333] *Comp*. l'article R. 1111-32 CSP, 3ème alinéa : " *Sans préjudice des dispositions de la sous-section 2 de la section 5 du présent chapitre relative aux modalités d'accès au dossier médical partagé et aux droits du titulaire, le titulaire peut autoriser un professionnel, un établissement de santé ou un établissement ou service social ou médico-social, à consulter ou alimenter tout ou partie de son espace numérique de santé de manière permanente dans les mêmes conditions et selon les mêmes modalités que celles prévues à l'article R. 1111-46 pour l'accès au dossier médical partagé*".

la spécification de la dimension sanitaire y est graduelle, sans qu'un contenu positif lui soit assigné. Son autonomie en droit européen a connu une dynamique similaire : une absence de définition dans les énoncés des droits fondamentaux, qui ne servaient qu'à tracer les contours. Ceux-ci ne commencent véritablement à se préciser que dans le droit commun des données personnelles, alors que germe la réflexion sur les soins transfrontières, et que se pose la question du statut de la donnée en tant qu'entité sélectivement partageable à ce titre.

* Dans une seconde section, nous avons restitué nos observations quant à la notion, cette fois en droit de la santé. Longtemps, cette construction s'est établie sur le seul tracé des contours de l'activité en matière de soins de santé, sans qu'en soit défini un contenu intrinsèque : ainsi, la « donnée de santé » est inférée du champ du secret de santé, dont les dépositaires se sont progressivement élargis, du fait des nouveaux modes d'exercice et notamment la pluridisciplinarité des prises en charge. Le champ de protection ne devient explicite qu'avec la loi de 2002 : elle renverse la perspective, en instituant un droit unifié pour le patient, au-delà des obligations historiques dispersées es professionnels. De ce fait, elle tend à définir de façon positive les informations couvertes, dont les débiteurs et les modes de partage continuent à s'élargir, imposant une approche nouvelle, car désormais analytique, de l'information sous la cloche du secret.

La question du besoin d'en connaître devient alors essentielle.

CHAPITRE II. LA DYNAMIQUE DU CONTENU DE LA NOTION DEPUIS L'ADOPTION DU DROIT EUROPEEN EN 2016

Dans ce second chapitre, nous considérons la façon dont **la même question du contenu de la notion de « donnée de santé » est envisagée** selon le paradigme européen.

La notion de « droit européen » recouvre nous l'avons vu, deux types de sources institutionnelles : celles de l'Union européenne, celles du Conseil de l'Europe. Nous concentrerons l'attention sur le droit dérivé de l'Union, car la Convention européenne des droits de l'homme de 1981, et la Charte européenne des droits fondamentaux, posent des principes fondamentaux, sans visée ni besoins de contextualisation technique.

A ce titre, c'est le droit européen, qui par le Règlement de 2016 dit « RGPD » [334] **a le premier introduit une définition positive de la notion de « donnée de santé » érigée en catégorie juridique**, sans que ce véhicule normatif ne relève du droit sanitaire (section 1).
Compte tenu de l'adoption simultanée et ultérieure d'autres textes portant leurs propres définitions, on peut se demander si le RGPD de 2016 **est un droit commun de référence quant au contenu de la « donnée de santé »** (section 2).

SECTION 1. L'INTRODUCTION D'UNE DEFINITION POSITIVE DE LA « DONNEE DE SANTE »

Aucun des textes européens ni nationaux précités n'avaient défini, sous ces termes, la notion de « donnée de santé » (nous reviendrons sur le « Système national des données de santé », « l'Institut des données de santé » introduits en France en 2016, et leur évolution depuis avec la Plateforme des données de santé dite *Health data Hub*). En effet, tous les textes **invoquaient jusqu'alors sans les définir** des données « de », « relatives à » ou « concernant » la santé ; des « données médicales », « informations médicales » ; un « secret médical », « secret de santé », mais c'est tout.

Peu avant l'adoption du RGPD en 2016, le groupe de travail dit « de l'article 29 » (devenu EDPB [335]) avait émis un très intéressant avis quant à la notion de « donnée de santé » [336]. Cet avis avait échappé à nos recherches en 2017. **Il résumait son analyse en pointant que les données personnelles étaient des données de santé quand** : « *a) les données traitées par l'application ou le dispositif sont intrinsèquement / clairement des données médicales. En d'autres termes, les données fournissent des informations sur l'état de santé physique ou mentale d'un individu généré dans un contexte professionnel de la santé (par exemple, les fournisseurs de soins de santé) ; b) les données brutes du capteur traitées par l'application ou dispositif peuvent être utilisés indépendamment ou en combinaison avec d'autres données, pour tirer des conclusions sur l'état de santé ou des risques réels pour la santé d'un individu ; c) les données* ***permettant de tirer des conclusions à propos de l'état de santé d'un individu***

[334] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[335] Comité européen pour la protection des données (titré EDPB pour ne pas le confondre avec le Contrôleur).
[336] Article 29 Data Protection Working Party, Lettre du 5 février 2015, voir surtout son « ANNEX - Health Data in Apps and Devices ». L'annexe n'est pas paginée, mais c'est en page 5.

(indépendamment du fait que ces conclusions sont exactes ou inexactes, légitimes ou illégitimes, suffisantes ou insuffisantes) [337].

Or, cette présentation **à la fois analytique et extensive**, dont les données biométriques et génétiques devaient être définies séparément, n'a pas été retenue dans l'élaboration du RGPD de 2016. On rappellera les circonstances d'élaboration du Règlement européen (§1), avant de relever la définition inédite de la « donnée de santé » qu'il consacre (§2).

§1. L'ELABORATION DU RGDP POUR UNE PROTECTION « GENERALE » DES DONNEES PERSONNELLES

Il n'est pas lieu ici de longs développements : **ce Règlement qui abroge la directive 95/46 CE se revendique des principes** posés par la Charte des droits fondamentaux européens, et par le Traité sur le fonctionnement de l'Union européenne (TFUE).
Les deux convergent pour disposer que la protection des personnes physiques à l'égard du traitement de données à caractère personnel est un droit fondamental (article 8§1 Charte), lequel trouve pour corollaire que toute personne a le droit à la protection des données à caractère personnel la concernant (art 16§1 TFUE).

Cette approche européenne a été remarquée, car **l'outil est un règlement général** (les champs d'inapplicabilité sont une exception, *infra*), préféré à des textes d'application sectorielle, donc très fragmentés comme on l'a vu aux Etats-Unis.

Voyons rapidement la justification de ce règlement pour abroger la directive de 1995 (A), puis son champ d'application pour les éléments pertinents dans notre recherche (B).

A. BUT DU RECOURS AU REGLEMENT POUR LA PROTECTION DES DONNEES

Du fait de son but, de son champ large et de ses conséquences systémiques, le RGPD a donné lieu à une abondante production doctrinale qu'il n'est pas lieu de rapporter ici, du fait de l'objet spécifique de notre recherche. Rappelons que son objectif est d'« *assurer un niveau*

[337] La lettre est en anglais. Nous reprenons littéralement la traduction de J.B. Malafosse, qui la cite en bas de page de la page 5 du rapport de présentation visant à mettre à jour la recommandation n° R(97) 5 du Conseil de l'Europe sur la protection des données médicales, lequel préconisait l'abandon du terme « *information médicale* » au profit du terme « *donnée de santé* » (cf. notre introduction).

équivalent de protection des personnes physiques et le libre flux des données à caractère personnel dans l'ensemble de l'Union ».

Cela **justifie l'action de l'Union, en application du principe de subsidiarité** consacré à l'article 5 du Traité, dans la mesure où il est constaté que cet objectif « *ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des dimensions ou des effets de l'action, l'être mieux au niveau de l'Union* » (Consid. 170).

Ce qui nous intéresse ici, **est le constat des limites de la directive de 1995 qui possédait le même objet** [338], dans un but d'unification de la protection des données personnelles à l'heure d'une échelle, volumétrie et vitesse fondamentalement différentes des échanges de données, pour des applications très diversifiées, devenues aussi largement marchandes.

1. Limites de la directive 95/46/CE face à la révolution technologique

La directive de 1995 avait été motivée par les objectifs de la Communauté tels qu'énoncés dans le Traité, à savoir l'établissement de « *liens toujours plus étroits entre les peuples européens* » (considérant n°1). Rappelant que les systèmes de traitement de données devant être au service de l'homme, et respecter les libertés et droits fondamentaux, la directive souligne qu'ils doivent également « *contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus* » (Consid. n°2). L'établissement et le fonctionnement du marché intérieur supposent la liberté de circulation des personnes, marchandises, services et capitaux, laquelle liberté **trouve pour corollaire la liberté de circulation des données**, sans préjudice des droits fondamentaux (Consid. n°3).

La notion de « santé » ne trouve dans cette directive de 1995 que 5 occurrences [339] : ainsi, quant au besoin de que le « *traitement de données sensibles puisse être mise en œuvre à **certaines fins relatives à la santé*** », en considérant n° 33 ; pour une dérogation de l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie **dans des domaines tels que la santé publique** et la protection sociale » (consid. n° 34) ; où l'accès des « **données à caractère médical** ne peut être obtenu que par un professionnel de santé » (consid. n° 42) ; puis dans l'article 8 : il interdit le traitement des

[338] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[339] On pourrait certes être frappé de cet a priori faible nombre d'occurrences, mais c'est une des plus fortes, avec celles des droits fondamentaux consacrés dans la CEDH de 1981.

« **données relatives à la santé** » sauf exceptions, dont celle de son alinéa 3, lequel évoque les **finalités médicales** (prévention, diagnostic, administration des soins, traitements).

Les limites de ce premier texte fondateur sont énoncées dans le RGPD (Considérant n° 9) : il reconnaît la valeur de la Directive de 1995, laquelle « *demeure satisfaisante en ce qui concerne ses objectifs et principes* ».

Mais le RGPD relève dans la foulée que, en tant qu'outil d'harmonisation des droits nationaux, elle *« **n'a pas permis d'éviter une fragmentation de la mise en œuvre** de la protection des données dans l'Union* », et par ailleurs du fait de son contenu même, qu'elle n'a pas permis d'empêcher « *une insécurité juridique ou le sentiment, largement répandu dans le public, **que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne*** ». La directive de 1995 a donc été abrogée par le Règlement 2016/679 du Parlement et du Conseil.

Paradoxalement, le règlement 2016/679 n'intègre pas la catégorisation par le groupe de travail de l'article 29, qui proposait que les données personnelles fussent qualifiées « de santé » selon une approche extensive [340]. Nous avons certes déjà cité ce point. Cette catégorisation ne sera pas non plus reprise par la CNIL, *infra*.

2. Unification du droit de protection des données sensibles, à quel point ?

Selon le Règlement de 2016, l'obsolescence des dispositions de la directive de 1995 résulte de ce que (inutile de paraphraser) « *l'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. **L'ampleur de la collecte et du partage de données** à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère **personnel comme jamais auparavant dans le cadre de leurs activités**. De plus en plus, les personnes physiques rendent des informations les concernant **accessibles publiquement et à un niveau mondial*** » (Consid. n°6).

[340] Annexe à la lettre du 5 février 2015 du groupe de l'article 29, préc.

Cela est la justification, que l'on pourrait dire d'environnement de fait. Mais aussi, le RGPD relève des **différences de niveau de protection en droit**, qui « *résultent de l'existence de divergences dans la mise en œuvre et l'application de la directive 95/46/CE* » (Consid n°9), sachant que ces différences peuvent en outre « *constituer un obstacle à l'exercice des activités économiques au niveau de l'Union, fausser la concurrence et empêcher les autorités de s'acquitter des obligations qui leur incombent en vertu du droit de l'Union* » (ibid.).

En terme d'effectivité, les évolutions relevées sur le plan technologique, des usages, de la volumétrie et vélocité des échanges de données « *requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car* ***il importe de susciter la confiance*** *qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur* » (Consid 7), condition majeure de cohésion.

Nous ne passerons pas ici en revue les 173 considérants du Règlement de 2016/679 (à comparer aux 72 considérants de la Directive 95/46 !). Leur nombre inhabituel, l'ampleur et la précision de leurs développements hors du *corpus* normatif proprement dit, ne sont pas conséquences : ils marquent d'abord **l'importance d'une justification politique** de l'unification du droit, dans un champ de susceptibilités ombrageuses dont témoignent les écarts relevés entre les droits nationaux.

En outre, ces considérant fournissent une **matière importante à l'interprétation téléologique**, celle-ci consistant à interpréter à la lumière de l'intention et des buts poursuivis par un texte [341].
Pour expliquer cette méthode de raisonnement, le Doyen Carbonnier invoque son application au niveau européen : « *l'interprétation téléologique, en faveur à la Cour de justice, commande de retenir le sens qui donne un effet utile au droit communautaire »* [342]. Mais l'effet utile, dans quel sens, pour quelle acceptabilité politique ? La recherche d'efficacité unificatrice **suppose ici de mieux dessiner la finalité** (ce que ne faisait pas la Directive de 1995, d'où la difficulté à résorber certains écarts en droit comparé internes à la Communauté).

L'intention, qu'invoque l'argument téléologique, est en effet plus ou moins explicite. La téléologie **s'appuie parfois sur l'inférence**, c'est-à-dire, par défaut de clarté littérale du but,

[341] Jeanneney J, « *« Le recours aux intentions du législateur face aux énoncés normatifs ambigus »,* Droit et Philosophie, 2018, vol. 9.
[342] Cornu G, *Vocabulaire juridique, Quadrige/PUF, 13ème édition, 2020.*

sur l'appréhension de l'objectif, comme l'a précisé en 2020 la Cour de cassation [343]. Ici peu de risque de recours « par défaut » de clarté de la lettre du texte : le degré de précision des considérants du Règlement 2016/679 vise à baliser de manière fine le potentiel d'interprétation du texte en cas de besoin, et à **exclure au maximum les ambiguïtés, sources d'interférences.** Mais l'écart est grand ici, entre la définition et les considérants !

Cette unification du droit européen s'appuie sur le double mécanisme classique : celui du *corpus* du règlement, lequel porte un droit commun aux Etats membres sans, à la différence des directives, d'agenda de transposition ; celui de ses considérants, qui éclairent le but (ambition et limites) du texte. Cela tant dans le cas de son invocation de **contentieux éclatés devant les juridictions nationales**, puisque le texte vise à la correction d'écarts relevés ; qu'en cas de **centralisation du contentieux d'interprétation / d'application** devant la CJUE, si elle était saisie d'un recours préjudiciel ou d'une action en manquement, etc.

Les organes juridictionnels voient ici leur action non bornée, **mais étroitement enserrée par des considérants à haute teneur politique et technique**, tant l'équilibrage de la liberté et sécurité est ici spécialement délicate, dans un champ qui va intéresser la souveraineté nationale autant qu'européenne (*infra*, Partie II).

B. CHAMP D'APPLICATION DU REGLEMENT EUROPEEN

Le champ d'application matériel est défini dans l'article 2, et ne prête pas à discussion quant aux inclusions et exclusions, celles-ci conduiront à l'adoption de textes spécifiques [344]. Le champ d'application territoriale, objet de l'article 3, mérite ici d'être détaillé.

---

[343] Civ. (soc.) 25 mars 2020, 18-12.467, Publié au bulletin. En l'espèce, la question de pose certes au sujet d'une convention collective en droit du travail ; mais les attendus nous semblent extrapolables : une convention collective donc, « *si elle manque de clarté, doit être interprétée comme la loi, c'est à dire d'abord en respectant la lettre du texte, ensuite en tenant compte d'un éventuel texte législatif ayant le même objet et,* ***en dernier recours, en utilisant la méthode téléologique*** *consistant à rechercher l'objectif social du texte* » (attendu n° 4).

[344] Thelisson E., « la portée du caractère extraterritorial du règlement général sur la protection des données », Rev. int. dr. éco. 2019/4 (t 26), 501-533 ; Deroudille A et Fatah A, « L'extraterritorialité du RGPD dans le contexte du "Cloud Act" », *RUE*, 2019, p. 442.

1. un critère d'application territorial … ou personnel ?

L'article 3 du Règlement de 2016/679 définit son champ d'application ainsi : il **«** *s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union,* ***que le traitement ait lieu ou non dans l'Union*** » (al. 1). Ce premier alinéa met en exergue un critère territorial, quant au siège de l'établissement du responsable du traitement ou du sous-traitant, quel que soit le lieu du traitement. C'est un **critère de territorialité juridique de l'opérateur, non de territorialité matérielle des opérations**.

De même, l'alinéa 2 du même article 3 : le règlement « *s'applique au traitement des données à caractère personnel relatives* ***à des personnes concernées qui se trouvent sur le territoire de l'Union*** (indifféremment quant à leur nationalité, donc) *par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes* ***concernées dans l'Union****, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes,* ***dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union***. »
Les critères de rattachement sont donc doubles : critère matériel (apport de l'article 2), critère territorial (apport de l'article 3).

Enfin, l'alinéa 3 du même article 3 dispose que le règlement « s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union **mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public** ». Cette disposition est classique ; mais l'on parle ici de l'applicabilité du droit d'un Etat membre, non du droit de l'Union, **ce qui revient à une forme de bi-latéralisation en base nationale du dialogue quant au droit applicable**.

Or, nous verrons dans les contentieux portés devant la juridiction européenne, la **portée personnelle** du droit, lorsque la CJUE sera amenée en 2015 puis 2020 à constater l'insuffisance, pour la protection des droits des citoyens européens, des garanties données en cas de transfert international des données personnelles pour fin de traitement (Partie II).

Cette portée est également personnelle, du fait que peuvent en bénéficier des citoyens qui ne sont pas ressortissants de l'UE, au titre d'accords avec l'Union [345].

2. **Un préalable à la régulation des marchés et services numériques**

La question précitée est d'autant plus cruciale, que le RGPD **est le préalable d'une vaste construction** que nous ne détaillerons pas ici, mais évoquerons en seconde partie de notre thèse : il était nécessaire que le développement unifié des garanties quant au traitement des données personnelles, précédât d'autres textes majeurs de l'Union, qui visent aussi à protéger le marché intérieur à l'égard de dominations du marché numérique (a), et à réguler des services numériques diversifiés en développement exponentiel (b). Ces deux textes fondamentaux sont remarquablement rédigés, de concision et efficacité.

a. La santé dans le Règlement (UE) 2022/1925 sur les marchés numériques

Le Règlement (UE) 2022/1925 traite de la **structure des marchés sous l'angle du droit de la concurrence**, et modifie des directives pourtant très récentes (2019/1937 et 2020/1828) [346]. Il relève le développement exponentiel des services de plateforme essentiels, lesquels permettent « *par exemple des économies d'échelle extrêmes, qui résultent souvent de coûts marginaux presque nuls pour ajouter des entreprises utilisatrices ou des utilisateurs finaux* » (consid 2), sources d'un « *degré considérable de dépendance des entreprises utilisatrices et des utilisateurs finaux, des effets de verrouillage, l'absence de multihébergement aux mêmes fins par les utilisateurs finaux, l'intégration verticale et les avantages liés aux données* » avec l'effet de déséquilibre fondamentaux sur les marchés.

Mais si le but du règlement est promouvoir / restaurer l'équité compétitive, **la question de la souveraineté (européenne / nationale), terme certes absent** des considérants et du *corpus* normatif, n'est pas loin. Rappelons que dès 2013, madame Morin-Desailly avait dans un rapport pointé le risque, pour l'Europe, d'être ravalé au rang de « *colonie numérique* » [347].

[345] Le bénéfice « international » du RGPD s'étend en effet à l'Islande, au Liechtenstein et à la Norvège. La décision d'incorporation du règlement (EU) 2016/679 dans l'annexe XI de l'accord sur l'Espace Economique Européen (EEE) a été adoptée le 6 juillet 2018 et est en vigueur depuis le 20 juillet 2018.

[346] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).

[347] Rappelons l'expression, dès 2013, de « colonie numérique » employée par C. Morin-Desailly, *in* Rapport d'information fait au nom de la commission des affaires européennes : « l'Union européenne, colonie du monde numérique ? », Rapport d'information n° 443 (2012-2013), déposé le 20 mars 2013.

Cela n'empêche pas l'existence dans le règlement 2022/1925, d'une exemption d'application des obligations faites aux entreprises qui seraient devenues de fait « contrôleurs d'accès », pour « ***raisons de santé publique*** *et de sécurité publique* » (article 10). Sur ces raisons, l'article 10§3 est certes laconique (son contenu correspond en effet exactement au titre synthétique de l'article 10). Mais le considérant 67 le met en perspective : il doit s'agit de « *circonstances exceptionnelles, uniquement justifiées par des raisons de santé ou de sécurité publiques définies par le droit de l'Union et interprétées par la Cour de justice* ». **Ce n'est donc pas si souverain.**

Le même considérant 67 d'expliquer que « *si une atteinte est portée à ces intérêts publics, cela pourrait indiquer que la mise en œuvre d'une obligation spécifique* ***est, dans un cas exceptionnel précis, trop coûteuse pour la société dans son ensemble****, et donc disproportionnée* » (*ibid.*). L'expérience de la pandémie de Covid19 a précédé l'adoption du règlement, et a pu l'inspirer quant à la mise en place d'outils nouveaux de résilience au regard de la conception classique de la souveraineté dans le champ de la santé (*infra*, Partie II).

Or, dès ici, cet article 10 du règlement du 2022/1925 sur les marchés numériques **peut être mis en perspective par le règlement 2022/2065 sur les services numériques**.

En effet, le considérant n° 91 du règlement 2022/265 dispose, de façon à nouveau remarquable, pour interpréter l'article 10 précité du 2022/1925 (**il n'existe aucun renvoi textuels entre ces règlements**), que « *en temps de crise, les fournisseurs de très grandes plateformes en ligne pourraient devoir prendre certaines mesures spécifiques d'urgence,* ***en plus des mesures qu'ils prendraient compte tenu de leurs autres obligations*** *au titre du présent règlement. À cet égard, il y a lieu de conclure à une crise lorsque des circonstances extraordinaires peuvent entraîner une menace grave pour la sécurité publique ou* ***la santé publique dans l'Union ou dans des parties importantes de l'Union****. Ces crises pourraient* ***résulter de conflits armés ou d'actes de terrorisme, existants ou nouveaux****, de catastrophes naturelles telles que des tremblements de terre et des ouragans,* ***ainsi que de pandémies et d'autres menaces transfrontières graves pour la santé publique*** *».*

Pour quelles conséquences légitimes, selon toujours le considérant n° 91 ? La Commission « ***devrait être en mesure d'exiger*** *que des fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne* ***initient d'urgence une***

réaction aux crises. *Les mesures que ces fournisseurs peuvent déterminer et envisager d'appliquer comprennent, par exemple, l'adaptation des processus de modération des contenus et l'augmentation des ressources consacrées à la modération des contenus, l'adaptation des conditions générales, des systèmes algorithmiques et des systèmes publicitaires concernés, l'intensification de la coopération avec les signaleurs de confiance, la prise de mesures de sensibilisation, la promotion d'informations fiables et l'adaptation de la conception de leurs interfaces en ligne* ». Ceci dans un délai très court pour une durée justifiée, **avec une auditabilité exigible** de tels protocoles d'urgence (consid. n°9) etc.

b. La santé dans le Règlement (UE) 2022/2065 sur les services numériques

On vient déjà de citer le Règlement 2022/2065, dont la connexion avec le règlement 2022/1965 est remarquable, alors que n'existent aucun renvoi de l'un à l'autre. Le Règlement 2022/2065 a **pour objet la réglementation d'activité diversifiées,** non la régulation des effets structurels des « services de plateformes essentiels » sur le marché européen [348].

Il modifie une directive beaucoup plus ancienne, l'offre en matière de services numériques ayant beaucoup évolué depuis les années 2000, et l'expérience des marchés nationaux et européen s'étant accumulée [349]. Ce point nous a incidemment intéressé dans nos recherches en 2020, du fait de son **impact probable sur les professions historiquement réglementées en santé** notamment, posant le statut des algorithmes pouvant conditionner l'accès aux produits de santé (et requérir des données de santé) selon le droit national applicable [350].

Plus fondamentalement, le règlement relève des risques inédits liés à l'essor technologique. Pour ce qui est de la santé, son considérant n° 83 relève une quatrième catégorie de risques induits [351] par la conception, le fonctionnement ou l'utilisation, « ***y compris par manipulation****, de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne* ***ayant un effet négatif réel ou prévisible sur la protection de la santé publique*** *et des*

[348] Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).
[349] Directive 2000/31/CE du Parlement européen et du Conseil.
[350] E. Pinilla, P. Bordas, F. Megerlin, « Le juge européen et les services dématérialisés des professions réglementées : quelle pharmacie à l'aube du Digital Market Act ? » Rev Gén Dr Méd 2021(1), 175-185.
[351] La première catégorie est celle des risques associés à la diffusion de contenus illicites (détaillés *in* consid. 80) ; la seconde catégorie recouvre « *l'incidence réelle ou prévisible du service sur l'exercice des droits fondamentaux* » (détaillés in consid. 81) ; la troisième catégorie recouvre « La troisième catégorie de risques concerne les effets négatifs réels ou prévisibles sur les processus démocratiques, le discours civique et les processus électoraux, ainsi que sur la sécurité publique » (consid. n°82).

mineurs, ainsi que des ***conséquences négatives graves sur le bien-être physique et mental*** *d'une personne (…) Ces risques peuvent également résulter de* ***campagnes de désinformation coordonnées liées à la santé publique ou de la conception d'interfaces en ligne susceptibles de stimuler les dépendances comportementales*** *des destinataires du service* ». Le considérant est synthétisé dans l'article 34 d), laconique. L'ensemble doit être lu.

L'article 36 est dédié au « mécanisme de réaction aux crises », et dispose qu'une crise est constituée « ***lorsque des circonstances extraordinaires entraînent une menace grave pour la sécurité publique ou la santé publique*** *dans l'Union ou dans des parties importantes de l'Union* » ; l'article 48 institue la possibilité pour la Commission, de **lancer l'élaboration de protocoles de crise**, dans des situations « *strictement limitées à des circonstances extraordinaires affectant la sécurité publique ou la santé publique* ».

On voit la **prégnance de la question de la santé, et de façon sous-jacente des données de santé** qui éclaireront la décision d'anticipation ou de rédaction (Partie II), dans un texte qu'une approche superficielle pourrait reléguer à un but de régulation des services marchands.

Mais le droit européen prévoit que **l'ensemble du potentiel privé notamment de portée transnationale est mobilisable (réquisitionnable) au côté des moyens régaliens** sur le fondement de la sécurité publique ou la santé publique, motifs consubstantiels d'impérativité. Cela supposait en amont l'énoncé d'un cadre commun des « données de santé » et de leur transfert transfrontière, en voire au-delà de l'Union.

§2. LA DEFINITION CONTRASTEE DU CONTENU DE LA « DONNEE DE SANTE » PAR LE RGPD

Revenons à l'appréhension, puis à la définition de la « donnée de santé » : le RGPD est le **premier texte qui définisse de façon positive la notion de « donnée de santé ».**

Nous avons précédemment vu comment cette définition était, jusqu'alors, le fait de raisonnements par inférence : du droit commun ou sanitaire, du champ du secret et des modalités d'échange / partage d'informations etc., ou n'était qu'une composante non définie du « dossier médical », lui même défini pour des applications transfrontières.

Cette définition s'impose dans le droit des Etats membres ; mais comme nous l'avons vu, le Règlement de 2016 possède des considérants développés. Ils visent à justifier politiquement la norme, permettre son acceptabilité, et unifier son interprétation par l'argument téléologique. Or, **n'existe-t-il pas un écart important entre la définition** stricte de la « donnée de santé » dans le corpus normatif, et la façon dont elle est appréhendée dans les considérants ?

Si la chronologie voudrait que l'on étudiât les considérants avant le *corpus*, nous procéderons à la démarche inverse : le but est de mettre en exergue le potentiel interprétatif ouvert aux autorités et aux juridictions (sans compter les plaideurs, personnes physiques ou morales).

A. LA QUALIFICATION DE LA « DONNEE DE SANTE » DANS LE *CORPUS* DU REGLEMENT

Le *corpus* du Règlement contient **plusieurs définitions pertinentes**, outre la définition primordiale de la donnée personnelle [352]. Il ne s'agit pas seulement des « *données concernant la santé* » (objet de l'article 4.15), mais aussi des « *données biométriques* » (objet de l'article 4.13), et des « *données génétiques* » (objet de l'article 4.14), qui sont donc séparées.

D'emblée, on constate ici que les données concernant la santé sont définies *après* les données génétiques et biométriques, dont on peut imaginer que les contours plus nets et les applications immédiates, justifient la préséance. On considérera ces catégories dans l'ordre du règlement (1), avant de relever les interférences (2).

1. Définitions des données pertinentes selon les catégories

*** Les « données génétiques »** sont entendues (article 4.13) comme les « *données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui* ***donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique*** *et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* ». Ce qui nous intéresse ici est qu'il s'agit d'une donnée hautement fiable d'identification d'une personne, à usages multiples.

[352] Pour rappel toutefois, l'article 4.1 du Règlement 2016/679 entend par « données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

*** Les « données biométriques »** sont entendues (article 4.14), comme les « *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* ». Ce qui nous intéresse ici est qu'il s'agit d'une donnée, moins fiable mais d'accès si facile, **d'identification multi-usages** d'une personne.

*** Les « données concernant la santé »** (article 4.15), sont entendues comme les « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».
Dans ce texte, ces données, au potentiel de grande variabilité selon les situations, ne prétendent plus à l'identification d'un individu. On notera ici que **la définition focalise sur la nature des informations, non sur leurs conditions d'acquisition, en contraste du droit français** [353]. Soulignons aussi d'emblée qu'elle est **fois large… et apparaît tautologique** (« *données relatives à la santé (…) qui révèlent des informations sur l'état* ») [354].

2. Interférences entre les catégories de données prévues dans le règlement

Les données génétiques et les données biométriques sont autonomisées en raison de leurs **nombreux usages hors santé**, du fait de leur potentiel d'identification unique des personnes auxquelles elles se rapportent. Les finalités intéressent au premier chef les libertés publiques, mais également de nombreuses autres (droits d'accès à des emprises sécurisées, d'activation de systèmes d'information ou de systèmes d'arme, etc. outre les aspects parfois administratif, les applications judiciaires, parfois médico-légales etc.).

Mais les mêmes ont **par nature un intérêt dans le champ de la santé** : ceci à nouveau en raison du potentiel diagnostic, voire prédictif des données issues de l'analyse génétique, également de variations biométriques pouvant affecter un individu. Les interférences entre ces catégories nous conduiront dans notre recherche à considérer les données « génétiques » et « biométriques », comme **consubstantielles aux « données concernant la santé ».**

[353] Cf. l'article L. 1110-4 CSP depuis 2002, préc. *supra*.
[354] Megerlin F, préc. « notion de donnée de santé », Fasc 8-10 JCL, Traité de droit pharmaceutique, Litec 2023.

Le fait que l'article 14.15 ne les réincorpore pas explicitement dans son libellé, n'a aucune incidence sur ce fait, d'évidence scientifique et clinique. Cela établit bien que la définition normative des « *données concernant la santé* » **n'avait pas de prétention exhaustive, et que de toute façon, une telle prétention eût été impossible** dans le règlement 2016/679 : son considérant dédié va en attester.

Mais rappelons que **cela contraste avec la réflexion du groupe de travail de l'article 29, qui était d'une parfaite clarté** [355]. Elle est donc complétée par les données biométriques et génétiques. En outre, nous avons pointé qu'une proposition de droit européen (non encore adoptée) portait, en mai 2022, une définition de « *donnée de santé **électronique*** », pour réunir des éléments tantôt séparées on vient de le voir (données de santé, génétiques), tantôt inédits (données relatives à des déterminants de santé, de bien-être) [356].

B. L'APPREHENSION DE LA « DONNEE CONCERNANT LA SANTE » DANS LES CONSIDERANTS

Nous avons vu **l'ampleur inhabituelle des considérants dans le Règlement 2016/679,** ce que peut expliquer le besoin de justifier un texte qui entend par l'unification impérative, résorber les écarts entre les droits nationaux dans le marché intérieur ; et de cerner l'intention du Parlement et du Conseil afin de livrer aux personnes physique et morales, aux autorités au aux juridictions, **les éléments interprétatifs permettant la bonne application du droit**.

Rappelons que le but essentiel est, en préalable de la circulation et de la gouvernance, d'assurer les droits et libertés fondamentales des personnes, ce qui conduit à ce que soit interdit sauf dérogations légitimes, le traitement des « données concernant la santé » (art. 9).

1. Quelle place dans les considérants ?

Le Règlement 2016/679 ne contient pas seulement 173 considérants (contre 72 pour la directive 95/46 qu'il abroge) ; il contient également 46 occurrences des mots « santé » et « santé publique » dans les seuls considérants, et 17 dans le corpus normatif, soit en tout 63

[355] Annexe à la lettre du 5 février 2015 du groupe de l'article 29, préc.
[356] Voir l'article 2§2 a), b) et c) de la proposition le 3 mai 2022 de règlement européen sur l'espace européen des données de santé, COM(2022) 197 final. Nous développerons largement ce point dans notre thèse.

hors notes (contre 5 en tout pour la directive 95/46). On conçoit **la place forte de la « santé »** dans ce texte. Qu'en est-il de la façon dont la notion de « *donnée concernant la santé* » est appréhendée dans le considérant pertinent [357] ?

Citons littéralement le considérant pertinent (n° 35) : « *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; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic* in vitro. »

2. Quelle appréhension par les considérants ?

L'appréhension est vaste, en ce qu'elle recouvre « *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 ».* « L'*ensemble des données* » est un concept très large, « *l'état de santé future* » également, puisqu'il **englobe toutes certitudes et spéculations** fondées sur l'appréciation, par exemple de comportements et d'environnements, et de leurs variations par suivi continu (pour détection et corrélation signaux faibles, comme dans les systèmes de maintenance prédictive).

[357] Les considérants 45, 52, 53, 54, 63, 65, 71, 73, 75, 91 , 112, 115, 159 etc. se réfèrent à la notion de santé dans des contextes variés, sans modifier le contenu dressé par le considérant n° 35, ni pouvoir le réduire.

Il est **possible d'en inférer des vulnérabilités, des facteurs de risque, de complications**, etc. et de proposer des actions de réaction, voire d'anticipation: c'est l'objet de la prévention primaire et secondaire en santé [358], et des actions de promotion de la santé [359] etc.

Mais l'appréhension est limitée, car le considérant évoque les « *informations **obtenues lors du test ou de l'examen*** (etc.) » Certes, il cite « *indépendamment de sa source* » ; **mais il limite les exemples de sources** aux organes du système de santé (professionnels, établissements), ou au recours à des technologies médicales (dispositifs médicaux ou dispositifs médicaux de diagnostic *in vitro*).

Or, nous verrons que **le critère de la finalité déclarée médicale de la technologie générant l'information, est très réducteur**, du fait de la diversification des capteurs, senseurs, logiciels non « dispositifs médicaux », finalités et conditions d'usages, et potentiel informationnel. Cela contrastera avec la proposition de texte européen en mai 2022, laquelle intègre implicitement ces nouvelles technologies « santé » mais « non médicales » et dimensions (*infra*).

L'appréhension nous semble faible, au regard de la qualité de la réflexion rapportée en 2015 par le Groupe de travail de l'article 29, précédemment développée [360]. Il semblera que le texte de 2022 intègre les éléments de 2015 non retenus dans le RGDP.

SECTION 2. LE REGLEMENT EUROPEEN DE 2016 CONSTITUE-IL LE DROIT COMMUN DE REFERENCE ?

Le Règlement 2016/679 est intitulé « *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)* ».

[358] Selon la nomenclature de l'OMS, la prévention primaire vise à éviter qu'un risque n'apparaisse ; la prévention secondaire vise à la détection précoce de sa réalisation, pour engager rapidement des soins adaptés (et éviter des complications) ; la prévention tertiaire vise à la surveillance des soins d'une affection diagnostiquée, pour éviter des risques iatrogènes notamment.

[359] La promotion de la santé, composante des politiques de santé publique, « utilise des stratégies permettant d'agir sur la responsabilité sociale et commerciale et donc sur différents acteurs permettant d'accroître les capacités de la communauté elle-même (travail, culture, famille, société) ». Elle peut donc être d'impulsion publique ou privée, et n'est généralement pas médicalisée.

[360] Annexe à la lettre du 5 février 2015 du groupe de l'article 29, préc.

Un « règlement général » est il un droit commun de référence, auquel renverraient les autres textes ? Non, si leur objet est distinct : la loi spéciale peut déroger, de façon implicite comme explicite, à la loi générale. **D'autres textes, voire des doctrines spécialisées, adoptés concomitamment ou ultérieurement, sont d'ailleurs nécessaires** pour la régulation des données personnelles dans l'Union européenne.

Nous relevons ici la généalogie de la notion qui, comme en droit français, ne trouve pas sa source dans le droit sanitaire, mais dans une réflexion sur les données sensibles. Cette doctrine **voulait, par une notion générale, imprégner le droit commun européen**, mais n'a pas été suivie (§1).
Le règlement n° 2016/679 , qui pose les notions fondamentales, n'est en fait pas le seul à ce faire. De la sorte que, même s'il y est renvoyé par les textes subséquents, **il n'est pas l'unique porteur de la définition** européenne de « données concernant la santé » (§2).

§1. LA PERCEPTION DE LA DONNEE DE SANTE PAR LA DOCTRINE DU CEPD

Nous avons vu précédemment que le Contrôleur européen pour la protection des données avait été saisi de la proposition de directive sur les soins transfrontaliers ; qu'il avait dans ce cadre regretté l'absence de conceptualisation du débat, et **notamment l'absence de conceptualisation de la notion** de « donnée de santé » (ou « donnée relative à la santé »).

Rappelons brièvement son champ général d'intervention (A), avant sa doctrine quant aux données « relatives à » ou « concernant » la santé (B).

A. CHAMP GENERAL D'INTERVENTION DU CEPD

Le but du Contrôleur européen pour la protection des données, institué en 2001, est de veiller au respect, **par les institutions, organes et organismes de l'Union,** des libertés et droits fondamentaux des personnes physiques en ce qui concerne le traitement de leur données à caractère personnel, notamment leur droit à la protection des données [361]. Cela vaut dans leur propre **gouvernance interne, mais aussi et d'abord quant à la production de droit dérivé** pouvant les impacter.

[361] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

1. Compétence matérielle du Contrôleur européen pour la protection des données

Le CEPD doit être spécialement sollicité en vue de contrôles préalables, pour (article 27, règlement de 2001) « Les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités (…) ». Parmi les traitements concernés, figurent notamment « ***les traitements de données relatives à la santé*** *et les traitements de données relatives à des suspicions, infractions, condamnations pénales ou mesures de sûreté* » (article 27§2-a). On voit ici la santé à nouveau considération primordiale.

En outre, le CEPD est « *responsable de la surveillance des traitements de données à caractère personnel effectués par les institutions et organes de l'Union* ». **Mais il ne s'applique « *pas* *au traitement des données à caractère personnel dans le cadre des activités des institutions et organes de l'Union* *qui ne relèvent pas du droit de l'Union*** ».

Or, c'est le cas de la directive n° 2016/680 précitée ; du règlement n° 2016/794 du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (EUROPOL) [362] ; du règlement n° 2017/1939 du Parlement européen et du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen [363] ; du règlement n°2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (EUROJUST) [364].

Parmi les principes directeurs du CEPD (article 3 et 4, décision de 2020), figurent son indépendance, exemplarité et transparence ; la coopération « *entre les autorités de contrôle de la protection des données ainsi qu'avec toute autre autorité publique dont les activités sont susceptibles d'avoir une incidence sur le respect de la vie privée et la protection des données à caractère personnel* » (article 5). Ce qui nous intéresse ici, est qu'il dispose d'une autonomie, à la fois procédurale et doctrinale.

[362] Remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).
[363] (JO L 283 du 31.10.2017, p. 1).
[364] Remplaçant et abrogeant la décision 2002/187/JAI du Conseil (JO L 295 du 21.11.2018, p. 138).

2. Autonomie doctrinale du Contrôleur européen pour la protection des données

Le CEPD dispose **d'une autonomie doctrinale, dans la fixation de ses propres règles de procédure**. Ces règles ont été édictées pour la première fois en 2020 ; d'un point de vue juridique, elles participent des « règlements intérieurs et de procédure » [365]. Rappelons qu'il ne doit pas être confondu avec le *Comité européen de protection des données* (appelé EDPB), lequel vient également de modifier son règlement intérieur [366].

En 2022, le CEPD modifie le 14 octobre, le règlement intérieur adopté le 15 mai 2020, à nouveau par décision, donc [367]. Ce point ne nous retiendra pas ici, sauf pour souligner que l'article 16§4 du règlement intérieur de 2020 est complété d'un alinéa selon lequel « *Le CEPD déclare irrecevable et* ***ne traite pas les réclamations introduites plus de deux ans après que le réclamant*** *a eu connaissance de la violation alléguée, sauf dans des circonstances dûment justifiées et exceptionnelles* », lesquelles ne sont pas précisées.

Cela est une précision doctrinale (autonomie du règlement intérieur) apportée en application de l'article 57§1(e, du règlement n°2018/1725, lequel prévoit que le CEPD traite ces réclamations et examine l'objet de la réclamation, dans la mesure nécessaire.

Le but est naturellement de désemboliser le CEPD de demandes tardives insuffisamment justifiées (mais deux ans est long !) ; ce qui **pourrait résulter du mode d'exercice des droits par les personnes concernées, tout comme de l'acception qu'elles pourraient retenir des droits protégés**, sachant parfois l'écart parfois pour un même type de donnée protégée, entre l'ampleur du considérant, et sa définition normative. Nous avons vu cet écart manifeste, pour les données « concernant la santé ».

Si la question de l'autonomie doctrinale du Contrôleur EPD se pose, c'est parce qu'elle pourrait être confondue avec celle du Comité EPD (appelé EDPB pour éviter les confusions). Mais la doctrine n'approfondit pas l'étude de leurs relations [368], dont on peut supposer qu'elles ont évolué depuis le règlement de 2018 qui renforce les pouvoirs du CEPD. Ce point serait intéressant à approfondir, mais n'est pas l'objet de notre recherche.

---

[365] Décision du contrôleur européen de la protection des données du 15 mai 2020 portant adoption du règlement intérieur du CEPD.
[366] Règlement intérieur du Comité européen de la protection des données, V8, modifié et adopté le 6 avril 2022.
[367] Décision du contrôleur européen de la protection des données (CEPD) du 14 octobre 2022 portant modification du règlement intérieur du CEPD du 15 mai 2020, JOUE 24 oct. 2022, L 274/78.
[368] Nerbonne S, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? » Legicom 2009/1 n°42, pp 37-46.

B. LES « DONNEES « *RELATIVES A* » OU « *CONCERNANT* » LA SANTE SELON LE CEPD

Le CEPD est fréquemment sollicité (parfois se saisit d'office) sur nombre de questions impliquant la notion de « *données concernant la santé* ». Il n'est pas lieu ici de faire l'inventaire des avis, recommandations et études qui impliquent ces notions [369] : en effet, les questions **ne portent pas tant sur la notion même, que sur le régime des traitements**, même pour les textes relatifs aux situations de menaces transfrontières pour la santé [370], ou en 2020, dans l'avis préliminaire sur l'espace européen des donnée de santé (EEDS) [371].

Nous avons vu précédemment que la **première expression au fond du CEPD en matière de santé** avait porté sur la proposition de Directive relative aux soins transfrontaliers [372], dont il a été saisi en 2009, avant son adoption en 2011. Rappelons la position au fond (1), avant sa portée doctrinale (2).

1. Les « *données relatives aux soins de santé* » préférée aux « *données médicales* »

Critiquant l'absence de définition autonome de la notion de « donnée de santé », le CEPD avait alors souligné que les données relatives à la santé sont considérées comme une catégorie particulière de données, qui mérite une protection renforcée (point 14) ; que la directive 95/46/CE ne comporte pas de définition explicite des données relatives à la santé (point 15) ; qu'une acception large (en fait pas si large …) en est généralement retenue par les groupes de travail *ad hoc* : ainsi en 2007, un groupe de travail la définit comme « *données à caractère personnel (qui)* ***présentent un lien clair et étroit avec la description de l'état de santé d'une personne*** » [373] (approche qui ne retient pas le défi des inférences).

---

[369] Les avis sont tous publiés sur le site du CEDP (http://www.edps. europa.eu)

[370] Résumé de l'avis du contrôleur européen de la protection des données sur la proposition de décision du Parlement européen et du Conseil relative aux menaces transfrontières graves pour la santé (Le texte complet de l'avis en anglais, français et allemand est disponible sur le site internet du CEPD) (2012/C 197/05)

[371] CEPD, 17 nov. 2020, Avis préliminaire 8/2020 sur l'espace européen des données de santé.

[372] Projet d'avis du contrôleur européen de la protection des données concernant la proposition de directive du Parlement européen et du Conseil relative à l'application des droits des patients en matière de soins de santé transfrontaliers(2009/C 128/03).

[373] Groupe de travail dit « Article 29 » : document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), février 2007, WP 131, point II.2 ; nous avons vu en introduction, que la même formule était utilisée par Recommandation n° R (97) 5 du Comité des ministres aux Etats membres relative à la protection des données médicales, adoptée par le Comité des ministres le 13 février 1997, lors de la 584e réunion des délégués des ministres.

Dès lors, le CEPD **réunit et synthèse plusieurs sources**, pour présenter les « données relatives à la santé » comme « *englob(ant)* ***en principe les données médicales*** *(orientation d'un malade par un généraliste vers un spécialiste et prescriptions médicales, rapports d'examens médicaux, tests de laboratoire, radiographies, etc.),* ***ainsi que des données administratives et financières relatives à la santé*** *(documents concernant l'admission dans un hôpital, numéro de sécurité sociale, calendrier des rendez-vous médicaux, factures de prestation de services de santé, etc.)* » (projet d'avis, point n° 15).

A l'expression « données médicales », le CEPD indique alors préférer l'expression de « données relatives aux soins de santé » (point 15) ; mais adoptant cette expression, il renvoie à la définition qui en est donnée par la norme ISO 27799, laquelle apparaît assez mécaniste ; elle ne porte en outre que sur la « *Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002* » [374].

2. Portée de la position du CEPD à l'égard des « *données relatives aux soins de santé* »

Dans son projet d'avis sur la proposition de directive [375], **son but est de fonder une doctrine**, nous l'avons déjà souligné *infra*. Ainsi, il y énonce : « *certaines des observations qui suivent ont une portée très large — elles abordent des questions générales relevant de la protection des données à caractère personnel dans le secteur des soins de santé —* ***et pourraient dès lors valoir aussi pour d'autres instruments législatifs (contraignants ou non) relevant du même domaine*** » (ibid., point 6).

En outre, sa position est *in fine* insistante : il « ***encourage vivement l'adoption d'une définition spécifique de l'expression «données relatives à la santé»*** *dans le contexte de la proposition à l'examen, définition* ***qui pourrait aussi être utilisée à l'avenir dans d'autres textes législatifs pertinents de la CE*** » (ibid., point 17).

---

[374] ISO 27799:2008 « *Informatique de santé — Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002* » : « *toute information qui se rapporte à la santé physique ou mentale d'une personne, ou à la prestation de services de santé pour cette personne, et qui peut comprendre: a) des informations sur l'inscription de la personne concernée en vue de la prestation de services de santé; b) des informations sur les payements ou l'admissibilité à des soins de santé concernant ladite personne; c) un chiffre, un symbole ou un signe particulier attribué à une personne pour l'identifier de manière unique à des fins de santé; d) des informations sur la personne concernée recueillies lors de la prestation des services de santé dont elle fait l'objet; e) des informations provenant de tests ou d'examens d'une partie du corps ou d'une substance corporelle; et f) l'identification d'un individu (professionnel de la santé) en tant que prestataire de soins de santé pour la personne concernée.-* ».

[375] Projet d'avis du contrôleur européen de la protection des données concernant la proposition de directive du Parlement européen et du Conseil relative à l'application des droits des patients en matière de soins de santé transfrontaliers (2009/C 128/03), préc. point n° 6.

En ce sens, dans le corps du projet (point 43), il recommande, pour l'introduction d'une telle définition, de « ***partir d'une interprétation large de ce concept, telle qu'elle est décrite à la section II du présent avis*** *(points 14 et 15)* » ; il ré-insiste dans les conclusions (point 50), sur le fait que la définition des données relatives à la santé devrait « (englober) ***toutes les données à caractère personnel présentant un lien clair et étroit avec la description de l'état de santé d'une personne****. Elle devrait en principe comprendre les données médicales, ainsi que les données financières et administratives se rapportant à la santé* ».

Dès lors, le contraste est fort entre la directive 2011/24/UE ainsi éclairée [376], et le règlement 2016/679, **textes pourtant adoptés de façon rapprochée**. Mais cela s'explique par le fait que l'interprétation en apparence large préconisée par le CEPD (en fait, pas si large que cela, puisque la construction « par inférence » en est absente), **ne pouvait être que bridée par l'objet de la directive de 2011 :** l'organisation des soins transfrontaliers supposait la transmission de données **au sein d'un dossier**, dont elles se sont depuis évadées.

Après le Règlement récent et en apparence complet de 2016, **on pourrait certes imaginer qu'il n'y a plus beaucoup à dire au fond,** sur la notion de « donnée de santé ». Mais nous avons noté que le règlement de 2016 est, en ce qui concerne la donnée de santé en retrait, au regard de l'avis formulé en 2015 par le groupe de travail de l'article 29 [377] ; et que la proposition de règlement EESD en 2022 a déjà prévu de le dépasser avec une notion large de « *donnée de santé électronique* » [378] (mais qui se trouve englobée dans la définition de 2016, celle-ci étant on l'a vu tautologique [379]).

L**a question des algorithmes dits d'« intelligence artificielle » et la construction de données par inférence,** pourraient à nouveau solliciter sa création doctrinale.

---

[376] Directive n° 2011/24/UE du 9 mars 2011 préc. relative à l'application des droits des patients en matière de soins de santé transfrontaliers.

[377] Article 29 Data Protection Working Party, Lettre du 5 février 2015, voir surtout son « ANNEX - Health Data in Apps and Devices ». L'annexe n'est pas paginée, mais c'est en page 5.

[378] La lettre est en anglais. Nous reprenons littéralement la traduction de J.B. Malafosse, qui la cite en bas de page de la page 5 du rapport de présentation visant à mettre à jour la recommandation n° R (97) 5 du Conseil de l'Europe sur la protection des données médicales, qt qui préconisait l'abandon du terme « information médicale » au profit du terme « donnée de santé », cf. notre introduction.

[379] Introduction, et Fasc 8-10 « Données de Santé » JCL LexisNexis, Traité de droit pharmaceutique Litec 2023.

§2. LA DEFINITION DES « DONNEES CONCERNANT LA SANTE » PAR D'AUTRES ACTES DE DROIT DERIVE

Annoncés par le RGPD même, deux outils de droit dérivés ont été adoptés, qui recouvrent également le traitement des données à caractère personnel dans l'Union européenne. Or, ces deux textes vont porter leur propre définition de la « donnée concernant la santé », **sans renvoyer au RGPD sur ce point**.

Il s'agit de normes de droit dérivé applicables d'une part en matière judiciaire (A), d'autre part aux personnels employés par les institutions européennes mêmes (B).

A. AUTONOMIE DE LA DIRECTIVE 2016/780 A L'EGARD DU RGPD 2016/679

Le règlement 2016/679 met en exergue dans son considérant n° 19, le fait **qu'il ne devrait pas s'appliquer** à la protection « *des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données* ».

Ainsi, cette matière **fait l'objet d'un acte juridique spécifique de l'Union**, donc un droit spécial. Voyons son champ (1) puis son contenu (2) à cet égard.

1. Le champ du droit spécial porté par la directive 2016/780

La directive 2016/780 du Parlement et du Conseil du 27 avril 2016 (adoptée le même jour que le règlement 2016/679) est titrée « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données* ». Elle **abroge un texte dans ce champ, lequel n'était pas une directive, mais une décision du Conseil** [380].

[380] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO L 350 du 30.12.2008, p. 60).

Son considérant n° 4 motive le besoin de faciliter / de sécuriser le « *libre flux (sic)* » des données à caractère personnel entre les autorités compétentes, essentiellement ici étatiques, mais pas seulement. Le but est la prévention et la détection d'infractions pénales, la conduite d'enquêtes et la mise en œuvre de poursuites en la matière, ou encore l'exécution de sanctions pénales.
Ces activités recouvrent la **protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union** (compétences régaliennes), **le transfert de telles données vers des pays tiers** (coopérations judiciaires) **et à des organisations internationales** (par exemple INTERPOL), « *tout en assurant un niveau élevé de protection des données à caractère personnel* ».

Par un niveau élevé et homogène de protection, le but est de « *garantir l'efficacité de la coopération judiciaire en matière pénale et de la coopération policière* » (considérant n°7). Ce but avait été reconnu en 2007 dans la (courte) déclaration n°21 sur la protection des données à caractère personnel dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière [381], à l'origine de la décision cadre de 2008.

Toutefois, **dans le cas où certaines de ces activités seraient externalisées** vers d'autres entités de droit public voire de droit privé habilitées selon le droit national [382], **le droit commun du Règlement 2016/679 s'applique, du moins pour les traitements dont les finalités ne sont pas celles spécifiques couvertes par la directive 2016/780 ;** dans l'hypothèse sous-traitant privé, cela pourrait conduire à l'application d'un double régime.

En outre, la directive 2016/680 ne doit pas s'appliquer au traitement de données à caractère personnel effectué dans le cadre d'une activité qui ne relèvent pas du champ d'application du droit de l'Union. **Cela en exclut expressément les « *activités relatives à la sécurité nationale, les activités des agences ou des services responsables des questions de sécurité nationale* *et le traitement de données à caractère personnel par les États membres dans le cadre d'activités relevant du champ d'application du titre V, chapitre 2, du traité sur l'Union européenne* »** (considérant n° 14, directive 2016/680).

[381] Annexée à l'acte final de la Conférence intergouvernementale qui a adopté le traité de Lisbonne signé le 13 déc. 2007. JOUE 26.10.2012, C 326/337, voir p 347.
[382] Le considérant n° 11 souligne que « Les autorités compétentes en question peuvent comprendre non seulement les autorités publiques telles que les autorités judiciaires, la police ou d'autres autorités répressives mais aussi tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique aux fins de la présente directive. »

2. Les « données concernant la santé » dans la directive 2016/680

Il n'est pas lieu ici de détailler le contenu de cette directive, dont nous venons de souligner l'autonomie à l'égard du RGPD. **Autonomie, à quel point ?**

Le considérant n° 24 de la Directive 2016/780 a le même objet que le considérant n° 35 du Règlement 2016/780. Il formule la pétition quant à la protection aux « données concernant la santé » **de façon strictement identique**. L'article 3.14 de la Directive 2016/780 présente une définition des « données concernant la santé » également strictement identique, à celle portée par l'article 4.15 du Règlement 2016/679. **Quel intérêt ici ?**

Adoptés le même jour, le Règlement 2016/679 cite la Directive 2016/680, et inversement. Sur ce point, on peut bien dire que le Règlement constitue un règlement général ; mais pas un droit commun : la directive 2016/680 n'y renvoie pour aucune de ses définitions, **même lorsqu'elles portent sur les mêmes termes.**

Nous venons de constater l'identité de l'énoncé, qui marque en fait une double autonomie : juridique, car **même si la définition est la même, le but du texte est différent, et porté par une directive à transposer (non par un règlement d'application immédiate)** ; matérielle, car bien que la définition soit la même, il fallait que le corpus de la Directive 2016/680 fût formellement autonome, pour des raisons que l'on pourrait dire d'ergonomie intellectuelle.

Mais le fait qu'il s'agisse de la même définition des « données concernant la santé », pour les mêmes implications, bien que dans des environnements différents, **ne devrait pas conduire à une divergences d'interprétation jurisprudentielle, au moins au niveau européen** (la matière pénale peut conduire à des analyses d'une nature différente, de la matière du droit commun ; au moins à des analyses approfondies, on l'a vu, avec la jurisprudence en 2012 du Conseil d'Etat, en environnement carcéral –mais il s'agissait de la question du partage avec l'administration pénitentiaire des données détenues par des professionnels de santé).

Or, **on ne trouve pas dans la directive 2016/680, de dispositions enjoignant une homogénéité d'interprétation jurisprudentielle par la CJUE**, en contraste du règlement 2018/1725 qui dans son considérant n°5, le prévoit expressément (*infra*).

B. AUTONOMIE DU REGLEMENT 2018/1725 A L'EGARD DU REGLEMENT 2016/679

Le règlement 2016/679 met en exergue dans son considérant n° 17, le fait qu'il n'a pas vocation à s'appliquer « *au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union* » (considérant n° 17), lequel échappe au droit commun.

Il était déjà l'objet d'un droit antérieur autonome (2001), actualisé seulement en 2018 malgré cette pétition : il convient « *après l'adoption du présent règlement* (i.e. 2016/679)*, d'apporter les adaptations nécessaires au règlement (CE) n° 45/2001 de manière à ce que celles-ci s'appliquent* ***en même temps que le présent règlement*** *»*, ce qui ne sera pas le cas.

1. Le champ du droit spécial porté par le règlement 2018/725

Le règlement 2018/1725 du Parlement européen et du Conseil a été adopté le 23 octobre 2018. Il est (son libellé) « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données ». Les personnes physiques **dont les données à caractère personnel sont traitées par les institutions, organes et organismes de l'Union échappent donc au champ du règlement 2016/679**.

Cette situation n'est pas nouvelle : **le règlement de 2018 ne constitue pas une dérogation au règlement (UE) 2016/679 :** ce dernier signalait dans son considérant n°17, l'autonomie du traitement de telles données. Celle-ci était l'objet du règlement (CE) n° 45/2001, et de la décision n° 1247/2002/CE.

Ainsi, le règlement (CE) n° 45/2001 du Parlement européen et du Conseil, lequel « *donne aux personnes physiques des droits juridiquement protégés* », définit les obligations des responsables du traitement au sein des institutions et organes communautaires en matière de traitement des données. Il a été adapté par le règlement 2016/679 « *en vue de garantir un cadre de protection des données solide et cohérent dans l'Union et permettre que celui-ci s'applique en parallèle avec le règlement (UE) 2016/679* ».

Ceci sachant qu'il « *est dans l'intérêt d'une approche cohérente (...) d'aligner autant que possible les règles en matière de protection des données pour les institutions, organes et organismes de l'Union* ***sur les règles en matière de protection des données adoptées pour le secteur public dans les États membres*** » (considérant n° 5, règlement 2018/1725).

2. l'identité des « données concernant la santé » dans le règlement n° 2018/725

Ces données sont définies dans l'article 3.19 du règlement n° 2018/1725, de façon identique à l'article 3.14 du règlement n° 2016/679 (l'emploi du mot « fourniture », plutôt que « prestation » de soins de santé relève de la traduction, et ne change rien en droit - que la prestation soit matérielle ou dématérialisée, comme par exemple les "thérapies digitales" traduction devenue dominante de *digital therapies*, en fait les thérapies numériques, comme le souligne la Haute Autorité de santé [383]).

A la différence du règlement n° 2016/769 et de la directive n° 2016/680, le règlement n°2018/1725 **ne contient aucun considérant qui, en amont de sa définition, présente les « données concernant la santé ».** Si cette emphase était nécessaire dans la directive n°2016/680, laquelle traite de la matière judiciaire et carcérale, avec une certaine autonomie d'organisation etc., **elle n'est pas nécessaire dans le règlement 2018/1725.**

En effet, ce règlement de 2018 spécifie que les deux ensembles de dispositions « *devraient, conformément à la jurisprudence de la (CJUE),* ***être interprétées de manière homogène, notamment en raison du fait que le régime du présent règlement devrait être compris comme étant équivalent*** *au régime du règlement (UE) 2016/679* » (considérant n° 5, règlement n°2018/1725). L'équivalence est en tous cas formelle dans l'article 3 portant définitions : les données y sont définies à l'identique, ainsi les données génétiques (article 3 point 17), données biométriques (ibid., pt 18), et données concernant la santé (ibid., 19).

Rappelons ici qu'une telle précision dans le considérant n°5, qui vise expressément l'homogénéité d'interprétation**, est absente de la directive n°2016/680**, dont on ne sait si elle serait interprétée de la même manière, du fait de son objet spécifique. **Mais son silence ne devrait selon nous pas conduire à un écart** dans l'interprétation jurisprudentielle.

[383] HAS, Rapport d'analyse prospective 2019 - Numérique : quelle (R)évolution ? site HAS.

Enfin, cette **approche unifiée est confirmée par la proposition de règlement en 2022**, lequel vise l'institution d'un espace européen des données de santé [384]. Dans son considérant n° 4, il postule en effet que « *les références aux dispositions du règlement (UE) 2016/679 doivent être considérées comme des références aux dispositions correspondantes du règlement (UE) 2018/1725 pour les institutions et organes de l'Union,* ***le cas échéant*** (*sic*) ».

Mais nous allons voir que la proposition de règlement de 2022 va, en fait si non en droit, bien plus loin : elle va acter l'extension de la notion de « donnée de santé », par l'évolution du mode de sa définition : du contenu, au contexte. **Cette intégration d'éléments invoqués en 2015 par le groupe de travail « de l'article 29 », mais non retenus dans le RGDP, nous semble étendre la catégorie « donnée de santé » au-delà de sa définition de 2016.**

SYNTHESE P1T1C2

Ce second chapitre du Titre I **« définition de la donnée de santé, du contour au contenu »** était le cadre de restitution de nos observations, qui deviennent prospectives, de la dynamique de la notion de « donnée de santé » depuis l'adoption du droit européen en 2016.

***** Dans une première section, nous relevons la première définition positive et autonome d'une « donnée de santé », laquelle est distinguée des données génétique et biométrique, dont le vecteur est pourtant un règlement européen dédié à la protection générale des données personnelles. Cette définition est tautologique pour être accueillante, du fait de la dynamique du secteur et surtout de contours que l'on a vu difficiles à tracer. Au-delà de cet objet de protection intrinsèque des droits individuels, ce règlement préparait en 2016 une construction normative beaucoup plus vaste, qui depuis 2022 accompagne la « transformation numérique » de l'Union européenne : la définition positive des catégories de données est un préalable à la définition et régulation des stratégies sectorielles de l'Union et des marchés numériques, que les services proposés soient réputés « essentiels » ou non.

[384] Proposition de Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final 2022/0140(COD). Développé en Partie II, titre II.

* Dans une seconde section, nous relevons que cette définition de la donnée de santé en droit européen, qui n'a pas connu de transposition dans le droit de la santé national (où elle transposition n'était pas requise), offre un droit commun de référence. Le but est d'unifier en théorie les pratiques de régulation fondées sur cette nouvelle catégorie du droit, au nom d'un « principe d'homogénéité d'interprétation jurisprudentielle » qu'il met en exergue. Mais l'on perçoit par l'analyse déjà un *hiatus* entre la définition normative posée en 2016, et des considérants du même règlement : son ambition annonçaient une extension considérable, acquise depuis 2022, de la notion de donnée de santé en droit européen. Cela explique la dimension tautologique de la définition de la donnée de santé comme information relative à la santé : elle vise à couvrir tout ce qui pourrait y être aspiré.

SYNTHESE P1T1

La notion de « donnée de santé » ne possède de contenu positif que depuis récemment. De façon contre-intuitive, ce contenu n'a pas été défini par le droit de la santé, mais par les textes nationaux et européens qui traitaient des droits fondamentaux pour la protection des libertés et la régulation des transferts de données personnelles. Même le développement initial de l'informatique en santé, n'a pas requis que le droit de la santé s'en emparât. Il faut en droit français attendre 2002 pour tracer des contours de la notion.

C'est d'abord le résultat d'un raisonnement par inférence du champ du secret, qui constitue une cloche protectrice sous laquelle les informations n'apparaissent différenciées que selon le besoin d'en connaître. De pure obligation à la charge des professionnels, le secret devient aussi un droit au bénéfice du patient « usager » du système de santé.

Son champ s'étend alors des « informations médicales », aux informations « concernant la personne ». En outre, la transformation des modes d'exercice professionnels conduit de façon croissante à redéfinir le régime des collaborations en secteur sanitaire et médico-social à son profit, marquant une transformation de l'environnement qui appelle une évolution du droit : le paramétrage du besoin de connaître l'information, dans le contexte d'échange / partage.

Les pratiques, responsabilités et techniques ne s'accommodent ainsi plus de la vision historique dominante en silo de la production, de l'utilisation et de la protection de l'information en santé, souvent accaparée par des producteurs parfois ombrageux. Elles supposent un paramétrage plus fin de l'information et de sa distribution dans le système. Or,

en précisant et resserrant les contours de la notion, ce paramétrage affiné rapproche de son contenu.

A une approche indistincte de l'information, sous une cloche protectrice donc de mieux en mieux cernée, succède ainsi sous l'effet du droit européen, une définition analytique des données : elles sont devenues détachables d'une relation de soins, qui s'est multi-latéralisée et se dématérialise. Elles vont s'inscrire dans une dynamique internationale.

TITRE 2. LA DEFINITION DE LA NOTION DE « DONNEES DE SANTE » : DU CONTENU, AU CONTEXTE

Dans le Titre 1, nous avons relevé la dynamique du tracé d'abord tâtonnant des contours de la notion de « donnée de santé », puis la définition graduelle d'un contenu positif. Depuis 2016, la « *donnée de santé* » **est qualifiée *per se* au plan européen donc national** – c'est-à-dire distinctement d'une relation de soins ou d'un dossier de santé, dont elle s'est détachée. En 2022, la proposition de règlement EEDS promeut son extension normative **au-delà de l'ambition historique mais déjà croissante, des « considérants » des textes antérieurs**.

Dans ce sillage, nous restituons dans ce titre II nos observations d'une autre dynamique : elle intéresse le **contenu même de la notion**. Elle s'exprime d'abord hors de la recherche biomédicale, en pratiques des soins et suivi des personnes (chapitre I) ; mais aussi dans les contextes de la recherche et des utilisations secondaires des données, qui contribuent à sa définition (chapitre II).

Nous verrons que ces nouvelles déclinaisons, qui apparaissent au gré d'applications nouvelles, ne s'emboîtent parfois qu'imparfaitement ; que la catégorie dérivée des « utilisations secondaires » va paradoxalement nourrir celle définie par les utilisations « primaires », *infra* ; que **des données « non santé » sont aspirées dans le champ des données « de santé »**, avec l'effet d'ébranler des catégories juridiques qui semblaient tout juste se fixer [385].

CHAPITRE I. DYNAMIQUE HORS CADRE DE LA RECHERCHE BIOMEDICALE

Nos recherches dans ce champ (dont nous avions publié une première étape début 2018), nous ont conduit à **ne pas retenir les distinctions classiques** présentées en introduction. Nous avons distingué deux approches de la qualification de la « donnée de santé », distinction depuis confortée par la dynamique normative française et européenne. Nous reprenons notre distinction ici, étayée par un développement original ; ce dernier mobilisera les constats que nous avons posés dans le titre I, et les trouvera amplifiés depuis par la pratique.

[385] Nous reprenons ici avec sa permission, des éléments originaux de « Notion de donnée de santé », JCL, Fasc 8-10 n°48 et suiv., Traité de droit pharmaceutique, Litec, Lexis Nexis 2023.

En effet, il est possible de distinguer la « donnée de santé » d'autres données, **selon l'origine organique de leur production** ; c'est-à-dire émanant de **l'activité du système de santé** telle que définie dans le Code de la Santé publique (CSP). Ce critère organique conduit d'office à une donnée de santé « par qualification de la loi », laquelle n'est pas discutable (section I).

Mais toutes les données « relatives à la santé » ne trouvent pas pour origine l'activité du/des systèmes de santé ainsi entendu. Des « zones grises » ou angle-morts sont apparus [386]. Ainsi, des données sont produites péri-système, **sans intention ni nécessairement application médicale, mais avec potentiellement une signification médicale** ; nous les avions appelées données de santé « par destination » [387]. Or, ces dernières sont en fort développement du fait de l'hybridation des outils et pratiques (section II).

SECTION I. LES DONNEES DE SANTE « PAR QUALIFICATION DE LA LOI »

Cette qualification des données découle de la simple application de la loi française **qui avait déterminé les conditions initiales** de leur production. Ce point nous conduit à relever la diversité des acteurs/contextes de production de données qui, même dans le cas de violations de la loi, peuvent sans ambiguïté être considérées être des « *données de santé* », (§1).

Mais la même qualification découle de **leur rattachement juridique à la catégorie des « données de santé »,** par attraction dans des « espaces numériques » récemment créés par le législateur dans le Code de la santé publique.
Or, cela n'est pas redondant avec ce qui précède. Nous constaterons que toutes les données « de santé » produites par le système de santé, n'y sont pas attirées ; que, en outre et surtout, des données vont y être attirées à compter de 2022, **alors qu'elles ne relèvent pas d'une production native par le système de santé** (§2).

[386] Dès 2016, la Haute Autorité de Santé invoque la notion de « zone grise » in « Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth) » ; également Conseil d'Etat, in « Révision de la loi de bioéthique : quelles options pour demain », Rapport et études, 28 juin 2018, pt. 197. Cette acception à bien distinguer de l'acception de « *grey area* » au sens de Adams J, Hillier-Brown FC, Moore HJ et al. « Searching and synthesising 'grey literature' and 'grey information' in public health: critical reflections on three case studies ». Syst Rev. 2016 Sep 29;5(1):164, sachant que la notion de « zone grise » au sens français n'y est pas connue aux Etats-Unis, du fait des règles fédérales qui ne tracent pas un tel angle mort.
[387] Nous verrons que la CNIL a depuis également recouru à la notion de donnée de santé « par destination », mais pour une signification différente de celle que nous avions proposée, et qui ne la recouvre pas, *infra*.

§1. QUALIFICATION DES DONNEES SELON LEURS CONTEXTES DE PRODUCTION / DE PARTAGE

En droit français, **le contexte de production ou de partage est le critère historique** de qualification des données : nous avons vu comment le champ des « *données de santé* » avaient initialement été inféré du champ du « *secret de santé* », avant le tracé autonome de ses contours, *infra*. Dans ce contexte, le Conseil d'Etat a en 2018 distingué selon que les données « relatives à la santé » étaient recueillies dans, ou hors du cadre d'une relation de soins : cela le conduit alors à esquisser une distinction entre **donnée publique, ou privée**.

Mais nous n'avons pas retenu cette distinction ici, car elle n'apparaît qu'une esquisse dans un propos incident ; elle n'est pas, en l'état, à l'origine d'une construction doctrinale ni jurisprudentielle. Elle paraît inspirée par la vocation des données **à être ou non rattachées à la plateforme publique** des données de santé (*infra*) ; or, ceci intéresse **le régime d'accès** notamment pour les « utilisations secondaire », lequel n'est pas l'objet de notre recherche.

Dès lors, tenons nous en ici à l'existence d'une relation de soins. Celle-ci **semble un critère net de qualification des « données de santé », mais à l'examen, s'avérera ne pas l'être.** Nous proposons en effet de distinguer les contextes de production des données de santé « par qualification de la loi » selon deux critères légaux.

Le premier est un **critère organique** : la loi a pu qualifier un acteur, un établissement une technologie *es* qualités – et par induction, la nature des données qu'ils produisent (A). Le second est un **critère matériel**, car hors de notre système de santé, il est d'autres circonstances de production de données, qui ne les qualifient pas moins « de santé » (B).

A. LE CRITERE « ORGANIQUE » DE QUALIFICATION DES DONNEES DE SANTE

Par « critère organique », nous entendons ici le producteur (professionnel, établissement ou technologie) de la donnée quel qu'il soit, dès lors qu'il est défini et opère dans le cadre d'activités **définies et organisées par la loi** (1).
En miroir, cela nous conduit à nous considérer que relève aussi d'une production organique, mais cette fois négativement, la production de données lors d'activités qui sont **expressément qualifiées** d'illégales par le Code de la santé publique (2).

1. La détermination positive par la loi d'activités génératrices de données de santé

Cette section sera courte : on y rappelle le principe (a) et les applications déjà évoqués (b), avant de relever l'existence implicite d'un tel critère dans les textes européen en vigueur (c).

a. le principe de soumission organique au secret renforcé

Pour rappel, la loi dispose depuis 2002 que « *Toute personne prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins* ***dont les conditions d'exercice ou les activités sont régies par le présent code,*** *le service de santé des armées, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 (CASF) a droit au respect de sa vie privée et du secret des informations la concernant* » (… Ce secret…) « *s'impose à tous les professionnels intervenant* ***dans le système de santé*** » (article L. 1110-4 CSP).

On a vu la définition des « données de santé » par inférence du secret, bien avant leur conceptualisation en soi, *supra*. Formulée comme un droit du patient, cette obligation **est par nature indifférente** aux circonstances particulières d'exercice, en secteur public ou privé, ambulatoire ou hospitalier, à but lucratif ou non. Elle est tout autant indifférente au statut et l'implication de la personne prise en charge (patient, ou sujet bien portant pour la prévention).

Les définitions des exercices sont disséminées dans différents Codes (CASP et CASF, mais également Code de la sécurité sociale, CSS, pour les Praticiens-Conseils, ce que n'évoque pas l'article L. 1110-4 CSP). Cet **éclatement fonctionnel n'altère pas la qualification unitaire de la donnée protégée** : elle relève d'une production soumise au secret « organique ».

b. applications organiques de la soumission au secret renforcé des données

* Si l'on s'en tient ici au CSP, partie législative, IVe partie, le Livre 1er traite des « *professions médicales* » (articles L. 4111-1 CSP à L. 4163-11 CSP), lesquelles recouvrent les professions de médecin, de chirurgien dentiste, de sage femme ; le livre II « *Professions de la pharmacie et de la physique médicale* » (L. 4211-1 à L. 4252-3 CSP), recouvre les professions de pharmacien, de préparateur en pharmacie et de préparateur en pharmacie hospitalière, de physicien médical ; le Livre III (L. 4301-1 à L. 4394-4 CSP) organise les

professions d'« *auxiliaires médicaux, aides-soignants, auxiliaires de puériculture, ambulanciers et assistants dentaires* », lesquelles recouvrent les professions d'infirmiers, masseur-kinésithérapeutes, pédicure podologues, ergothérapeutes, psychomotriciens, orthophonistes, orthoptistes, audioprothésistes, opticien lunetiers, prothésistes et orthésistes pour l'appareillage des personnes handicapées, diététicien.

En tant que régis par le CSP, tous sont débiteurs de l'obligation, **quand bien même l'organisation de leur activité propre ne contiendrait pas** d'énoncé ni sanction spécifiques.

* Dans la VIe partie, sont définis les établissements et services de santé. Il est auparavant rappelé au titre de la Ière partie que « *Les établissements sont tenus de protéger la confidentialité des informations qu'ils détiennent sur les personnes qu'ils accueillent* (...) » (L. 1112-1-III CSP). La notion de secret couvrant les données, entendue comme « secret médical », n'apparaît ensuite que dans l'article L. 6113-7 CSP, qui l'impose dans la mise en oeuvre de systèmes d'information. **Le secret est donc également à la charge de l'établissement,** et s'impose à l'autorité qui organise la mise en relation des traitements [388].

En matière de compromission de données, il n'existe pas de dispositions équivalentes à celles réunies dans le Chapitre III "*Responsabilité des établissements à l'égard des biens des personnes accueillies* (L. 113-1 à L. 113-10)".

* En tout état de cause, les professionnels mentionnés à la IVème partie du CSP, tout comme les services et établissements à la VIème partie « *ne sont responsables des conséquences dommageables d'actes de prévention, de diagnostic ou de soins qu'en cas de faute* (...) » (L. 1142-1 CSP). Cet article vise les conséquences des actes, non la compromission éventuelle des données. Celle ci **ne pourrait-elle résulter que d'une faute**, au sens du manquement à une obligation prédéterminée ? il n'existe pas de précédent tranché par le Conseil d'Etat [389]. En revanche, on examinera en Partie II les **problèmes soulevés en droit par la cybersécurité** et l'assurabilité de risques non accidentels.

---

[388] Dernièrement, CE, 10ème - 9ème ch. réunies, 27/03/2020, n° 431350. Il s'agissait d'une adjonction par décret, à la finalité principale préexistante de suivi administratif des personnes faisant l'objet de soins psychiatriques sans consentement, une *"autre finalité permettant l'information du représentant de l'Etat sur l'admission des personnes en soins psychiatriques sans consentement, nécessaire aux fins de prévention de la radicalisation à caractère terroriste"*.
En l'occurrence, il n'est pas porté atteinte au secret garanti par les dispositions de l'article L. 1110-4 CSP.

[389] Conseil d'Etat, *L'engagement de la responsabilité des hôpitaux publics* (dossier thématique), janv. 2015. Il n'existe pas de jurisprudence rapportant une telle hypothèse (site du Conseil d'Etat, vérifié en 2023).

c. Un critère organique implicitement présent dans le RGPD de 2016 ?

Certes, le RGPD ne traite pas du champ du secret, mais de la protection des données personnelles [390]. Toutefois, il est intéressant de relever dès ici son apport, du fait du lien que nous avons exploré entre « donnée personnelle de santé » et « secret professionnel de santé ».

Le RGPD entend par « donnée de santé » dans son considérant n° 35, « *toute information concernant, par exemple (...) une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée,* ***indépendamment de sa source, qu'elle provienne par exemple*** *d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic* in vitro ».
Or, ce qui est ici frappant, n'est pas que ce considérant n°35 mette en exergue l'indépendance de l'information à l'égard de la source et la diversité potentielle de celles-ci, mais qu'en guise exemples, il ne cite pour sources que des professionnels, établissements ou technologies de santé **qualifiés *per se*** (en France, dans le CSP) – **c'est-à dire des sources organiques**.

Cela contraste avec le contenu sensiblement plus large de la proposition de règlement EESD, présentée en mai 2022 : son considérant n° 5 dispose (à la date de notre rédaction) que « *ces données de santé électroniques à caractère personnel* ***pourraient inclure*** *des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de services de soins de santé (...)* ***ainsi que des données sur des facteurs déterminants pour la santé, tels que*** *le comportement, les facteurs environnementaux, les influences physiques, les soins médicaux et les facteurs sociaux ou éducatifs* » [391]. Le champ des sources est ici élargi **bien au-delà du système de santé.**

Ainsi voyons nous ici déjà une tendance d'attraction, dans le contenu initial de la notion de « donnée de santé », des éléments de contexte (*infra*).

[390] Règlement. (UE) 2016/679, 27 avr. 2016 préc., cons. 35
[391] Proposition de Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022)197 final.

2. Une détermination de la « donnée de santé » indifférente à la légalité de l'exercice ?

Restons dans le critère organique : l'éventualité d'un exercice en santé qualifié « *d'illégal* » (a), n'affecte selon nous pas la qualification de la donnée qui en résulterait (b). Cela, même si la **vocation d'une telle donnée est la destruction** (après épuisement, le cas échéant, des contentieux en matière pénale, disciplinaire, civile, administrative [392]) : elle n'aurait pas vocation à abonder le système national des données de santé.

a. Hypothèses d'illégalité d'exercice

*** La notion d'« exercice illégal » vise la sanction pénale** de l'infraction aux règles organisant les activités sensibles (notamment la santé). En effet, ces activités requièrent des garanties de qualification, compétence, moralité, d'identification, localisation, d'assurance de responsabilité etc. Parfois, les règles visent à prévenir aussi l'empiètement entre professions : l'exercice illégal sert aussi à la régulation de la compétition interprofessionnelle.

Ainsi, il n'est pas de « Profession de santé » définie dans la IVème partie du CSP (*supra*), dont le périmètre d'activité ne soit pas exclusif ; ceci hors, dérogations, tâches ponctuelles et coopérations inter-professionnelles ; selon les critères explicitement posés par la loi. Dès lors, leurs **monopoles respectifs sont protégés par l'énoncé des conditions de légalité** de chacun et, en miroir, par la sanction pénale de son exercice illégal.

En outre, dans l'hypothèse de soins transfrontaliers organisés par la Directive 2011/24, *infra*, l'Etat membre d'affiliation du patient (i.e. l'Etat qui couvrira tout ou partie des frais engagés) peut vouloir confirmation que ces soins seront ou auront été prodigués par un professionnel de santé « *exerçant en toute légalité* ». C**e critère n'induit pas que toute prestation conforme au droit local soit éligible** au paiement par l'Etat d'affiliation : ceux-ci peuvent poser des conditions préalables de prise en charge ; or, nous avons vu que ces conditions recouperont, en France, les seules prestations délivrées, et référencées, au sein du système de santé.

*** L' « usurpation de titre » dans le Code de la santé publique**, est une incrimination récente (2002) et distincte dans le CSP : un titre peut être usurpé (créer une apparence), sans que l'activité correspondante soit pour autant pratiquée (sans donc « exercice illégal »).

[392] La donnée en effet peut servir à la preuve de l'exercice illégal, et au fondement de réparation d'un dommage.

Consacré par l'article 433-17 du Code pénal, ce principe sanctionne « ***L'usage, sans droit, d'un titre*** *attaché à une profession réglementée par l'autorité publique* (…) ». Le législateur a cru bon de créer des dispositions spécifiques pour chacune des professions concernées dans le CSP : pour médecins et assimilés (L. 4162-1 [393]), pharmaciens (L. 4223-2[394]), préparateurs en pharmacie (L. 4243-2[395]), infirmiers (L. 4314-5 [396]), ce incluant les personnes morales support. On notera que la protection du titre de « pharmacien » depuis 2002, a conduit certains acteurs à un déport vers **l'invocation du titre de « docteur en pharmacie » dans une fonction non organique** du système de santé : cette pratique est licite, si le diplôme est détenu [397].

Certes, les données issues d'activités **« non santé »** menées par une personne usant indûment d'un « titre de santé », ne sont pas des données de santé ; **on retrouve là le critère organique**.
Mais l'éventualité de confidences (sans qu'un avis ne soit demandé ou rendu, sans direction de soins ni suivi de la personne) peut être problématique : l'usurpation du titre fait bénéficier celui qui s'en prévaut d'une aura de moralité professionnelle, donc d'une **présomption de confidentialité**. En pratique, elle peut donc susciter une confiance indue.

b. conséquences sur la qualification des données

L'article L. 1110-4 CSP invoque la « *prise en charge par un professionnel de santé, un établissement ou service, un professionnel ou organisme concourant à la prévention ou aux soins* ***dont les conditions d'exercice ou les activités sont régies par le présent code*** *(…) ».*

En l'absence de contentieux connu qui réfute notre hypothèse, nous ne voyons pas que l'exercice illégal d'une profession de santé **ait une quelconque incidence sur la qualification de la donnée** qui en résulterait : la donnée doit être protégée, parce que recueillie **au titre de l'activité prétendue** ; elle n'est pas moins sensible, **que cette activité**

[393] Modifié par Ordonnance n°2005-1040 du 26 août 2005. Couvre l'usage sans droit de la qualité de médecin, de chirurgien-dentiste ou de sage-femme ou d'un diplôme, certificat ou autre titre légalement requis pour l'exercice de ces professions.
[394] Modifié par la loi 2011-525 du 17 mai 2011.
[395] Modifié par la loi n° 2009-879 du 21 juill. 2009.
[396] Modifié par la loi n° 2009-526 du 12 mai 2009. Nous citons ces textes modificatifs, pour montrer par leur dispersion dans le temps que la question n'a jamais fait l'objet d'une approche systémique globale.
[397] Traité de droit pharmaceutique, Fascicule Monopole, n°11-00, Litec 2021.

soit légale ou pas ; qu'elle **suppose ou non l'accès frauduleux** à un système d'information traitant des données de santé, avec ou sans carte de professionnel de santé [398].

Ceci permet d'ajouter un chef de poursuite pénale, en cas de capture de données sensibles par des opérateurs illégitimes (il ne s'agirait pas d'un « vol ») : **le recel de données obtenues *sans qu'elles aient été volées*** (art. 321-1 CP) [399] ; cela sans pour autant qu'il s'agisse d'une atteinte à un système automatisé de traitement des données (art. 323-1 à 323-8 CP), *infra* [400]. Cela est distinct de la vente, pénalement sanctionnée (article L. 1111-8 – VII, CSP).

Certes, la sanction du « secret professionnel » (226-13 CP) ne semble alors pas possible. Pour rappel, la loi sanctionne la « *révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire (…)* ». **Mais pourrait-on jouer d'une théorie de l'apparence** (d'état de profession, de fonction ou de mission) pour la fonder ?

Dans un autre domaine, la Cour de cassation s'est en 2020 prononcée quant au secret de l'enquête ou de l'instruction en matière pénale. En l'occurrence, elle juge que « *constitue une violation du secret professionnel, la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession,* ***soit en raison d'une fonction ou d'une mission temporaire, quelles que soient la portée et la valeur de celle-ci*** » [401].

Certes, il serait ambitieux d'extrapoler cette solution à la violation du secret par une personne **dont l'activité / la fonction serait illégale, donc sans portée et de valeur nulle**. Mais les juridictions sont souveraines. En outre, la question pourrait en pratique se poser, du fait de la multiplication des opportunités de confusions, orchestrées ou non, à l'ère des plateformes, blogs, réseaux sociaux et messageries numérique intéressant la santé [402].

---

[398] La carte CPS (article L.1110-4 CSP) permet seule l'accès aux données de santé à caractère personnel, notamment dans le cadre du partage de l'information médicale. Elle est inscrite dans le référentiel d'authentification de la Politique Générale de Sécurité des systèmes d'Information de Santé (PGSSI-S).

[399] Article 321-1 CP : « Le recel est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, ***en sachant que cette chose provient d'un crime ou d'un délit*** (…) », c'est-à-dire qu'elle qu'en soit l'incrimination.

[400] Code pénal, partie législative, livre III, titre II, Chapitre III : « *Des atteintes aux systèmes de traitement automatisé de données* » (articles 323-1 à 323-8) CP.

[401] Crim., 24 mars 2020, n° 19-80.909, (P).

[402] Car alors la personne y a volontairement rendu publique une information relative à santé ; en contraste dans les autres cas, une attente légitime de sécurité a pu être suscitée par les apparences de tunnel protégé provoquant fallacieusement un « colloque singulier ».

Dans un autre champ, la société Doctolib a du en 2022 sous la pression publique (sans qu'elle ait violé le droit), écarter de son site des acteurs **qui ne relevaient pas des « Professions de santé »** selon le CSP ; mais qui y proposaient des services « alternatifs » de santé, s'entourant ainsi d'un halo de crédibilité quasi-institutionnelle. Cela ne pouvait qu'abuser les patients-consommateurs, et ulcérer les professionnels définis par le CSP.

En outre, **l'expression de besoins** par les utilisateurs en recherche de soins conventionnels ou non y a, sur plusieurs points critiques, été recueilli dans des conditions non conformes : cela vaut en mai 2023 à cette société, une condamnation par la CNIL distinctement de ce qui précède, et qui n'était pas répréhensible en droit [403].

B. UN CRITERE « MATERIEL » DE QUALIFICATION NON AMBIGUË DES DONNEES ?

Le critère matériel se distingue ici du critère organique, en ce que l'action **n'est pas le fait d'une profession ou d'un établissement de santé au sens du CSP** qui, par état ou par profession, est amenée à générer, partager et/ou protéger des données de santé au sens large.

La « fonction » / « mission » même temporaire pourrait certes être considérée comme impliquant « organiquement » son dépositaire dans le champ précité. Mais la loi les a bien distingués par la définition des acteurs, et par la restriction de l'obligation de L. 1110-4 CSP. C'est pourquoi nous en traitons au titre **non de l'organe, mais de l'action** (1) ; de même lorsqu'est en cause **l'usage autonome par le patient** de certaines technologies (2).

1. Inapplicabilité du critère organique en cas de fonction / mission temporaire

Ce critère est né du besoin de qualifier le concours, au côté de professions qui relèvent du CSP, de professionnels qui n'en relèvent pas [404], pour la conception et conduite de projets de soins ou d'accompagnement. Ainsi des équipes pluridisciplinaires **peuvent juridiquement être hétérogènes, sans que cela n'impacte l'unicité des obligations à l'égard du patient** en ce qui concerne les données et leur qualification [405].

---

[403] CNIL (communiqué de presse, 17 mai 2023), Données de santé et utilisation des cookies : Doctissimo sanctionné par une amende de 380 000 euros.

[404] Rappelons Mme M.-L. Moquet–Anger, « Professions et professionnels de santé », in Actes du colloque AFDS 2022, RDSS hors série, 99 ; mais son article ne traite pas de la question du statut de l'information et de la nature de sa protection.

[405] En ce sens, Mme P. Fombeur, « Le secret médical partagé », in Actes du colloque Santé et protection des données, La documentation française 2020, spéc. 109.

En ce sens, le décret du 20 juill. 2016 préc. identifie les professionnels qui ne sont pas Professions de santé, mais sont habilités à l'échange ou au partage d'informations [406]. Pourrait-on inférer de ce décret, que les professionnels cités sont dès lors rattachables aux sources organiques, **et par inférence générateurs de « données de santé »** ?

Selon nous, non : les sources organiques sont strictement définies par l'article L. 1110-4 I CSP, auquel le décret ne peut déroger. L'extranéité des professionnels cités par le décret de 2016 est irréductible, sauf cas exceptionnels de citation incidente dans le CSP.

Le corollaire de l'assujettissement à l'obligation de secret, au titre donc de la seule fonction ou mission temporaire ou d'une activité non CSP mais visée par lui, est que la donnée produite, collectée, ou connue de façon incidente, **participe de l'action de santé** (au sens large) à laquelle il est contribué [407].
Dès lors, toutes données liées à l'activité dans cette fenêtre de fonction ou de mission temporaire, **acquièrent la qualification de « donnée de santé ».**

En outre, l'obligation de secret **ne se limite pas à de telles équipes** : la loi couvre sans les citer, les hypothèses de services externalisés, sous-traitance, etc. pour des activités de « back-office ». Ainsi l'art. L. 1110-4 al 2. dispose que « (…) *ce secret couvre l'ensemble des informations concernant la personne* ***venues à la connaissance*** *du professionnel, de tout membre du personnel de ces établissements, services ou organismes* ***et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes*** (…) ».

Ceci sans que ces personnes n'aient en principe à connaître des données. Le cas échéant, il serait fautif qu'elles les révèlent, comme il serait **fautif en soi qu'elles aient pu y accéder.**

[406] Décret n° 2016-994 du 20 juillet 2016 relatif aux conditions d'échange et de partage d'informations entre professionnels de santé et autres professionnels des champs social et médico-social et à l'accès aux informations de santé à caractère personnel.
[407] En ce sens, Mme A. Laude, préc. in Actes du Conseil d'Etat, spéc. 113.

2. Inapplicabilité du critère organique en cas de technologie autonome

De façon croissante, les activités de soins, d'accompagnement etc. peuvent s'appuyer sur des technologies connectées. Lorsque le patient est autonomisé, **le critère de qualification est alors tiré de la technologie utilisée**, puisque celui des sources organiques définies par le CSP (professionnels de santé, établissements de santé) n'est plus applicable.

a. la technologie de santé qualifiée à fin médicale

En droit européen donc français, il n'existe qu'une qualification juridique de technologies de santé, celle de « dispositif médical » [408], laquelle qualification **suppose que son fabricant en revendique la destination**. Le « dispositif médical » est défini par l'article L. 5211-1 CSP, (modifié en 2022 sur plusieurs points que nous reverrons mais qui n'affectent pas sa définition générale [409], sachant le dispositif de diagnostic *in vitro* relève d'un droit distinct [410]).

Ainsi, par « dispositif médical », on entend « *tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article,* ***destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales mentionnées ci-après*** *(...)* ». Pour ce qui nous intéresse ici, il s'agit de la prévention, prédiction, du diagnostic, pronostic, de la surveillance, et de la « *communication d'informations au moyen d'un examen in vitro d'échantillons provenant du corps humain* (…) », **en tant que ces dispositifs génèrent des données, et sont susceptibles d'être connectés**. Nous reviendrons sur le droit européen en gestation, quant à la cyber-sécurité des DM connectés, *infra*.

Que signifie **« *destiné par le fabricant* »** ? il doit revendiquer la finalité (allégations, présentation, promotion, étiquetage, notice d'emploi, publicité etc.). Mais de façon croissante, on voit apparaître **des dénégations de qualification** (« *ceci n'est pas un dispositif médical* ») : elles ne visent pas seulement à éluder le régime spécifique de certification des DM, mais aussi à **éviter la qualification des données** qui en sont issues, *infra*.

---

[408] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.
[409] Ordonnance n° 2022-1086 du 29 juillet 2022 portant adaptation du droit.
[410] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission.

Il n'est pas lieu ici d'entrer dans ce régime de certification ; notons seulement qu'après certification, lorsque les DM sont connectés (faisant ou non appel à l'intelligence artificielle), ils font l'objet d'une évaluation par la Haute Autorité de Santé (intérêt thérapeutique dans la ou les indications revendiquées) selon une méthode spécifique [411] ; et que la CNIL **distingue le régime des logiciels et des données (non leur qualification)** selon que les données sont conservées / traitées dans le seul dispositif porté, ou transférées sur un serveur distant.

b. la condition de l'autonomie du recours à la technologie

* L'hypothèse ici pertinente, est celle d'une mise en œuvre de la technologie **par le patient même**. Naturellement, la mise en œuvre initiale et maintenance peuvent être assurées par un professionnel de santé du CSP.

Les débats entourant les conditions et effets de mise en œuvre d'une **technologie connectée visant l'autonomisation du patient diabétique** [412] sont emblématiques. Le dispositif avait pour but **de réduire la fréquence de contact avec le système de santé**, et pouvait être initié par d'autres professionnels de santé que ceux habituellement impliqués [413].

Dès lors, ces derniers s'estimant « désintermédiés » ont refusé de participer aux réunions de négociation du tarif de remboursement de la prestation permise par la technologie. Ils ne voulaient pas aligner leur rémunération sur le tarif, plus bas que leurs honoraires habituels. Ce tarif a été accepté par les autres prestataires impliqués de façon inédite, dans la mise en œuvre d'une technologie ergonomique qui autonomise le patient [414].

Quoiqu'il en soit, on entre bien dans un **critère matériel de qualification** : la donnée est « *de santé* », parce qu'elle aura été produite par un appareil autonome **destiné par son fabricant à une finalité médicale**, mis en œuvre par le patient. Nous le distinguerons *infra* des dispositifs

[411] HAS, Évaluer les dispositifs médicaux connectés, y compris ceux faisant appel à l'intelligence artificielle, 19 février 2019, site HAS (contrôlé déc ; 2022).
[412] Le diabète est une maladie qui ne peut en l'état des connaissances, être guérie ; un diabète ne peut être qu'équilibré, pour prévenir des complications etc., d'où résulte le besoin d'un suivi au long cours très impactant pour la vie des malades, dont la sécurité et le confort par l'autonomie sont dès lors un enjeu fort.
[413] Avis HAS / CNEDiMTS 15décembre 2020 modifiant l'avis du 28 janvier 2020, DBLG1,Système de boucle semi-fermée dédié à la gestion automatisée du diabète de type 1.
[414] De façon emblématique, v. M. Mazière, « Pancréas artificiel : bagarre entre pharmaciens et prestataires autour du dispositif Diabeloop », L Qu. Pharm. 12 juil. 2021 ; L. Ganalopoulo, « Pancréas artificiel » : désormais remboursé, le dispositif Diabeloop va être délivré par les officines, courroux des prestataires de santé à domicile », L Qu. Méd. 17 sept. 2021 ».

ne revendiquant pas voire déniant une finalité médicale, et qui ne prétendent qu'à l'analyse ou la quantification de soi d'une personne qui n'est pas nécessairement « patient ».

* Le développement de telles hypothèses est exponentiel. **Cela vient de justifier en 2022, une modification significative de l'art. L. 5211-2 CSP**, lequel définit la notion de dispositif médical (non *in vitro*), sur un point qui nous intéresse tout spécialement ici [415].

Pour ce qui est du contrôle de la surveillance après commercialisation et de la surveillance du marché, l'article L. 5211-2 II adjoint à la compétence de l'ANSM, celle de la DGCCRF « *pour les produits mentionnés à l'article premier du règlement (UE) 2017/745* ***lorsque ceux-ci sont destinés à être utilisés directement par les consommateurs ou par des utilisateurs professionnels, autres que les professionnels de santé,*** *dans le cadre d'une prestation destinée aux consommateurs* ».

Or, ces technologies n'en sont pas moins, selon la définition légale, destinées par leurs fabricants à des « *fins médicales* ». Ces « consommateurs » **n'en sont pas moins des patients,** bien qu'évoluant hors du système de santé au sens organique, ce que conforte l'invocation d'utilisateurs « *autres que les professionnels de santé* ».

Ce texte de 2022 **caractérise le dépassement du traditionnel critère organique** par un critère matériel de qualification des données « de santé ».

§2. QUALIFICATION DES DONNEES SELON LEUR ATTRACTION DANS DES BASES LEGALES

L'autre approche qui permet ici d'invoquer des données de santé « par qualification de la loi » n'est pas analytique, mais synthétique. Elle s'appuie sur la **qualification du cadre dans lequel ces données peuvent être attraites** : soit qu'elles y ont vocation par essence (ainsi les données issues de la production organique du système de santé, *supra*) ; soit qu'elles y ont une vocation à s'y agréger **du fait de la pertinence de leur rapprochement en santé**.

La structuration des bases informatiques date de quelques décennies, mais **leur essor, centralisation, interconnexion et accès formalisé sont récents** : ils découlent, d'une part, de

[415] Ordonnance n° 2022-1086 du 29 juillet 2022 portant adaptation du droit, préc., art. 10.

la dynamique depuis 2016 du système national des données de santé, qui est une centralisation à finalité institutionnelle (A). D'autre part, de la conversion du « dossier médical partagé » et des données qui s'y agrègent, en un **espace numérique d'accès individuel** : il s'agit alors depuis 2022 d'une centralisation à finalité personnelle (B).

A. LA CENTRALISATION A FINALITE INSTITUTIONNELLE DES BASES DE « DONNEES DE SANTE » (SNDS)

A nouveau, cette centralisation est le résultat d'une **dynamique par vagues**. En 2016, le législateur a en effet entendu réunir, au sein d'un « *système national des données de santé* », la production de multiples acteurs et établissements [416]. Cela était d'abord restreint aux données liées à une activité médico-administrative (1). Mais en 2019, la loi y intègre des données diversifiées, qui en étendent considérablement le champ sous couvert de données de santé (2).

1. L'institution du SNDS en 2016 : les données médico-administratives

Dès 2013, le rapport de messieurs Bras et Loth souligne l'acquis et l'atout français, consistant en l'existence historique de bases de données massives et structurées **selon des nomenclatures et codages univoques**, liés à la situation de monopsone de l'assurance maladie obligatoire pour les soins remboursés. Néanmoins, le rapport relève les difficultés de l'exploitation de ces bases de données à des fins d'études et de recherche – un paradoxe, à l'ère de l'économie de la connaissance [417].

Les piliers du SNDS sont les bases massives issues de la production des soins par les hôpitaux et les cliniques (résultat du Programme de médicalisation des systèmes d'information, PMSI [418]), et issues de l'activité de remboursement des soins par les régimes obligatoires d'assurance maladie (système national d'information inter régime de l'Assurance maladie, SNIIRAM [419]), sachant que le SNIIRAM a lui-même progressivement intégré les informations de remboursement relatives à l'activité hospitalière rapportée dans le PMSI [420]. Autour s'articulent nombre d'autres bases, dont la description est étrangère à notre propos [421].

---

[416] Loi n° 2016-41 du 26 janvier 2016

[417] P-L. Bras, A. Loth, Rapport sur la gouvernance et l'utilisation des données de santé, septembre 2013, sur solidarites-sante.gouv.fr (contrôlé sept 2022).

[418] Le PMSI est géré par l'Agence technique de l'information sur l'hospitalisation (ATIH).

[419] géré par la Caisse nationale d'assurance maladie (CNAM)

[420] P-L. Bras, A. Loth, Rapport sur la gouvernance et l'utilisation des données de santé, préc.

[421] A. Lutun, *Le Big Data en santé, richesse et conditions d'accès*, thèse pour le doctorat en droit, Paris, 2021.

a. la création du « SNDS » par la loi de 2016 : une approche initialement restreinte

Le rapport de MM. Bras et Loth sous-tend la création par la ministre en charge de la santé, d'une commission de réflexion sur l'opportunité et les modalités de l'Open Data en santé. Par *Open Data*, le communiqué du ministère entend « ***l'effort que font les institutions, notamment gouvernementales, qui partagent les données dont elles disposent****. Ce partage doit être gratuit, dans des formats ouverts, et permettre la réutilisation des données* » [422]. Or, cela implique, dans un système de santé organiquement défini (CSP), et solvabilisé par un mécanisme d'assurance maladie obligatoire (CSS), que les données qui résultent de ces activités deviennent disponibles sous conditions à ce titre.

Cette approche institutionnelle est **fondamentalement distincte des applications altruistes de la « portabilité »**, qui consistent en le partage spontané à titre facultatif et privé par des patients de leurs données pour des fins de recherche : il sera l'objet d'une autre réflexion portée en 2020 par la mission Bothorel [423] ; nous l'avons précédemment évoquée.

La signification de l'Open Data ainsi posée, la réflexion quant à une ouverture spécifique dans le champ des données de santé est justifié par le fait que « *l'accès aux données de santé est porteur d'enjeux majeurs pour améliorer l'information des patients sur le système de santé, mais également pour favoriser la recherche et soutenir l'innovation et le développement économique* ». Cela suppose « *de bien faire la* ***distinction entre les données anonymes ouvertes à tous*** *(…)* ***et les données directement ou indirectement nominatives qui ne sauraient être rendues accessibles en dehors d'un cadre juridique et technique préci*****s** » [424]. Le rapport de la Commission Open Data en santé est rendu en 2014; il va avec le rapport Bras et Loth de 2013, inspirer le projet de loi « relatif à la modernisation de notre système de santé », lequel a pour objet les conditions d'un accès ouvert aux données de santé.

Ainsi, le « Système National des Données de Santé » (SNDS) est créé en 2016 par la « loi de modernisation de notre système de santé » [425], sous son titre IV « renforcer l'efficacité des

[422] Gouv., « L'ouverture des données publiques », sur gouvernement.fr, mis à jour le 15 mai 2017.
[423] E. Bothorel, S. Combes, R. Vedel, « Pour une politique publique de la donnée », déc. 2020 préc., spéc. p 181.
[424] Min. Aff. sociales et de la Santé, Communiqué de presse, « Marisol Touraine lance le débat sur l'open data en santé le 21 novembre 2013 », sur drees.solidarites-sante.gouv.fr, publié le 7 novembre 2013.
[425] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

politiques publiques et la démocratie sanitaire ». Son Chapitre V est libellé **« créer les conditions d'un accès ouvert aux données de santé** » (voir l'article 193), accès dont la Cour des comptes avait en 2016 relevé l'étroitesse [426]. L'intention et le cadre législatif sont alors précisés par plusieurs textes d'applications (modifiés par la suite) [427].

Ce texte ouvre une intense activité doctrinale, qui constate le **changement de paradigme, de bases fermées à bases ouvertes**, nécessitant outre la précision du régime d'accès antérieur et sa dynamique, des garanties fortes quant à l'anonymisation des données, etc. Mais ces doctrines **focalisent sur la vie privée, sans alors traiter d'enjeux de souveraineté** [428], ou n'abordent la notion de « souveraineté » qu'à l'échelle de l'individu [429].

Ainsi, l'exploitation des données **par des opérateurs privés de l'économie marchande compétitive est explicitement anticipée, non celle par des puissances publiques dans une dialectique géopolitique** (mais les deux défis apparaitront parfois consubstantiels).

En ce sens, l'arrêté de juill. 2017 met en exergue la question fondamentale du référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études visés à l'article L. 1461-3 CSP qui désirent accéder à ces données [430], lorsque ces fins de recherche, d'étude et d'évaluation sont « *commandités par des personnes produisant ou commercialisant des produits* » (au sens de L. 5311-1 II CSP), d'organismes à vocation d'assurance, réassurance et prévoyance en santé (1,2,3,5 et 6° de L. 612-2, I B du code monétaire et financier) ; et d'intermédiaires d'assurance (L. 511-1 code des assurances).

---

[426] Cour des comptes, « Les données personnelles de santé gérées par l'assurance maladie, une utilisation à développer, une sécurité à renforcer », mars 2016, p. 92

[427] Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé », JO, 28 décembre 2016 (modifié par la suite) ; Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé, JO, 24 mars 2017 ; arrêté du 17 juillet 2017.

[428] V. not. J. Bossi-Malafosse, « Les nouvelles règles d'accès aux bases médico-administratives », Dalloz IP/IT, 2016, p. 205-211 ; J. Cattan, « La mise à disposition des données de santé », D. A., 2016, ét. 9 ; E. Debies, « L'ouverture et la réutilisation des données santé : panorama et enjeux », RDSS, 2016, p. 697-709 ; L. Morlet-Haïdara, « Le système national des données de santé et le nouveau régime d'accès aux données », RDSS, 2018, p. 91-106.

[429] E. Netter, « La portabilité, un droit à inventer ? », Dalloz IP/IT, Dalloz, 2020, pp.352-357.

[430] Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé, JO, 24 mars 2017 ; arrêté du 17 juillet 2017 relatif au référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études, JO, 25 juillet 2017.

2. L'extension en 2019 : des données médico-administratives, aux données cliniques

La mise en place législative du SNDS a été suivie d'un rapport en 2018 dans le cadre de la « Stratégie de transformation du système de santé » sous l'égide du ministère ; titré « Accélérer le virage du numérique », ce rapport a fortement inspiré la loi de 2019 qui a largement étendu l'attraction des données dans le SNDS. Ce rapport proposait notamment de « *structurer les bases de données des professionnels, des établissements et des patients* ***afin d'alimenter les capacités de création de services et le*** **big data** ***en santé*** » [431].

a. Adjonction de « données de santé » inédites au SNDS initial

Au-delà donc des piliers institutionnels que sont le PMSI et le SNIIRAM, et des bases articulées autour d'eux, l'objectif est alors notamment **d'intégrer « *le recueil de données médicales (résultats des examens médicaux, connaissances des facteurs de risques...) et relatives à l'environnement physique / social des usagers* »**. Cela est, de loin, détaché des nomenclatures et codages voués à la connaissance analytique de la production hospitalière (objet du PMSI), comme de ceux voués au suivi des remboursements (objet du SNIIRAM) :

L'article L. 1461-7 CSP a prévu qu'un décret en Conseil d'Etat concrétise le contenu du SNDS. Tel sera l'objet de deux décrets successifs : le premier publié en décembre 2016 sous l'empire du droit initial [432] ; le second en juin 2021 sous l'empire du droit modifié [433], les deux étant séparés par une période de latence, **vouée à l'augmentation raisonnable du champ des données de santé concernées** au regard de la loi de 2019 préc., adoptée entre temps.

Le décret de 2021 modifie l'article R. 1461-2 CSP d'origine, qu'il réarticule autour de deux pôles de données de santé : les données de santé à géométrie variable au sein du SNDS ; les jeux de données sur la plateforme des données de santé.

---

[431] D. Pon, A. Coury « Accélérer le virage numérique », Rapport final de la stratégie de transformation (09/2018).

[432] Décret n° 2016-1871 du 26 déc. 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

[433] Décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

b. Le paramétrage réglementaire complexe des « données de santé » attirées

L'article R. 1461-2-I distingue la « **base principale** », laquelle couvre l'ensemble de la population (dont le contenu correspond aux 1° à 4° de l'article L. 1461-1 CSP, complété progressivement des données visées du 5° au 11°, déterminées par arrêtés) ; et « un ensemble de bases de données ne couvrant pas l'ensemble de la population dénommé " **catalogue** " » lequel recoupe du 1° au 11° au même article, mais avec une couverture donc partielle.

En outre, le règlement prévoit qu'un arrêté pris après avis de la CNIL « ***liste les données (des 1 à 11°) qui alimentent la base principale*** », et par ailleurs « ***désigne les bases de données figurant dans le catalogue*** ». Il est « *actualisé selon la disponibilité des données* », ce qu'appelle une mise en place nécessairement progressive.

Ce qui nous intéresse ici est, d'une part, que l'arrêté est à la main du ministre en charge de la santé, ce qui apparaît une approche raisonnablement souple (la question de l'abondement des bases est à distinguer de leur exploitation) ; d'autre part, l'avis de la CNIL est demandé **en dépit du fait que le transfert survienne dans un environnement homogène de hautes protections déjà acquises pour les données et bases de données séparément considérées**. L'objet de la CNIL pourrait-il être amené à s'étendre, vers des aspects de souveraineté distincts de la question des libertés individuelles ? [434]

*** Les jeux de données sur la plateforme des données de santé. Le II de l'article** R. 1461-2.-I. traite lui, non de l'abondement du SNDS, mais de la constitution « *par la Plateforme des données de santé ou la Caisse nationale d'assurance maladie* », de jeux de données à partir des bases de données du SNDS. En quelque sorte, le texte permet de passer d'un matériau brut, à une matière pré-raffinée ; ceci pour répondre rapidement à des besoins récurrents.

Ainsi, cette anticipation permet de répondre par des **jeux de données anonymes** (II-1°) à des « demandes du public » formulées dans le cadre de l'article L. 1461-2 CSP. Puis, sans que les auteurs des demandes ne soient précisés, en contraste du 1°, des **jeux de données agrégées et semi agrégées** « *adaptés à différents types de recherches, d'études ou d'évaluation* » [435] (II-2°), et **des échantillons** « *comprenant tout ou partie des données relatives aux personnes dont*

[434] Pointons ici le fait qu'en 2021, le décret préc. a reformulé les attributions du comité ad hoc, dont la mission « d'expertise » est remplacée par « éthique et scientifique » (nouvel article R. 1121-1 CSP).
[435] Le 2° précise que « Les données semi-agrégées sont individualisées pour les professionnels ou les établissements de santé et agrégées pour les bénéficiaires des soins »

elles sont issues » (II-3°) dont les caractéristiques sont publiées sur la Plateforme, tout comme la liste des jeux précités de données, lorsqu'ils sont mis à disposition par elle.

Leur actualisation doit faire « *l'objet d'une information de la (CNIL)* », dont l'article R. 1461-2-II n'indique pas que cette information doive être préalable. En tous cas l'enjeu s'est déplacé : il n'est plus tant ici la protection de l'individu au travers de ses données personnelles, **que la protection du système au travers de données populationnelles**.

B. LA CENTRALISATION PERSONNELLE DES DONNEES : DYNAMIQUE DE L'ESPACE NUMERIQUE DE SANTE (ENS)

Au-delà de la télémédecine, définie par l'article L. 6316-1 CSP comme permettant « *d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique (…) ou d'effectuer une surveillance de l'état des patients* » [436], l'accélération technologique a conduit à plusieurs réformes pour la transformation numérique. Il n'est pas lieu ici d'en retracer la généalogie, laquelle déborde de loin notre champ de recherche : considérons son apport le plus récent spécialement pertinent, quant aux « données » en soi.

En octobre 2022, une stratégie « Ségur du numérique » vient d'être formulée [437]. Son but est de « *généraliser le* ***partage fluide et sécurisé des données de santé entre professionnels et usagers*** *pour mieux soigner et accompagner* » ; ce programme alimentera « *Mon espace santé, qui permet à chaque citoyen de disposer d'une vision consolidée de son parcours de soin* ***afin d'être acteur de sa santé*** » [438]. Porté par la proposition en mai 2022 de règlement sur l'espace européen des données de santé [439], le « DME » (dossier médical électronique [440]) est en quelque sorte l'écho de l'ENS ; ce règlement vise à le généraliser à l'échelle de l'Union [441], ce sur quoi sur laquelle nous reviendrons en partie II.

---

[436] L. 6316-1 CSP, modifié en dernier lieu par la loi n°2019-774 du 24 juillet 2019.
[437] Sous l'égide du Ministère de la santé et de la prévention, Ségur du numérique, oct. 2022.
[438] Pour une approche pratique : ANS, Ségur du numérique en santé, Note sur la vision métier et les apports concrets du Ségur numérique, 6 juill. 2022 (version 1.0).
[439] Proposition de Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé (EEDS), COM(2022) 197 final, 2022/140 (COD).
[440] Article 2§2, m) on entend par «DME» (dossier médical électronique), un ensemble de données de santé électroniques relatives à une personne physique collectées dans le système de santé et traitées à des fins de soins de santé; »
[441] Ibid. préc., articles 1§2 b), et Chapitre III (qui liste les systèmes de DME et de bien être), articles 14 à 32.

Créé en 2019 par le législateur [442], précurseur national du futur DME européen, cet espace numérique de santé absorbe le dossier médical des personnes concernées, mais le dépasse (1). En effet, il a une vocation inédite à accueillir des données produites **non seulement hors du système de santé, mais également par des technologies non médicales** (2).

1. L'institution d'un "espace numérique de santé" personnel englobant les bases

La loi de 2019 relative à l'organisation et à la transformation du système de santé a modifié la section 3 du Chapitre 1er précité : elle est désormais titrée « *Espace numérique de santé, dossier médical partagé et dossier pharmaceutique* » [443]. Le législateur a prévu l'entrée en vigueur de l'espace numérique de santé (ENS) au plus tard au 1er janvier 2022.

Mi 2021, un décret a énoncé les dispositions d'application [444] permettant l'ouverture effective du service, dont la description ne nous retiendra pas ici. Relevons seulement que l'ENS, qui englobe conceptuellement les dossiers numériques préexistants (a), étend significativement au-delà le champ des données « de santé » qu'il réunit (b).

a. L'absorption des dossiers numériques professionnels préexistants dans l'ENS

Pour comprendre le rapport entre les dossiers dans l'ENS, il faut ici imaginer **l'emboîtement de réceptacles les uns dans les autres**. Pour schématiser, l'outil le plus accessible est le « dossier pharmaceutique » géré par les pharmaciens (L. 1111-23 CSP). Il n'est certes pas inclus « dans » le dossier médical partagé (DMP), mais est accessible à ses utilisateurs [445]. Ce DMP est utilisable par les professions médicales, non par les pharmaciens (L. 1111-14 CSP) [446].

Depuis 2019, il est « *intégré à l'espace numérique de santé dont il constitue l'une des composantes* » (L. 1111-13 CSP). Ainsi conçoit-on bien l'emboîtement des systèmes aux droits d'accès gradués, sachant que l'ENS va au-delà, pour intégrer des données relevant d'autres Codes.

---

[442] Article 45 II de la loi n° 2019-774 du 24 juillet 2019.
[443] Modifiée à la marge par la loi n°2020-1525 du 7 déc. 2020.
[444] Décret n° 2021-1048 du 4 août 2021 relatif à la mise en œuvre de l'espace numérique de santé NOR : SSAD2112391D
[445] En fait, les pharmaciens sont censés inscrire dans le DMP, les données pertinentes du DP.
[446] Selon L. 1111-23 al. 2 CSP, les informations du DP "*utiles à la coordination des soins sont reportées dans le dossier médical partagé*"; tel est le principe, qui devrait faire que les médecins n'aient pas à consulter le DP.

Par exemple, il est prévu l'inclusion dans l'ENS du titulaire qui en contrôle l'accès [447], de « *l'ensemble des données relatives au remboursement de ses dépenses de santé* » (article L. 1111-13-1, II - 4° CSP). Ces données relèvent typiquement du CSS. **L'ENS permet ainsi une approche holiste, inter-codes**. Mais le titulaire de l'ENS peut accorder ou refuser son accès aux professionnels et établissements de santé (*ibid*., IV-1°) ; il peut aussi l'ouvrir temporairement à des professionnels et établissements de son choix (R. 1111-32).

Nous n'approfondirons pas l'analyse de ce dispositif. Ce qui nous intéresse, est **l'extension des données attraites dans l'ENS, qui participent dès lors de sa qualification légale.**

b. L'extension du champ des données attraites dans l'ENS, une hybridation du système ?

Outre les données de santé correspondant aux contenus du DMP et du DP, l'ENS « *permet d'accéder* » (L. 1111-13-1-II) à des éléments inédits. Le but en 2019 est de permettre une autonomisation d'usage et de comportement du titulaire de l'ENS au sein, mais également en marge du système de santé ; cela a conduit à **incorporer dans l'ENS des outils et données externes au parcours de prévention / de soins** au sens historique du CSP/CSS/CASF [448].

* Au sein du système de santé, cela consiste en « 5° *Des outils permettant des échanges sécurisés* ***avec les acteurs du système de santé****, dont une messagerie de santé sécurisée permettant à son titulaire d'échanger avec les professionnels et établissements de santé et des outils permettant d'accéder à des services de télésanté* ».
Ce qui nous intéresse ici est que cette facilité de communication est également une **facilité de transmission le cas échéant, d'un nouveau type de données.** Or, elles n'auront pas été générées par les acteurs et établissements du système, *in situ* ou à distance, et sont donc importées dans cet espace par son titulaire (sous réserve du référencement des technologies ainsi communicantes, *infra*).

* En marge du système de santé au sens organique donc, il s'agit de la production de « *6° **Tout service numérique**, notamment des services développés pour favoriser la prévention et*

[447] Il s'agit de l'assuré social au profit duquel il est automatiquement ouvert sauf opposition, L. 1111-13-1-I alinéa 1 CSP.
[448] *Au sens historique*, car l'inscription de nouvelles pratiques dans le CSP conduit à modifier la conception traditionnelle du "système de santé" défini par les acteurs et établissements, auquel s'était adjoint les pratiques de télémédecine, etc. : un nouveau système, hybride, apparaît.

fluidifier les parcours, les services de retour à domicile, les services procurant une aide à l'orientation et à l'évaluation de la qualité des soins, les services visant à informer les usagers sur l'offre de soins et sur les droits auxquels ils peuvent prétendre ***ainsi que toute application numérique de santé référencés en application du même III*** ».

Le même article (L. 1111-13-1-II) dispose que l'ENS permet à son titulaire d'accéder notamment à « *3°* ***Ses constantes de santé éventuellement produites par des applications ou des objets connectés*** *référencés en application du III* ***ou toute autre donnée de santé utile*** *à la prévention, la coordination, la qualité et la continuité des soins* ». Cela n'est qu'une déclinaison spécialisé du 6° précité, ce que l'on retrouve dans le projet européen de 2022 [449].

Or, l'ensemble des services et outils ainsi rapprochés produit et utilise des données. La question du statut des données produites se pose donc, **lorsqu'il ne s'agit pas nativement de données de santé,** au sens de produites par les acteurs du système ou de la télémédecine.

Qu'en est-il alors du III ? celui-ci dispose que, « *Pour être référencés et intégrables dans l'espace numérique de santé, les services et outils numériques mentionnés aux 2° à 7° du II du présent article, qu'ils soient développés par des acteurs publics ou privés, respectent les référentiels d'interopérabilité et de sécurité élaborés par le groupement mentionné à l'article L. 1111-24, les référentiels d'engagement éthique ainsi que les labels et normes imposés dans l'espace numérique de santé mentionnés à l'article L. 1111-13-2* (...) ».

On y reviendra, **car ce texte ne cite pas expressément le statut de dispositifs médicaux [450], et permet *a priori* à des technologies non médicales d'abonder l'ENS** (*infra*).

2. L'adjonction dans l'ENS de données générées et utilisées hors du « système de santé »

La loi vise à rendre accessible à son titulaire / utilisateur ses constantes de santé produites par des applications ou des objets connectés référencés. **Le préalable est que de telles données y soient admises**.

Mais il ne s'agit pas seulement, pour les applications et objets connectés « référencés », d'abonder l'ENS. Ces applications peuvent y requérir des données pour leur propre finalité.

[449] Dans la proposition de règlement EEDS de mai 2022 préc., on trouve la même inclusion des données de « bien-être » dans le dossier de santé électronique ; si cela ne figure pas dans sa définition même (article 1§2-m), on le retrouve article 31, 33-f), mais également implicitement, article 5§1 dernier alinéa.

[450] Dans la proposition de règlement européen de 2022 préc., spéc. article 31§1, et 33§1-f.

Cela nous conduit à relever le référencement des services et outils numériques (a), avant de noter l'hybridation des données pouvant résulter de leur dialogue (b).

a. Le préalable du référencement des services / outils numériques connectés à l'ENS

L'article L1111-13-1-II **renvoie à un catalogue de services ou outils numériques référencés** qui ont vocation à abonder l'ENS, lequel propose, outre le 3° précité sur les constantes de santé "*produites par des applications ou objets connectés référencés*", (6°) "*tout service numérique (...) ainsi que toute application numérique de santé référencés*".

Dans la partie réglementaire du Code de la santé publique, ce référencement fait l'objet d'une sous-section 5 dédiée (R. 1111-37 à -39). Il est subordonné au respect des référentiels d'interopérabilité et de sécurité (mis en exergue par L. 1470-5 CSP) et d'engagement éthique, sachant loisible au ministre en charge de la santé « *de fixer par arrêté **d'autres critères** relatifs à la qualité des contenus numériques en santé* » (R. 1111-37, dernier alinéa). Leur satisfaction sera appréciée par une commission dédiée, dont l'avis favorable est décisif. Notons dès ici qu'il ne s'agit pas d'une procédure de certification en vue d'un marquage CE; ni d'une procédure d'évaluation en vue d'une inscription à la LPPR [451].

Après avoir en 2016 élaboré un Référentiel de bonnes pratiques sur les applications et les objets connectés en santé **[452]**, la Haute Autorité de Santé a en 2021 produit une doctrine d'évaluation des applications dans le champ de la santé mobile **[453]**. Or, dans le sillage de la loi de 2019 précitée, cette doctrine vise **à concrétiser les critères de référencement des technologies *non nécessairement médicales* évoquées dans le décret de 2021 [454]**. Elle donnera lieu à l'arrêté de juin 2022 précité, quant aux critères applicables selon la finalité, la criticité, etc. **[455]**.

[451] Sur ces points, *infra*.
[452] HAS, Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (mobile Health ou m-Health), validé par le collège de la HAS en oct. 2016, mis en ligne 7 nov. 2016.
[453] HAS, Évaluation des Applications dans le champ de la santé mobile (mHealth) - État des lieux et critères de qualité du contenu médical pour le référencement des services numériques dans l'espace numérique de santé et le bouquet de services des professionnels, validé par le collège de la HAS le 24 juin 2021.
[454] *Comp*. Proposition en 2022 du règlement EEDS, article 31 « étiquetage facultatif des applications de bien être », spéc. article 31§1.
[455] Arrêté du 23 juin 2022 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé - NOR : SPRD2214799A, JO 5 juillet 2022.

Ce qui nous intéresse ici, est que tout référencement dont la procédure aura abouti, donne lieu, avant sa mise en œuvre, à la signature d'une convention entre l'éditeur du service ou de l'outil numérique, et les membres du GIE [456]. Cette convention définit notamment « *les* ***catégories de données auxquelles le service ou l'outil pourra accéder*** *avec le consentement du titulaire* ».

En effet, de façon très fluide, *« le titulaire* (de l'ENS) ***peut autoriser les services et outils numériques en santé référencés dans*** **(l'ENS)** ***à accéder à certaines données de son dossier*** *dans les conditions prévues au III de l'article L. 1111-13-1. Cette autorisation est donnée depuis son* (ENS) *ou depuis le service ou l'outil numérique en santé référencé » (R. 1111-32),* sachant ces autorisations modifiables à tout moment.

b. Le statut des données résultant des interactions outils référencés / ENS

L'article L. 1111-13-1 CSP contient plusieurs dispositions essentielles, quant au statut des données qui y sont insérées ou en sont dérivées.

* La première est que (III, alinéa 2), « *Les services et outils numériques référencés ne peuvent accéder aux données de* (l'ENS) *du titulaire qu'avec l'accord exprès de celui-ci,* ***dûment informé des finalités et des modalités de cet accès*** *lors de l'installation de ces services et outils, et qu'à des fins de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour une* ***durée de conservation strictement proportionnée à ces finalités*** ».
Ainsi, les services et outils référencés **peuvent accéder à des données de santé déjà contenues dans l'ENS**, dans les conditions prévues par les textes d'application (cf. article R. 1111-32 CSP préc.).

Or, il peut s'agir de données de santé, dans des conditions toutefois à maîtriser, donc à préciser.
Mais tel ne semble pas encore le cas : l'article 1 de l'arrêté de 2022 relatif aux critères de référencement, constate que « *Les services conformes à ces seuls* ***critères ne peuvent pas encore proposer à leurs utilisateurs d'échanger des données*** *avec Mon espace santé* » [457].
Cela suggère qu'une disposition technique complémentaire et/ou un arrêté additionnel sont

[456] Convention entre l'éditeur du service ou de l'outil, le ministre chargé de la santé et la Caisse nationale de l'assurance maladie, contenu régi par l'article R. 1111-38 CSP.
[457] Arrêté du 23 juin 2022 préc., relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé, NOR : SPRD2214799A

requis. Cela pourrait éviter une approche invasive par aspiration de données de santé au-delà de la finalité consentie, à la faveur d'une autorisation trop large des titulaires de l'ENS.

* La seconde est que (IV, alinéa 3), « *La communication de tout ou partie des données de l'espace numérique de santé ne peut être exigée du titulaire de cet espace* ***lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et lors de la conclusion ou de l'application de tout autre contrat*** [458]*, à l'exception des contrats relatifs aux services et outils numériques référencés en application du III du présent article ».*
En revanche, l'exception est en termes catégoriques : ***« à l'exception des contrats relatifs aux services et outils numériques référencés*** *en application du III du présent article ».* Ainsi, le référencement et l'inclusion dans l'ENS aboutissent à l'exigibilité d'accès aux données.

Nous venons de voir que le III disposait que titulaire de l'ENS consente expressément, et soit « *dûment informé des finalités et des modalités de cet accès lors de l'installation de ces services et outils, et qu'à des fins de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour une durée de conservation strictement proportionnée à ces finalités ».*

Or, si le titulaire de l'ENS « ***A tout moment,*** *(...) peut décider : 1°* ***De proposer un accès temporaire ou permanent*** *à son* (ENS) *à un établissement de santé, à un professionnel de santé, aux membres d'une équipe de soins au sens de l'article L. 1110-12 ou à tout autre professionnel participant à sa prise en charge en application de l'article L. 1110-4,* ***ou de mettre fin à un tel accès*** » (L. 1111-13-1-IV, alinéa 2), **il n'existe pas formellement de dispositions symétrique pour les outils et services numériques visés au III**.

Mais quand bien même elle n'est pas expressément prévue, la rupture d'autorisation d'accès « *à tout moment* » ne nous semble pas moins possible en droit commun. Cela relativise la curieuse exception d'exigibilité des données dans le cadre des ***contrats relatifs aux services et outils numériques référencés (***(IV, alinéa 3, préc.). Elle ne peut dès lors être justifiée que par la fonction effective pour une finalité exclusive, explicite, consentie, proportionnée.

[458] On peut d'office intégrer dans ce champ les contrats de location immobilière, contrat d'emprunt bancaire immobilier, contrat de travail, contrat d'assurance risque, contrat d'assurance vie, contrat d'emprunt à la consommation etc.

S'il ne fait pas de doute que les données ainsi virtuellement partagées **sont des données de santé, du fait de leur incorporation dans l'ENS et leur assujettissement** à ses règles, et que l'éditeur du service doive lui-même justifier la nécessité d'accès aux données de l'ENS pour sa propre finalité (R. 1111-39 et L. 1111-13-1 CSP), cela bien que ce ne soit pas encore possible (cf. article 1 arrêté du 23 juin 2022 préc.), la question se pose ici du **statut juridique des services ou outils susceptibles d'y recourir** pour accomplir leur finalité propre.

En effet, aucune disposition de ces textes ne le précise ; ce texte ne trouve par ailleurs pas d'équivalent dans la proposition en 2022 de règlement EESD précitée, mais on verra néanmoins en gestation **un statut autonome « d'application de bien-être »**, *infra*.

SECTION II. DES DONNEES DE SANTE « PAR DESTINATION » ?

Sous l'intitulé données de santé « par qualification de la loi », nous avons dans la première section regroupé les données qui, selon des critères organiques ou matériels expressément définis par la loi, pouvaient être qualifiées de « données de santé » sans équivoque.
En miroir, nous relevons maintenant des données de santé « par destination » : **ces dernières ne répondent pas aux critères précités**, mais n'en possèdent pas moins une signification médicale potentielle sur un plan individuel, et médico-sociale à l'échelle populationnelle.

Hors du champ médical, le développement des biocapteurs et senseurs a ouvert l'ère de la « quantification de soi » (*quantified self*) et l'analyse de soi » (*self analytics*) [459], et leur corrélation avec les comportements et environnements grâce à des applications portatives [460]. Cela a conduit la Haute Autorité de santé à leur dédier un référentiel, lequel porte « *sur les applications et les objets connectés (Apps/OC)* ***n'ayant pas de finalité médicale déclarée. Il concerne donc tout particulièrement la zone dite « grise » des applications ou des objets***

[459] Monsieur Desrosières souligne que mesure et quantification doivent être distingués. Cette dernière ne vise qu'à « *exprimer et faire exister sous une forme numérique ce qui, auparavant, était exprimé par des mots et non par des nombres* ». La quantification n'a donc de sens autre que statistique, qu'avec l'avènement de « *conventions d'équivalences préalablement définie*s », lesquelles **prennent valeur d'indicateur** (ainsi en biologie, biométrie, actimétrie, imagerie) **pour une finalité de prédiction, mesure de dynamique ou attestation d'effet**, *in "*Pour une sociologie historique de la quantification. L'argument statistique", Presses de l'École des mines 2008, p. 10-11).
[460] Dès mai 2014 : CNIL, « Le corps, nouvel objet connecté - du quantified self à la m-santé : les nouveaux territoires de la mise en données du monde », Cahiers IP (innovation et prospective) n°02, mai 2014.

connectés *ayant un effet potentiel sur la santé sans être un dispositif médical.* ***Les dispositifs médicaux, qui entrainent le marquage CE, en sont donc exclus*** » [461].

Il est inutile de rapporter les exemples fourmillants d'objets et applications, et de paraphraser leurs typologies doctrinales, ainsi les classifications initiales et stables de Aungst [462], Mosa [463], Yasini [464], Labrique [465], Bender [466], Yetisen [467], Hussain [468] ou Cook [469]. Mais si elles possèdent une grande pertinence pour la régulation des offres et des usages en la matière, **tel n'est pas le cas pour le statut juridique des systèmes et des données :** ce n'était pas leur prisme.

§1. APPREHENSION DU PHENOMENE PAR LES CATEGORIES DU DROIT DE LA SANTE

Les outils et services numériques précités ne relèvent pas d'un statut homogène. Certains sont des dispositifs médicaux au sens de L. 5211-1 CSP, dès lors redevables d'une certification obligatoire ; d'autres, non. Ce qui nous intéresse, est l'hypothèse dans laquelle **la qualification juridique n'est pas possible ou pas souhaitée** [470].

« *Ceci n'est pas un dispositif médical* » : telle est la formule apparaissant en sous-titre de messages publicitaires promouvant des technologies portatives et connectées variées, dont

[461] HAS, Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (mobile Health ou mHealth), 7 nov. 2016.
[462] Aungst TD, Clauson KA, Misra S, Lewis TL, Husain I. « How to identify, assess and utilise mobile medical applications in clinical practice ». Int J Clin Pract 2014;68(2):155-62.
[463] Mosa AS, Yoo I, Sheets L. « A systematic review of healthcare applications for smartphones ». BMC Med Inform Decis Mak 2012;12:67.
[464] Yasini M, Marchand G. « Toward a use case based classification of mobile health applications ». Stud Health Technol Inform 2015;210:175-9.
[465] Labrique AB, Vasudevan L, Kochi E, Fabricant R, Mehl G. « mHealth innovations as health system strengthening tools: 12 common applications and a visual framework ». Glob Health Sci Pract 2013;1(2):160-71.
[466] Bender JL, Yue RY, To MJ, Deacken L, Jadad AR. « A lot of action, but not in the right direction: systematic review and content analysis of smartphone applications for the prevention, detection, and management of cancer ». J Med Internet Res 2013;15(12):e287.
[467] Yetisen AK, Martinez-Hurtado JL, da Cruz Vasconcellos F, Simsekler MC, Akram MS, Lowe CR. « The regulation of mobile medical applications ». Lab Chip 2014;14(5):8 33- 40.
[468] Hussain M, Al-Haiqi A, Zaidan AA, Zaidan BB, Kiah ML, Anuar NB, et al. « The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations ». Comput Methods Programs Biomed 2015;122(3):393-408.
[469] Cook SE, Palmer LC, Shuler FD, « Smartphone mobile applications to enhance diagnosis of skin cancer: A guide for the rural practitioner ». W V Med J 2015;111(5):22-8.
[470] L'unique exception légale expresse pour des produits de fabrication industrielle n'a pas de pertinence ici : l'article 59 du règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 prévoit sur demande dûment justifiée, la possibilité d'une "*dérogation à l'obligation d'évaluation préalable de la conformité de chaque dispositif prévue à l'article 52 du règlement (UE) 2017/745, autoriser la mise sur le marché ou la mise en service sur le territoire français d'un dispositif n'ayant pas fait l'objet d'une telle évaluation, mais dont l'utilisation est dans l'intérêt de la santé publique ou dans celui de la sécurité ou de la santé des patients*" (repris in article L. 5211-3-II CSP modifié par Ordonnance n°2022-582 du 20 avril 2022).

notamment des montres bardées de capteurs et de senseurs (mesure du nombre de pas ; de la longueur de pas, donc des distances parcourues corrélées à la vitesse de déplacement ; de la qualité de sommeil ; électrocardiogramme, tensiométrie, oxymétrie, etc.) reliées à des terminaux personnels portatifs (*smartphones*) et/ou communicant à distance [471]. **Quel but ?** L'ambiguité est en effet parfois possible [472].

Nous examinons la dénégation de la finalité médicale qui vise potentiellement à éluder la qualification « de santé » des données générées (A), sachant qu'une **catégorie de technologie autonome devrait apparaître** à terme en droit européen (de « *bien être* »). Puis nous en relevons les conséquences, lorsque ces données possèdent d'une signification intrinsèque ou par croisement (B), et que cette **signification est en fait, la raison même de leur génération**.

A. ELISION DE LA QUALIFICATION DES DONNEES, PAR DENEGATION D'UNE FINALITE MEDICALE ?

Rappelons qu'en France, l'article L. 1111-13-1 CSP modifié en 2020 a mis en exergue que, « *pour être référencés et intégrables dans l'ENS* » (**ce n'est donc pas une condition posée à leur commercialisation en soi)**, les services et outils qu'il mentionne respectent :
* les référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public chargé du développement des systèmes d'information en santé (L. 1111-24 CSP).
* les « *référentiels d'engagement éthique ainsi que les labels et normes imposés dans l'espace numérique de santé* » sous responsabilité étatique (L. 1111-13-2 CSP).

Il ne s'agit pas nécessairement de dispositifs médicaux, mais, lorsque c'est le cas, nous avons relevé que **le régime des données suivait celui de la technologie**.

Dès lors, nous relevons ici l'effort parfois mené par des fabricants pour écarter les obligations qui découleraient de la finalité médicale d'une technologie (1), avec l'effet voire l'objectif d'écarter les données générées, du champ des « données de santé » protégées à ce titre (2).

---

[471] A l'inverse, l'affirmation « *ceci est un dispositif médical* » est depuis longtemps pratiquée dans la publicité pour des produits qui, du fait de leur forme et mode d'administration, pourraient être confondus avec des médicaments.
[472] C. Courage, « Qualification du dispositif médical : quand les activimètres permettent d'affiner les critères de qualification » (note sous CE 10 février 2020, n° 421576), rev. dr. et santé 2020, n°97, 981-983.

1. Ecarter les responsabilités juridiques découlant d'une finalité médicale ?

Ecarter la qualification et toute confusion quant au statut de la technologie, vise *potentiellement* à éviter de la soumettre à une certification propre au droit de la santé (a) ; et à esquiver la responsabilité civile du fait des produits défectueux sur un point critique (b).

a. éviter la qualification de DM pour éviter la certification correspondante ?

Le droit européen impose la certification de conformité des technologies de santé, selon des normes spécifiques actualisées en 2017, *supra*. Certes, aucun objet connecté ne relève de l'annexe XVI du Règlement de 2017, laquelle liste les technologies dont la certification est exigible, quand bien même elles ne constituent pas des dispositifs médicaux. Mais ce point **n'interdit pas potentiellement, la requalification devant une juridiction**.

En matière de médicaments, la requalification jurisprudentielle est fréquente [473] et convoque de nombreux éléments (publicité, allégations sur conditionnement, notice, forme physique, vocabulaire, diffusion du produit, connaissance qu'ont les utilisateurs, opinion du « *consommateur moyennement avisé* »). Tous **participent de la méthode du faisceau d'indices**. Elle permet de sanctionner des stratégies commerciales habiles, qui visent à éluder l'application du droit pharmaceutique et l'exclusivité commerciale des pharmaciens.

En matière de dispositifs médicaux, l'absence de contentieux pénal pour exercice illégal de la pharmacie (il ne vaut que pour la vente de médicaments [474]) a pour effet que le droit n'est pas dissuasif de telles stratégies. Il est facile d'imaginer comment des réseaux sociaux, etc. peuvent orchestrer l'idée que l'usage d'une technologie pourrait être pertinent **pour un but autre que celui qui lui a été formellement assigné**, et cela en marge des normes applicables.

Or, la confusion est rendue aisée par la faible culture du public ; certaines publications de vulgarisation en santé parlent ainsi « d'objet connectés », sans un mot sur leur statut, ni sur le statut des données qu'ils génèrent. Pour raisons de coûts, nombre de consommateurs-patients

---

473 E. Fouassier, *Evolution récente de la jurisprudence en matière de définition du médicament*, thèse pour le doctorat en droit, 1996 ; F. Megerlin, E. Fouassier, « Le juge européen et la notion de médicament: la subsidiarité et la civilisation en question », Rec. Dalloz 1995, I 8 janv. 2015, 23-29.

[474] Et pour les DMDIV à usage individuel, à l'exclusion depuis 2014 des test d'ovulation et de grossesse.

aux Etats-Unis recourent pour une finalité de suivi personnel, à des technologies qui ne revendiquent pas une finalité médicale.

Telle est sans doute la raison pour laquelle certains opérateurs décident de **couper court à tout risque par une qualification négative explicite** : ainsi tel objet connecté, bardé de biocapteurs et biosenseurs « *n'est pas un dispositif médical* ». Mais cela n'exclut pas la fiabilité, ni le référencement de l'outil / du service pour l'abondement de l'ENS, on l'a vu.

Nous verrons qu'un nouveau régime (enregistrement d'applications à finalité non médicale mais de « *bien-être* ») **est en cours d'apparition en droit européen**, et que la dénégation de la qualité de dispositif médical peut également préfigurer une intention de s'y inscrire, *infra*.

b. Eviter de soumettre le fabricant à la responsabilité du fait des produits défectueux sur un fondement spécifique ?

Nul fabricant qui commercialise un produit ne peut échapper (sauf exceptions légales, ici sans pertinence [475]), à sa responsabilité du fait des produits défectueux. Dès lors, le but ici est d'éviter de surprendre le consommateur / utilisateur dans son **attente légitime de sécurité liée à un usage spécifique** ; l'usage spécifique sécrétant une attente légitime est donc ici l'enjeu de la qualification juridique. Comment ?

La « *responsabilité du fait des produits défectueux* » a été introduite en 1985 par une directive en droit européen, applicable selon le critère non exclusif, de territorialité du dommage. Cette directive pose les bases communes du contentieux de la réparation civile, **en l'absence de contrat liant l'utilisateur au fabricant, et en l'absence de faute de ce dernier :** le défaut résulte de la simple surprise de « *l'attente légitime de sécurité* » de l'utilisateur ; il peut notamment consister en un défaut de conformité du produit, et/ ou un défaut d'information.

Or, de cette acception de l'« *attente légitime de sécurité* », résulte en pratique l'inflation des notices d'information et d'explication fournies par les fabricants, notamment en santé (spécialement en matière de médicaments [476]). Le but est que le consommateur ne puisse

[475] Dont l'absence de mise en circulation.

[476] Pour la responsabilité du fait des produits défectueux, le Code civil identifie le fabricant comme étant le responsable du dommage. En principe, c'est donc sa responsabilité qui doit être engagée par le patient. Pour une approche plus classique de la sanction du défaut d'information assimilé à une « défectuosité », Civ. 27 nov. 2019, n°18-16.357 ; Civ. 1re, 9 juill. 2009, n° 08-11.073 ; Civ. 1re, 22 nov. 2007, n° 06-14.174 ;

prétendre être « surpris » de façon dommageable, par des conditions, des limites, et des risques d'usage du produit.

En conséquence, le signalement d'une limite de fiabilité, d'un effet indésirable ou même d'un risque fait qu'il ne s'agit plus d'un « *défaut du produit* », au sens de l'article 1245 et suiv. Code civil). Censé avoir lu la notice, le consommateur-utilisateur ainsi dûment informé a **implicitement consenti, par arbitrage bénéfice / risque, au risque inhérent à son usage.**

Quand bien même existent des communautés technologiques évidentes entre les dispositifs qui produisent des données (capteurs, senseurs, logiciels embarqués) du fait de la « différenciation retardée » de certains produits [477], l'enjeu ici est qu'un défaut de sensibilité, d'interprétation ou de notification ne soit pas qualifié de « *défaut* » au regard d'un usage **qui n'était pas revendiqué voire était déconseillé, et ne sera donc pas assumé** par le fabricant : il n'y a pas de place pour des atermoiements jurisprudentiels.

Ainsi en est-il par exemple, en cas de problème de capture / de restitution d'ECG aboutissant à une perte de chance pour un utilisateur qui imaginait surveiller d'éventuelles anomalies de son rythme cardiaque dans un but de prévention et d'alerte, alors que la technologie n'était **commercialisée qu'à fin « récréative »**. Mais reste la question du statut des données.

2. L'élision pour faciliter l'usage de données réputées (dès lors) « non santé » ?

Nul ne conteste que les capteurs et senseurs appliqués au corps humain produisent des données personnelles, potentiellement sensibles (a). Mais ces dernières n'entrent dans le champ de la LIL de 1978, que sous les conditions de leur transfert et traitement déportés (b).

Toutefois, lorsqu'il ne peut être identifié, le patient lésé par un produit de santé défectueux peut engager la responsabilité du distributeur, du vendeur ou du loueur. Il incombera par la suite à ces professionnels d'exercer un recours contre le fabricant, ce qui est prévu à l'article 1245-6 du Code civil, à condition que le fabricant ne remplisse pas les conditions d'exonération énumérées à l'article 1245-10 du même Code.

[477] Cette pratique désigne le fait de repousser le plus en aval possible, les opérations terminales de finition ou de personnalisation d'un produit ; parfois jusqu'à séparer ce processus terminal, de la production ou de l'assemblage. Il est des cas dans lesquels biocapteurs et biosenseurs sont communs, « encapsulés » dans des dispositifs au design et prétentions différentes.

a. De la métrologie du corps humain au transfert des données

La dénégation de la finalité médicale de la technologie, **implique élision de la qualification** « de santé » des données qui résulteraient de sa mise en œuvre. Ainsi, en cas d'abonnement à un service proposant un suivi des données générées, en vue de l'édition de graphiques, de statistiques (courbes de poids pour une balance connectée, nombre de pas, qualité de sommeil, oxygène dans le sang, électrocardiogramme, tension, etc), de messages de félicitations ou d'encouragement sur base de scores d'activité (régime alimentaire, coaching sportif), prescriptions comportementales (d'ordre hygiéno-diététique, activité physique) etc.

Nous avons vu que ces données étaient rattachées aux concepts a-juridiques de « soi quantifié » (*quantified self*) ou d'« analyse de soi » (*self analytics*). Aucune **conclusion interprétative ni même d'orientation** au sens clinique, ne sera alors proposée par le vendeur **: son propos s'affiche purement métrologique.** Des signaux faibles ne sont objectivés qu'à ce titre, ou au titre de « bien être », dont la corrélation avec l'état de santé est mis en exergue dans le considérant n°5 de la proposition de règlement européen de 2022 précitée [478]. Le but des fabricants est de maintenir les données **dans le giron du droit commun**.

Or, le traitement par un algorithme sophistiqué, capable de croiser plusieurs variables et de les corréler à des comportements / environnements, n'induit pas pour autant, en droit positif, la « finalité médicale » de la technologie (nous avons vu qu'il en était ainsi pour les prétentions récréative, de mesure de performance, *coaching* sportif, etc.). Ainsi, le critère n'est pas celui de la sophistication, mais de la prétention : **il peut y avoir une sophistication technologique élevée, pour une prétention applicative modeste**.
Dès lors, tout dépend du marché visé, et des modalités de sa « valorisation » [479] par le fabricant / diffuseur des technologies. Cela n'exclut pas que, si la proposition de règlement

[478] Considérant n° 5, « *Ces données de santé électroniques à caractère personnel pourraient inclure des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique* (…) ***ainsi que des données sur des facteurs déterminants pour la santé, tels que le comportement, les facteurs environnementaux, les influences physiques,*** *les soins médicaux* ***et les facteurs sociaux ou éducatifs*** **» (…).** **«** *Les données de santé électroniques concernent toutes les catégories* ***de ces données, indépendamment du fait que ces données sont fournies par la personne concernée ou par d'autres personnes physiques ou morales****, telles que des professionnels de la santé, ou sont traitées* ***en relation avec la santé ou le bien-être*** *d'une personne physique* »

[479] Comme en matière de terminaux portatifs en téléphonie où se distingue un marché de masse à prix bas, vs. et un marché de niche très onéreux, sur une base technologique pourtant très proche voire parfois commune, en dehors du *design* et de capacités marginalement utilisées par les consommateurs.

EEDS formulée en mai 2022 venait à s'appliquer, des fabricants désirent rejoindre le statut autonome de « application de bien être » en gestation, *infra* partie II.

b. Le statut des données déterminé par leur transfert ?

En droit, il y a en outre lieu de distinguer selon que les données sont traitées par/sur le dispositif même ; ou qu'elles sont transférées pour un traitement à distance. Lorsque la CNIL évoque le « *Corps, nouvel objet connecté* » [480], c'est en fait en cas de **transfert (prévu ou simplement possible) de données**, que leur statut juridique est en question : cela pose la question de l'applicabilité de la loi de 1978 (données « personnelles ») autant que du droit sanitaire (donnée « de santé »).

* Sur le terrain de la loi de 1978, la CNIL souligne que la loi ne s'applique pas aux traitements **qui comporteraient des données de santé à l'usage exclusif de la personne**. Elle fournit l'exemple « *d'applications mobiles en santé* » (elle n'emploie pas la qualification de dispositif médical), qui « *proposent dans leurs fonctionnalités, la collecte, l'enregistrement ou la conservation de données* ***à condition que ces opérations s'effectuent localement*** *sur un ordinateur, un ordiphone ou une tablette,* ***sans connexion extérieure et à des fins exclusivement personnelles*** **»** [481]. Ainsi, cela n'en ferait pas des « données personnelles », au sens de statut justifiant leur protection spécifique dans l'hypothèse de transferts / traitements.

* Sur le terrain du droit sanitaire, la question se pose différemment. Toujours dans sa doctrine, la CNIL énonce que n'entrent pas dans la notion de « donnée de santé », les données « ***à partir desquelles aucune conséquence ne peut être tirée au regard de l'état de santé*** *de la personne concernée* » ; la CNIL de donner l'exemple d'une application sur terminal mobile qui permettrait la connaissance du nombre de pas, sans croiser ces données avec d'autres [482].

Mais cette doctrine ne laisse-t-elle pas un peu sur la faim ?

En premier lieu, en supposant que les données issues de la mesure des pas demeurent traitées par un algorithme embarqué, sans donc de transfert pour traitement, nous avons vu que la loi de 1978 était inapplicable. Mais la miniaturisation n'exclut pas, que les algorithmes puissent

[480] CNIL, « Le corps, nouvel objet connecté ? », Cahiers IP (innovation et prospective), n°02, publié en 2014.
[481] CNIL, « Qu'est-ce ce qu'une donnée de santé ? », onglet dédié (non daté) sur site de la CNIL, vérifié décembre 2023.
[482] *Ibid.*

dans le futur et c'est déjà le cas dans le présent, traiter localement (sur le terminal, sans transfert) des données **issues de plusieurs capteurs, donc en fait les croiser**.

Or, ce croisement pourrait conduire à une « donnée de santé », alors que la technologie employée ne revendique pas de qualification médicale, voir la dénie ; d'autre part, imaginons les données ici de capteurs multiples non traitées sur le terminal même, mais transférées et croisées de façon externe (en temps réel ou différé). Ainsi, nous aurions des données personnelles soumises au droit commun, **dont le croisement aboutit à une « donnée de santé », hors de toute technologie et intention médicale**. Nous avons bien ici une nouvelle illustration de l'épuisement du critère organique, pour définir les « données de santé ».

En outre, nous trouvons également ici **une limite à l'interdiction de la cession / exploitation commerciale propre aux données de santé** (L. 1111-8 CSP préc.) : il suffit de céder par segments, en conscience ou non, des données personnelles intrinsèquement « non santé », dont l'acheteur par hypothèse hors Union européenne peut procéder à la combinaison pour en tirer des considérations « en santé », hors la protection du droit pertinent [483], la question de l'anonymat (désormais parfois relatif) pouvant faire obstacle.

B. Les limites de l'élision de la qualification des technologies

Si des fabricants peuvent chercher à éluder la qualification de « technologie médicale », rappelons d'abord que **cela peut résulter d'une stratégie de différenciation retardée**. En outre, cela pourrait résulter d'une autre considération, si de nombreux droits, à l'instar apparent du droit français [484] et comme le suggère la proposition de règlement EEDS de 2022, considéraient **la possibilité d'un dialogue entre systèmes de statuts juridique différents**, sans préjudice du respect des normes de sécurité et, en théorie, de protection des données.

En ce sens, nous relevons la dualité de statut des outils en présence (1), sachant que ceux non qualifiés de DM pourraient être référencés (2), mais leur usage alors ne pas être remboursé.

1. La dualité de statut des outils / services numériques référençables pour l'ENS

[483] En France, résultant de la soumission à l'article 8 et au Chapitre IX de la LIL de 1978 ; protection par le secret au titre de L. 1110-4 CSP ; soumission aux référentiels de sécurité et d'interopérabilité des données de santé (L. 1110-4-1 CSP) ; à l'hébergement des données de santé (L. 1111-8 et R. 1111-8-8 et s. CSP) ; à la mise à disposition des données de santé (L. 1460-1 et s. CSP).
[484] Nous avons souligné que l'article 1er de l'arrêté de juin 2022, SPRD2214799A, maintenait l'incertitude.

Il est nécessaire de distinguer le référencement de la technologie au sens de L. 1111-13-1-III CSP, et sa qualification de dispositif médical au sens de L. 5211-1 CSP. **La loi créant l'ENS ne contenait sur ce point pas de précision** (voir L. 1111-13-1, II et III), renvoi à un décret en Conseil d'Etat. Or, le statut n'est pas plus précisé dans les textes d'application (R. 1111-27 CSP) : il est seulement indiqué que sont potentiellement incluses dans l'ENS les « *constantes de santé* » (3°-a), et « *toutes autres données de santé* » (3°-c), produites par des services ou outils numériques référencés au catalogue mentionné au 6°.

Or, ce 6° **est mutique quant au statut juridique des outils.** Nous avons vu que l'arrêté de 2022 relatif aux critères de référencement des services et outils numériques au catalogue de service de l'ENS [485] énonçait parmi les conditions de recevabilité, la fourniture de « *toute pièce justifiant, **le cas échéant,** de la conformité aux règles prévues par le règlement 2017/745 du parlement européen et du conseil du 5 avril 2017 relatif aux dispositifs médicaux, **ou de toute autre procédure préalable requise au titre d'une réglementation nationale ou européenne*** » (article 4).
De ce « *cas échéant* », il résulte implicitement mais nécessairement que l'outil ou le service numérique pouvant abonder l'ENS et utiliser ses données, **pourrait ne pas constituer un dispositif médical au sens du règlement 2017/745**, sans préjudice du respect du règlement 2016/679 relatif à la protection des données personnelles, et du respect de la PGSSI-S [486].

En outre, ce point est acté dans le guide de juin 2021 de la HAS [487] : il relève une classification par IQVIA [488], de solutions "*ne constituant pas des dispositifs médicaux*", mais couvrant 5 catégories : bien être et prévention (cat 1), apparition des symptômes et recherche de soins (cat 2), "*diagnostic*" [489] (cat 3), suivi du problème (cat 4) et traitement (cat 5). Depuis 2016, cette doctrine de la HAS est constante [490].

---

[485] Arr. 23 juin 2022 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé, SPRD2214799A.
[486] PGSSI-S - Corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé.
[487] HAS, Guide méthodologique - Évaluation des Applications dans le champ de la santé mobile (mHealth)-État des lieux et critères de qualité du contenu médical pour le référencement des services numériques dans l'espace numérique de santé et le bouquet de services des professionnels, validé par le Collège, 24 juin 2021.
[488] IQVIA Institute for Human Data Science. The Growing value of digital health. Parsippany: IQVIA Institute; 2017.https://regresearchnetwork.org/wp-content/uploads/the-growing-value-of-digital-health.pdf
[489] Ceci procède de la traduction littérale du rapport IQVIA, mais ne relève pas d'une catégorie admise en droit français pour un dispositif à caractère non médical.
[490] HAS, Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou m-Health) oct. 2016 préc. spéc. page 5 : "*Ce référentiel porte sur les applications et les objets connectés n'ayant pas de finalité médicale déclarée. Il concerne donc tout particulièrement la zone dite « grise » des applications ou des objets connectés ayant un effet potentiel sur la santé sans être un dispositif médical. Les dispositifs médicaux, au sens de la directive européenne 93/42/CEE qui entraine le marquage CE, en sont donc exclus. **Ce***

Or, ceci est à bien distinguer de la classification fonctionnelle, validée en février 2021 par la HAS, des solutions utilisées **dans le cadre du système de santé** [491].

2. Des outils / services numériques « non DM » sont intégrables dans l'ENS

Ainsi, la qualification juridique de DM **n'est pas une condition du référencement des outils et services numériques** éligibles à l'Espace Numérique de Santé. Mais si la fiabilité du service est censée être établie par le référencement (et par les obligations contractuelles qu'il suppose, quant à la protection des données), le seul référencement est insuffisant à la prise en charge de la prestation de service numérique par la solidarité nationale.

En effet, le remboursement des outils ou services distincts des actes de soins suppose en application du Code de la sécurité sociale, leur inscription à la Liste des produits et prestations remboursables (L. 165-1 CSS). Certes, cet article qui encadre l'inscription au remboursement des « *dispositifs médicaux à usage individuel* » recouvre aussi « ***des produits de santé autres*** *que les médicaments (...) et des prestations de services et d'adaptation associées* ».

Pour autant, la plateforme « *Convergence* », destinée aux professionnels, postule que **seuls les fabricants d'un dispositif médical numérique** peuvent y certifier la conformité de leur offre aux exigences prédéfinies, pour sa prise en charge par l'Assurance Maladie [492]. Pour cette procédure, cela subordonne le remboursement à la condition cumulée, préalable mais non suffisante, de la qualification juridique et du référencement précité.

Or, c'est là une limite de l'élision volontaire de la qualification de dispositif médical, bien que, on l'a vu, un tel défaut de qualification n'était pas exclusif d'un usage pour l'ENS. Mais il existe nombre de situations dans lesquelles le remboursement d'usage ou d'abonnement d'un outil / service numérique n'est pas recherché, car le modèle économique peut être autre [493] :

---

référentiel ne se substitue pas à la loi ou la réglementation concernant les dispositifs médicaux *(au sens de la directive européenne 93/42/CEE qui entraine le marquage CE (...)"* depuis remplacé par le règlement de 2017. *"(...) L'application des bonnes pratiques définies dans le présent référentiel s'entend sans préjudice de la réglementation en vigueur*."

[491] HAS, Guide méthodologique - 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 févr. 2021.

[492] https://convergence.esante.gouv.fr/

[493] A. Boulard, E. Favier-Baron, S. Woillet, *Le business de nos données médicales*, FYP editions, Paris oct. 2021. Mais les auteurs n'y traitent pas du statut différencié des données, comme signalé en introduction.

achat personnel en ligne des applications, valorisation des données produites (dès lors qu'elles ne sont pas « de santé »), car « *quand c'est gratuit, c'est vous le produit* » [494].

§2. AUTONOMIE DE LA QUALIFICATION DES DONNEES, SELON UN CRITERE DE DESTINATION ?

En droit français et européen définissant la « donnée de santé », il n'existe pas de notion de donnée « par destination » ; ceci bien que l'idée soit latente, dans le considérant du règlement RGPD de 2016, et implicite, dans la proposition de règlement EEDS de 2022.

Il s'agit d'une création doctrinale qui procède de plusieurs sources, et possède plusieurs sens. Pour notre part, nous l'avions inférée d'observations, et publiée au début de nos recherches, avec une divergence ultérieure de la CNIL quant à sa signification (A).

Mais son intérêt intrinsèque, comme l'intérêt de la nuance entre les doctrines, sont confirmés par une extension, dans la proposition de règlement de 2022, de la définition de la « donnée santé », laquelle **dépasse la définition normative retenue dans le règlement de 2016** (B).

A. LA PROPOSITION DE NOTION DE DONNEE DE SANTE « PAR DESTINATION »

Dans les sciences juridiques, la notion de « destination » relève d'une **technique de qualification**, laquelle nous a servi en 2017 pour un raisonnement par analogie en matière de données de santé. Voici pourquoi :

Le droit civil fournit l'exemple de l'« *immeuble par destination* » : telle est la qualification d'un bien « *meuble* » qui participe de la qualification d'immeuble, parce qu'il s'y incorpore ; on ne pourrait l'en séparer sans démontage, dénaturation ou dégradation réciproque. **Cette consubstantialité est une fiction juridique** organisée par l'article 517 al. 2 du Code civil, concrétisée par la loi et par la jurisprudence. Cette dernière pose pour condition que le bien meuble et l'immeuble au service duquel il a été placé, appartiennent au même propriétaire [495].

---

[494] La formule généralement attribuée à Tim Cooks, PDG du groupe Apple, a été déjà invoquée par Richard Serra en 1973 "*if something is free, you're the product*".
[495] Civ. 3e, 5 mars 1980, Bull. civ. III, n°51, R., p.62 ; Dalloz 1980 IR. 477, obs. A. Robert.

Ainsi, une chose qui s'incorpore à une autre, ou est indissolublement liée à elle, participe de la qualification dominante de cette dernière dans le champ de laquelle elle est attraite, dès lors qu'elle émane d'une même personne. Cette fiction juridique **facilite la cession, ou la protection, du bien globalement considéré**, sans fragmentation de statut donc de régime.

Telle n'est pas la signification retenue par la CNIL, on va le voir. Nous allons pour cela intervertir l'ordre chronologique, en évoquant l'acception de la CNIL (1) avant la nôtre (2).

1. L'acception de la donnée de santé « par destination » selon la CNIL

Nous voyons ici la typologie des données de santé présentée par la CNIL (a), avant de relever que la loi de 2019 et les textes d'application de 2021 et 2022 confortent son approche (b), sans priver notre questionnement initial de son fondement, ni de ses applications.

a. La typologie des données de santé par la CNIL

Dans sa doctrine (cette distinction n'est donc pas de source légale ni réglementaire), la CNIL trois types de données de santé, dont celle par destination [496] :

* Les données de santé **« par nature »** qui recouvrent les « *antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc*. ».

* Les données de santé **« par croisement »** avec d'autres données : elles « *deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques...), croisement de la tension avec la mesure de l'effort, etc.* » [497].

* Les données **« par destination »**. Elle les entend comme « *celles qui deviennent des données de santé en raison* ***de leur destination,*** *c'est-à-dire de l'utilisation qui en est faite au plan médical* » [498].

---

[496] www.cnil.fr/fr/recherche/données de santé (sept 2020).
[497] *Ibid*. « celles, qui du fait de leur croisement avec d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques...), croisement de la tension avec la mesure de l'effort, etc. ».
[498] *Ibid.*

b. Les données « par destination » selon la CNIL : apport doctrinal ?

Peut-être ne s'agit-il là que d'une nuance d'expression ? au moment de sa publication, son acception de la donnée « par destination » nous semblait discutable [499]. En effet, le concept ne nous semblait opérant (apporter à la réflexion), que si la donnée « par destination » était définie **par sa signification médicale, pas seulement par son utilisation au plan médical**.

A défaut, n'y aurait-il pas tautologie ? on percevrait mal la distinction de la donnée « *par destination* », d'avec la donnée « *par nature* » produite par les professionnels, établissements ou technologies de santé au sens organique du CSP, ce qui est en fait une donnée de santé « par sa source » (*supra*). En outre, les exemples donnés de ces dernières par la CNIL (« *antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc*. ».) **nous semblent à chaque fois correspondre à des états diagnostiqués ou traités au sein du système de santé**.

Mais la question sans doute alors posée sans être explicitée, est celle de la génération et de l'utilisation de données hors du système de santé au sens organique, car l'attraction de la donnée pour une utilisation médicale **soumet au statut de « donnée de santé » sans qu'il y ait là matière à discussion.**

Or, **une donnée peut avoir une signification médicale, sans conduire à une utilisation au plan médical**. Cela pose la question de savoir **comment elle est générée, par qui et pour quoi elle est exploitée, sous quel statut elle peut être cédée.** Cela peut désormais être le cas en dehors du système de santé, et même en connexion avec lui, lorsque ces données externes lui sont transférées (*infra*).

Si l'on assigne à la notion de « donnée de santé » à quel titre que ce soit, le rôle de déclencher une protection juridique renforcée, **force est de constater que la situation ne se limite pas à l'utilisation médicale, qui réinscrit la donnée dans le système et la couvre de sa protection.**

[499] E. Pinilla, F. Megerlin, « De la donnée de santé par qualification de la loi, à la donnée de santé « par destination », Rev. gén. dr. méd 2018/1, 99-112.

2. La qualification de la « donnée par destination : notre approche

Dans notre recherche de 2017 parue en janvier 2018, nous avions proposé de distinguer les notions de données de santé « par qualification de la loi » et données « par destination » [500], pour distinguer leurs lieux et modes de génération, et cadre d'exploitation (a). En droit européen, la définition met en exergue la destination, avant même le cadre de production (b).

a. la place des données générées hors de la prestation de soins

Nous avons proposé d'utiliser la notion de données de santé « *par qualification de la loi* » pour décrire les données issues de **l'activité organique du système de santé (et médico-social), dans lesquelles elles sont encloses et protégées** au titre de L. 1110-4 CSP.

Or, ce qui marque en 2002 un progrès très bienvenu dans les droits du patient (l'unification de la protection de ses données dans le système de santé, indifféremment quant au régime d'action professionnelle), ne nous semblait pas permettre de cerner le spectre informationnel pertinent – c'est-à-dire ici méritant une vigilance renforcée pour la protection des personnes.

A contrario, nous avons proposé la notion de donnée de santé « *par destination* » pour décrire les données externes à l'activité organique des systèmes de soins : elles n'y **sont pas nativement encloses, et n'y seront pas protégées** au titre de L. 1110-4 CSP : il s'agit de tous les outils et services susceptibles de produire des données possédant simplement une signification, non nécessairement une utilisation, médicale [501].

Cette notion nous sert alors à soulever la question du cadre de leur production et détention, et protection : données personnelles certes ; mais protégée par un droit spécifique, ou par le seul droit commun ? La question se pose du fait de leur potentiel applicatif diversifié : **évidemment, mais pas seulement, ni prioritairement, ni même nécessairement, médical.**

[500] Pinilla E, Megerlin F, « De la donnée de santé par qualification de la loi » etc. préc. RGDM 2018(1), 99-112.
[501] Et non attirés dans l'ENS, car cela induit au moins en théorie, une utilisation médicale.

b. Quelle place relative des données générées dans le cadre de prestations des soins ?

Cette question est posée dans le règlement de 2016 sur la protection des données. Son considérant n° 35 postule que « *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 (…)* ». Or, cela est extraordinairement vaste.

Certes, du point de vue normatif, le règlement les définit ensuite de façon resserrée comme les « *données à caractère personnel* ***relatives à la santé*** *physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé****, qui révèlent des informations sur l'état de santé*** *de cette personne* » (article 4-15°).

Or, cela reste tautologique. Surtout, cet article nous sembler **inverser l'ordre du raisonnement** : dans le règlement de 2016, le contexte de « *prestation de services de soins de santé* » n'apparaît qu'un cadre de génération parmi d'autres : (« (...) *y compris la prestation* (...) »). Paradoxalement, il n'apparaît pas le cadre primordial natif de génération des « données de santé ». La diversité des circonstances et technologies de capture et de traitement des données n'est que suggérée ; le rattachement terminal (« y compris ») de la prestation de services de soins de santé, semble conférer à celle-ci un caractère résiduel. Ce choix rédactionnel **ne vaut certes pas pondération juridique**, mais nous le verrons non isolé.

En tous cas, il est à nouveau acté que l'activité du système de santé au sens organique **n'est plus le seul cadre de génération, ni d'emploi de telles données**. Cela était préfiguré dès le règlement 2017/745 relatif aux dispositifs médicaux [502] : il acte l'existence possible de technologies duales, et organise leur régime à l'avance :

* Ainsi, l'article 1.3 dispose que **«** *Les dispositifs* ***ayant à la fois une destination médicale et non médicale*** *respectent les exigences applicables aux dispositifs ayant une destination médicale et celles applicables aux dispositifs n'ayant pas de destination médicale* ».

* De même, l'article 1.5 dispose que « *Lorsque cela se justifie* ***en raison du caractère similaire d'un dispositif ayant une destination médicale*** *mis sur le marché* ***et d'un produit n'ayant pas de destination médicale*** *quant à leurs caractéristiques et à leurs risques, la*

[502] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

Commission est habilitée à adopter des actes délégués conformément à l'article 115 pour modifier la liste de l'annexe XVI ***en ajoutant de nouveaux groupes de produits*** *afin de protéger la santé et la sécurité des utilisateurs ou d'autres personnes, ou compte tenu d'autres aspects liés à la santé publique* ».

B. LA CONSECRATION DE LA NOTION DE DONNEE DE SANTE « PAR DESTINATION » ?

La pertinence de la notion de « donnée de santé par destination », qui n'est, rappelons le, pas à l'origine une catégorie juridique, mais une accroche de l'attention, a **depuis été validée** dans cette double acception doctrinale, tant au plan du droit national (1) qu'européen (2).

1. La consécration de la "donnée de santé par destination" en droit français

La création de l'ENS en 2019 et la possibilité d'intégration à compter de 2022 d'outils et services référencés dans ce cadre (a) met en exergue la production de données en marge du système de santé, qui peut – mais aussi pourrait ne pas – y trouver d'utilisation médicale (b).

a. Les données produites par l'intégration dans l'ENS d'outils numériques référencés

Pour rappel, la loi a en 2019 créé l'espace numérique de santé (ENS), permettant l'accès de son titulaire à la réunion personnalisée de bases de données par ailleurs définies de façon autonome [503] . En 2021, la partie réglementaire du Code de la santé publique a été complétée en conséquence [504]. Depuis, un arrêté de juin 2022 précise les critères de référencement des outils et services numériques intégrables dans l'ENS [505]. **Quelle pertinence ici ?**

En premier lieu, nous avons relevé que les données pouvaient être produites par les outils et services numériques référencés au sens de L. 1111-13-1-III, sachant que ceux-ci ne relèvent pas nécessairement de la qualification de technologie médicale.
Cela fait qu'il s'agit d'une production de données **qui n'est pas le fait du système de santé au sens organique** des professionnels, établissements et technologies médicales telles que définies par le CSP.

[503] Article 45 II de la loi n° 2019-774 du 24 juillet 2019.
[504] Décret n° 2021-1048 du 4 août 2021 relatif à la mise en œuvre de l'espace numérique de santé NOR : SSAD2112391D
[505] Arrêté du 23 juin 2022 relatif aux critères applicables au référencement des services et outils numériques au catalogue de service de l'espace numérique de santé - NOR : SPRD2214799A, JO 5 juillet 2022.

En outre, les données dont il s'agit sont :

* des « ***constantes de santé éventuellement produites par des applications ou des objets connectés référencés*** *(...)* ***ou toute autre donnée de santé utile*** *à la prévention, la coordination, la qualité et la continuité des soins* », ce qui les assimile à des données de santé, quand bien même elles ne résulteraient pas de dispositifs médicaux (ibid., II-3°) ;

* les données issues de « ***tout service numérique****, notamment des services développés pour favoriser la prévention et fluidifier les parcours, les services de retour à domicile, les services procurant une aide à l'orientation et à l'évaluation de la qualité des soins, les services visant à informer les usagers sur l'offre de soins et sur les droits auxquels ils peuvent prétendre* ***ainsi que toute application numérique de santé*** *référencés* » (ibid., II-6°), le tout concrétisé dans l'arrêté de 2022 pour les conditions pratiques de référencement.

b. Des dispositifs sans destination médicale, mais produisant des données de santé

Nous avons vu que les « outils ou services numériques » visés par la loi de 2019, le décret de 2021 et l'arrêté de 2022, n'étaient pas nécessairement des dispositifs médicaux.

Parlant des données produites, on peut donc bien évoquer des données qui selon la CNIL « *deviennent des données de santé en raison* ***de leur destination,*** *c'est-à-dire de l'utilisation qui en est faite au plan médical* », car elles ne le sont pas « par nature », ni nécessairement (quoi que virtuellement) par croisement. **Leur inscription dans l'ENS l'établit suffisamment**.

Mais force est de constater que les mêmes technologies qui ne pourraient, ou ne voudraient pas répondre aux critères de référencement, n'en sont pas moins commercialisables ; qu'elles n'en produisent pas moins des données, qui seulement **ne seront pas inscrites dans l'ENS**. Or, si les mêmes données **ne connaîtront pas d'utilisation médicale** au sens des finalités de l'ENS, elles **n'en possèdent pas moins une signification médicale, ce** qui devrait conduire à réfléchir à leur protection. Tel était le sens de notre doctrine.

Enfin, dans la proposition de règlement relatif à l'Espace européen des données de santé (EEDS) en mai 2022, est présentée une définition de l'« *application de bien-être* », avec une vocation normative : il y s'agit de tout appareil ou logiciel destiné par son fabricant à être

utilisé par une personne physique *« **pour le traitement de données de santé électroniques à d'autres fins que les soins de santé,** par exemple à des fins de bien-être ou de poursuite de modes de vie sains* » (article 2.2.o) [506].

Or, ces données feront partie des données susceptibles d'intégration dans le dossier médical électronique, et d'utilisation secondaire à ce titre, *infra*.

c. Enjeux de données de santé « *par destination* » hors du système de santé

L'enjeu est ici la production, la signification par croisement comme l'a souligné la CNIL, et l'usage de telles données hors des systèmes et finalités de soins : massives, ces données sont la matière première des actuaires, voués aux modélisations prédictives en matière de risques pour l'assurance et la gouvernance. Affinées, ces données permettent le profilage individuel pour le démarchage commercial, la génération de services personnalisés, mais aussi l'induction de besoins/désirs/craintes selon les centres d'intérêt/sensibilités etc. **bien au-delà donc d'une « utilisation secondaire » légitime**.

En outre, de telles données et leur recoupement éventuel sont à la base de la modulation potentielle de conditions contractuelles (cartes de fidélités, etc.), jusqu'à la discrimination (illégale en France) dans l'accès aux assurances, à l'emprunt, l'emploi, le logement, etc.

Or, l'institution même du « droit à l'oubli », lequel en France décrit la permission légale de ne pas déclarer des antécédents médicaux sans que ce point constitue un mensonge [507], n'empêche pas le **raisonnement par inférence** à partir d'informations semées (des requêtes tracées par cookies jusqu'aux imprudents échanges explicites sur forums ou réseaux sociaux) et recoupées hors du système de soins, et permettant parfois la ré-identification de patients [508]. **Et cela pas pour une utilisation médicale**.

---

[506] Voir l'analyse approfondie de Megelrin F, Fascicule 8-10 « Données de santé », *in* Traité de droit pharmaceutique Litec, Jurisclasseur LexisNexis (2023).
[507] Institué par la loi du 26 janvier 2016 (décrets 7 et 13 fév. 2017), suite de la convention AERAS née en 2001.
[508] McCoy TH Jr, Hughes MC, » Preserving Patient Confidentiality as Data Grow Implications of the Ability to Reidentify Physical Activity Data », JAMA Network Open 2018;1(8):e186029 ; Na L, Yang C, Lo C-C, Zhao F, Fukuoka Y, Aswani A. « Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning ». JAMA Netw Open. 2018;1(8):e186040.

Dès lors, c'est ici un raisonnement par l'absurde, il serait curieux que les données produites par des technologies non médicales, mais référencées selon la loi de 2019, soient des « *données de santé par destination* » sous prétexte qu'elles abondent l'ENS ; tandis que des technologies non médicales non référencées, produiraient des données qui ne seraient pas « de santé par destination », *par simple défaut de rattachement à l'ENS* (ou au Dossier médical électronique, pour prendre la terminologie européenne à venir).

En effet, dans les deux cas, une protection renforcée ne s'impose-t-elle pas ? On va voir pourquoi, avec le spectre d'activités non couvert, malgré l'élargissement en 2022 de la notion de donnée de santé par le droit européen. On sent dès ici les limites du paradigme classique.

2. L'élargissement en 2022 de la notion puis de la catégorie : à quel point ?

Présentée en mai 2022, la proposition de règlement européen sur un espace européen des données de santé [509] rappelle que le traitement des données de santé à caractère personnel doit être conforme au règlement (UE) 2016/679 ; pour les traitements opérés par les institutions et organes de l'Union, qu'il doit être conforme au règlement (UE) 2018/1725.

Nous avons relevé *supra* que le premier **porte une définition normative de la données de santé,** à laquelle le second renvoit en **invoquant un principe « d'homogénéité d'inteprétation »** [510]. Mais nous avons aussi relevé que la définition de la donnée de santé (article 4.15) y est plus étroite que son appréhension par son considérant n° 35.

Or, **le considérant n° 5 de la proposition de règlement de 2022 va encore au-delà des termes du considérant n° 35 du règlement de 2016 :** les « *données de santé électroniques à caractère personnel pourraient inclure des données à caractère personnel relatives à la santé physique ou mentale d'une personne physique* (…) » (le considérant joint les données génétiques)*, « **ainsi que des données sur des facteurs déterminants pour la santé, tels que le comportement, les facteurs environnementaux, les influences physiques,** les soins médicaux **et les facteurs sociaux ou éducatifs** »* **(…).**

[509] Proposition de Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM (2022) 197 final 2022/0140(COD). Développé en Partie II, titre II.
[510] Règlement n° 2018/1725, considérant n°5, voir *supra*.

Nous allons voir que ce considérant marque un élargissement significatif de la catégorie juridique (a) ; on peut se demander à quel point (b).

a. Un élargissement significatif de la notion, jusqu'à la catégorie juridique

Dans les textes européens précités, il est arrivé de voir des considérants ambitieux en forme de pétition de principe, sans que la norme annoncée ne remplisse pleinement le périmètre esquissé. Tel ne va pas être le cas ici : **on va voir le « bien-être » distingué de la « santé », mais pour en être mieux rapproché dans la définition de la « donnée de santé »**, sachant que, dans la définition de l'OMS, ces notions sont consubstantielles [511].

En premier lieu, l'invocation des « facteurs sociaux » ou « éducatifs » **marque une extension conceptuelle considérable.** En outre (dans le même considérant), un autre point essentiel, est que **«** *Les données de santé électroniques concernent toutes les catégories* ***de ces données, indépendamment du fait que ces données sont fournies par la personne concernée ou par d'autres personnes physiques ou morales****, telles que des professionnels de la santé,* ***ou sont traitées en relation avec la santé ou le bien-être*** *d'une personne physique* » (considérant 5).

Certes, ceci n'est à la date de la rédaction de notre thèse, qu'une proposition. Mais ce projet de considérant n°5 en 2022 est congruant avec le considérant n° 35 de 2016 (*supra*); **il en constitue une extension conceptuelle** : **ces éléments ne figuraient pas dans le droit européen antérieur, ni dans le droit français**. On pourrait certes arguer qu'il ne s'agit ici que d'élargissement de considérants, sans portée normative, d'ambition donc philosophique.

Mais l'article 1.2 a) de la proposition de 2022 (composante donc, du *corpus* normatif), **ne se contente pas de renvoyer au RGPD de 2016** : **il en étend la définition normative,** sous réserve de l'adoption à venir de la proposition publiée : ainsi, on entend par données de santé électroniques à caractère personnel, « l*es données concernant la santé* ***et les données génétiques*** *telles que définies dans le règlement (UE) 2016/679,* ***ainsi que les données se rapportant aux déterminants de la santé,*** *ou les données traitées dans le cadre de la prestation de services de soins de santé,* ***qui existent sous forme électronique*** ».

[511] Cf. introduction, définition de la santé par l'OMS en 1946.

Il n'est pas ici précisé ce que l'on entend par « prestation de soins de santé »; ce n'est par ailleurs pas le centre de gravité de la phrase, mais un dérivé : « *(...) ou les données traitées dans le cadre de (...) »*. Nous avons relevé supra qu'il ne fallait sans doute pas lire de pondération juridique dans ce choix rédactionnel, même s'il est récurrent [512].

b. L'élargissement de la catégorie, à quel point face aux nouveaux phénomènes ?

La notion de « prestation de soins de santé » peut désormais on l'a vu, englober des systèmes connectés mis en oeuvre en dehors du système de santé. En outre, la mesure des déterminants de santé **peut être le fait de capteurs, senseurs** etc. **qui n'ont pas ou n'ont plus de lien avec une prestation de soins** ; cette dernière peut par ailleurs ne plus procèder de technologies médicales, dont la mise en oeuvre induirait la qualification de donnée de santé.

Or, l'objectivation de données d'activité (comportements, corrélés à des environnements etc.) rapportées à une personne permet des comparaisons dans le temps et l'espace, inter-individuelles et populationnelles, voire des préconisations ou recommandations sur cette base, dans le domaine hygiéno-diététique, puis sportif, alimentaire voire social et spirituel etc.

* Cela peut conduire à la « normopathie », lorsque l'individu croit devoir imiter les performances invoquées, ou se voit enjoint par des médias ou réseaux de ce faire [513]. L'induction de comportements individuels et populationnels par ces outils simples est en soi un enjeu déjà critique.
Avant cela même, le Conseil d'Etat souligne lumineusement en 2018 que « *les instruments de* quantified self *introduisent une logique anxiogène de médicalisation « rampante », au nom de laquelle les individus acceptent de se soumettre à des injonctions comportementales, fussent-elles implicites, pour conjurer les risques éventuels censément révélés par les données ainsi recueillies* » [514].

* Le risque d'influence individuelle, voire insidieusement car discrètement populationnelle, est considérablement **renforcé avec le développement des agents conversationnels,** lesquels

[512] Déjà l'article 4-15° du RGPD, la « prestation de services de soins de santé » n'apparaît qu'un cadre de production des données de santé parmi d'autres ("(...) *y compris la prestation* (...)"). Elle n'apparaît pas le cadre premier, natif, de production des « données de santé », mais cela relève sans doute du choix rédactionnel, *supra*.
[513] Buin, Y. (2003) 'Normopathie', Le Passant Ordinaire. Revue Internationale de Création et de Pensée Critique, 45-46
[514] Conseil d'Etat, 2018, Loi bioéthique - Rapports et Etudes, p 196.

visent une information personnalisée sur la base, rapportée en 2023, d'un dialogue mimé par un programme interactif ; cela bien au-delà des usages classiques de ces « *chatbots* » [515].

Cela introduira aussi la question d'injonctions toujours plus invasives et puissantes, car cette fois d'apparence personnalisées, sur la base des données générées et recoupées, selon les écarts mesurés au regard de cibles recommandées ; **potentiellement donc l'induction d'états physiologiques et psychologiques, hors système et buts de santé**, donc hors « *prestation de soins de santé* » au sens de l'article 1.2-a de la proposition de règlement de 2022.

Il n'est pas lieu de développer ici l'induction possible, charlatanesque voire stratégique, de comportements ou de soins inappropriés voire dangereux ; ce risque sera explicitement pris en compte par le Règlement (UE) 2022/2065 sur les services numériques de 2022 (*infra*) [516]. Rappelons que des agents conversationnels sont utilisés en soins psychiatriques, mais que d'autres ne possédant pas cette visée ont conduit hors de cette finalité à des cas de suicide. Nous avons aussi relevé le potentiel d'encapsulation de tests type MBTI etc. dans des jeux vidéos, pour une finalité de profilage psychologique des joueurs, outre l'évaluation de leurs performances face à des *stimuli* variés.
Enfin, outre l'activité des influenceurs, des applications populaires de réseaux sociaux de portée internationale font actuellement l'objet d'enquêtes parlementaires pour induction de comportements dangereux (loisir, hygiène, alimentation, santé), ou suspicion de profilage d'utilisateurs de tous âges et de tous niveaux de responsabilités.

Ainsi, cette proposition en 2022 acte tant dans son considérant que corpus normatif, la dynamique de la notion de « donnée de santé » dans le sens observé durant nos recherches et publications : une définition du contenu, au contexte. Mais l'adoption du règlement européen dans les termes proposés pourrait **aboutir à une extension significative de la catégorie**

---

515 P. Lee, S. Bubeck, J. Petro, « Benefits, Limits, and Risks of GPT-4 as an AI Chatbot for Medicine », N Engl J Med 2023; 388:1233-1239.

516 Règlement (UE) 2022/2065 du Parlement et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE. Citons dès ici son considérant n° 83 : « *Une quatrième catégorie de risques découle de préoccupations similaires relatives à la conception, au fonctionnement ou à l'utilisation,* ***y compris par manipulation,*** *de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne ayant un* ***effet négatif réel ou prévisible sur la protection de la santé*** *publique et des mineurs, ainsi que des co****nséquences négatives graves sur le bien-être physique et mental*** *d'une personne, ou sur la violence à caractère sexiste. Ces risques peuvent également* ***résulter de campagnes de désinformation coordonnées liées à la santé publique ou de la conception d'interfaces en ligne susceptibles de stimuler les dépendances comportementales*** *des destinataires du service*. »

juridique de notion de donnée de santé [517], hors d'un contexte de recherche biomédicale. Voyons maintenant ce qu'il en est dans un tel contexte.

SYNTHESE P1T2C1

Ce premier chapitre du **Titre II « définition de la donnée de santé, du contenu au contexte »** était le cadre de restitution de nos observations, de plus en plus prospectives, de la dynamique de la notion de « donnée de santé » désormais autonome, en dehors du cadre de la recherche, c'est à dire dans les pratiques courantes de soin et de suivi de santé, dans lequel nous approfondissons la distinction que nous avions publiée en 2018.

* Dans une première section, nous identifions des données dont le statut n'est pas douteux, car il s'agit de donnée nativement de santé « par qualification de la loi ». Nous y relevons comment les données peuvent ainsi être qualifiées selon un critère « organique » posé par la loi même, de production au sein du système de santé ou par une technologie qui en relève ; mais aussi selon un critère « matériel » que nous proposons : des données de production non organique selon les critères légaux, peuvent être attraites dans des bases qui ont le statut « santé ». C'est le cas pour les bases institutionnelle comme le système national des données de santé (SNDS) depuis 2016, ou personnelle comme l'espace numérique de santé (ENS) depuis 2022, lequel anticipe en France l'obligation du Dossier médical électronique (DME) portée par la proposition de règlement européen sur l'espace européen des données de santé.

* Dans une seconde section, nous relevons le problème de qualification de données qui ne sont ni produites par, ni aspirées dans le système de santé. Des difficultés d'appréhension naissent du fait que des fabricants de technologies de biocapteurs et biosenseurs cherchent à en dénier la qualification médicale, afin d'éviter le régime de certification légale des dispositifs médicaux, éventuellement d'en éluder la qualification « de santé » des données. Cela nous avait conduit à nous interroger sur un nouveau critère de qualification, de données de santé « par destination », proposition que nous approfondissons pour distinguer du sens ensuite donné par la CNIL. Nous relevons que la dynamique européenne depuis, conforte la

[517] Rappelons que cela ne peut servir que d'alerte intellectuelle, à moins d'une extension forte de la protection renforcée dans le futur aux données jusqu'alors conçues selon le droit de 2016.

distinction que nous avions proposée, du fait de l'hybridation des données, et de l'avènement annoncé d'une nouvelle catégorie plus vaste : les « données de santé électroniques ».
Le but n'est pas de proposer un nouveau statut juridique, mais de pointer l'affaiblissement ou plutôt le dépassement nécessaire du régime existant à l'aube même de son édification, nombre de données « non santé » intéressant la santé. En fait, un nouveau statut apparaîtra (IInde partie), à la lumière de l'abondement du DME par les applications de « bien être » si elles sont enregistrées selon le droit européen à venir.

CHAPITRE II. DYNAMIQUE DE LA DONNEE DE SANTE DANS LE CADRE DE LA RECHERCHE

Après l'analyse de la dynamique de la notion en contexte de soins/ d'accompagnement et d'auto-mesure/analyse de soi (poursuivant ou non une finalité médicale), nous examinons ici sa dynamique **en contexte de recherche, où elle est mue par d'autres moteurs**.

Certes, la protection des données n'y est pas séparée de la protection générale des données de santé. En outre, nous ne traiterons pas de l'hypothèse où une communication scientifique rapportant un cas clinique, publie des données à caractère personnel dans l'intérêt public avec l'accord du patient : cela relève des « pratiques altruistes », précédemment évoquées [518].

Par « recherche », nous entendons ici tout à la fois, d'une part, la recherche scientifique et clinique qui vise au **développement initial** de technologies et de services nouveaux en santé. Cela relève d'un cadre juridique particulier, propre aux études interventionnelles et observationnelles (section 1).
D'autre part, une recherche qui participe **de l'« *utilisation secondaire* » des données** : elle peut viser à la compréhension des performances (système, technologies, organisations etc.) et comportements (individus, institutions, marchés etc). Ses buts vont de la R&D et de la santé publique jusqu'au *marketing*, non sans potentiel d'application géopolitique (section 2).

[518] *Supra*. Depuis 2022, le partage « altruiste » relève d'une politique nationale autonome, dont le cadre est depuis 2022 défini à l'échelle européenne lorsque des institutions publiques et intermédiaires sont impliqués.

SECTION 1. DYNAMIQUE DE LA GENERATION DES DONNEES DANS LA RECHERCHE BIOMEDICALE

En France, il aura fallu attendre en 1988 la loi « Huriet-Sérusclat », pour poser le premier cadre juridique de la recherche pratiquée sur l'être humain [519]. Son paradigme a changé en 2012 avec la loi « Jardé » : cette loi pose un concept beaucoup plus large : le critère n'est plus que la recherche soit « *pratiquée sur* », mais qu'elle « *implique* » la personne humaine [520].

Or, les conséquences sont importantes. Leur découverte au fil de l'application de la loi de 2012, puis de l'ordonnance de 2016 qui la modifie sans altérer son architecture, va **appeler de multiples correctifs réglementaires et jurisprudentiels** : la multiplication des exceptions conduit d'ailleurs à se demander si ce cadre a une vocation pérenne : c'est une facette de nos travaux publiés, le professeur Huriet nous ayant honoré de sa confiance [521].

Mais ce qui nous intéresse ici, est la diversification des catégories d'études participant de la recherche scientifique pouvant générer ou mobiliser des données de santé (§1). On peut en effet s'interroger sur la **catégorisation juridique des données produites** selon les différents types de recherche, dont l'objet et le grade de sensibilité ne sont pas les mêmes (§2).

§1. CATEGORISATION DES ETUDES PARTICIPANT DE LA RECHERCHE

La recherche non-interventionnelle se distingue de la recherche interventionnelle. Seule cette dernière désigne la recherche biomédicale pratiquée sur l'être humain : la première loi française qui l'a encadrée, dite « loi Huriet-Sérusclat », a notamment distingué selon que cette recherche possédait ou non un bénéfice direct pour les personnes, a créé les Comités de protection des personnes qui s'y prêtent (CPPRB), et institué leur avis consultatif sur les projets qui leur sont impérativement soumis [522]. Ce paradigme fondateur a inspiré la directive européenne de 2001, qui a harmonisé la protection des personnes dans l'Union [523].

---

[519] Loi n°88-1138 du 20 décembre 1988 relative à la protection des personnes se prêtant à la recherche biomédicale, dite loi « Huriet-Sérusclat ».
[520] Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine, dite loi « Jardé ».
[521] F. Megerlin, E. Pinilla, Cl. Huriet, « Etudes observationnelles et données de santé « par destination » : quelles protections en droit ? », Rev Gen Dr Méd 2021(1), 151-164.
[522] Loi n°88-1138 du 20 décembre 1988 préc.
[523] Directive sur les essais cliniques de médicaments (2001/20/CE) ; abrogée par le Règlement (UE) n° 536/2014 du Parlement et du conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain.

Or, ce cadre été modifié en 2012 par la loi dite « loi Jardé », laquelle institue une « *protection des personnes impliquées dans la recherche humaine* » (RIPH). Le but n'est plus l'encadrement éthique de la recherche biomédicale *« **pratiquée sur** »* l'être humain, mais une prétention à protéger toute personne *« **impliquée dans** »* la recherche en santé, à quelque titre que ce soit [524]. Depuis lors, à l'instar des projets de recherche interventionnelle, tous projets de recherche non interventionnelle doivent être soumis à l'examen des Comités de protection des personnes (CPP) [525], dont l'approbation est devenue obligatoire (L. 1121-4 CSP).

Cette loi a été modifiée en 2016 sans évolution de son architecture [526], laquelle nous intéresse seule ici : elle réunit recherche interventionnelle et non interventionnelle, cette dernière étant définie par le Règlement européen de 2014 (substitué à la directive européenne de 2001) comme « une étude clinique **autre qu'un essai clinique** », soit « *toute investigation **en rapport avec** l'homme, destinée à* » etc. [527]. « Pratiquée sur », « impliqué dans », « en rapport avec », « participe à » (*infra*) : la diversification conceptuelle – non seulement sémantique – des rattachements juridiques et l'élargissement technologique du potentiel de recherche mettent à l'épreuve la catégorisation des RIPH et des données qui en résulte.

Nous constatons ici comment la mise en pratique du critère de définition et de rattachement au cadre de la RIPH en 2012, en a rapidement révélé les limites. A côté du droit de la recherche **« impliquant »** la personne humaine (A), il a fallu par un tour de prestidigitation juridique, conceptualiser un droit de la recherche **n'impliquant pas** la personne humaine (B) ; mais cette dernière ne génère-t-elle pas moins des données de santé ?

A. LE DROIT DE LA RECHERCHE « IMPLIQUANT » LA PERSONNE HUMAINE

Le critère juridique de « *l'implication* » est très large, le concept n'étant pas auto-explicatif (à la différence celui de recherche « *pratiquée sur* »). Il vise à appliquer à la personne, des protections additionnelles consistant notamment en l'activation préalable et impérative des Comités de Protection des Personnes (CPP [528]) ; et en l'application de méthodes dédiées au

[524] Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine, dite loi Jardé.
[525] Les CPPRB sont devenus CPP depuis la loi n°2004-806 du 9 août 2004.
[526] Ordonnance n°2016-800 du 16 juin 2016.
[527] Article 2, 4° du Règlement n° 536/2014 préc. La suite de cet article 2 s'inscrit dans un contexte purement médicament. Cette définition n'a pas de pendant dans le Règlement (UE) 2017/645 en matière de dispositifs médicaux, ni dans la Directive 2001/83 CE instituant un Code communautaire du médicament à usage humain.
[528] Qui ont remplacé les CCPPRB.

traitement de l'information, les « méthodologies de référence » (MR) élaborées par la CNIL, on le verra *infra*, **ce qui aboutit de façon indiscutable à des données de santé.**

Nous voyons ici la dichotomie initiale des régimes de recherche recouverts par le concept de RIPH (1), avant de relever la porosité depuis 2012 des catégories du droit (2).

1. La dichotomie juridique initiale entre recherche « interventionnelle » et « observationnelle »

Toutes les RIPH sont soumises à des procédures d'approbation par les CPP, selon des régimes plus ou moins contraignants. Sous couvert de RIPH, la loi de 2012 a réuni les recherches interventionnelles (a) et non-interventionnelles, dites donc « observationnelles » (b).

a. La catégorie juridique de la « recherche interventionnelle »

Les recherches interventionnelles sont définies par les risques. Ces risques peuvent être physiques et/ou psychiques pour la personne qui s'y prête. Le législateur de 2012 a distingué deux cadres, correspondant à des procédures de validation plus ou moins contraignantes devant les CPP.

* Le premier cadre est celui d'une **intervention « non justifiée par (la) prise en charge habituelle** » (L. 1121-1-1° CSP) comme par exemple l'essai de nouvelles molécules, technologies médicales, actions chirurgicales, combinaisons inédites etc.

* Le second cadre est celui de **recherches interventionnelles présentant des « risques et contraintes minimes »** (L. 1121-1-2° CSP), concrétisées par un arrêté de 2018, lequel abroge le précédent [529].

Cette distinction détermine le régime des projets soumis aux Comités de protection des personnes (CPP) : dans le cas L. 1121-1-1° CSP, l'autorisation par l'Agence nationale de sécurité des médicaments s'impose **en sus** de l'approbation des CPP. Dans le cas L. 1121-1-2° CSP, cette dernière est seule requise, ce qui fait des CPP une instance consultative obligatoire et surtout décisionnelle.

[529] Premier arrêté du 12 avril 2018 NOR (SSAP1810239A) fixant la liste des recherches mentionnées au 2° de l'article L. 1121-1 du code de la santé publique. Il abroge l'arrêté du 3 mai 2017 de même objet.

b. La catégorie juridique de la « recherche observationnelle »

En contraste des précédentes, les recherches non interventionnelles **sont réputées sans risque**. Elles sont régies par L.1121-1-3° CSP et dites « observationnelles », car l'observation des personnes (parcours de soins, effets de thérapies courantes, etc.) est leur unique but. L'action ne vise pas à générer une donnée sur une situation d'intervention inédite, mais à **recueillir des données produites lors de situations de routine**.

Depuis 2012, les recherches observationnelles n'en sont pas moins également soumises à l'**approbation obligatoire des CPP**. Cette catégorie est *a priori* claire, à défaut d'être utile pour l'éthique de la recherche biomédicale sur la personne humaine : il y a en effet antinomie entre recherche « pratiquée sur », et « non interventionnelle ». On peut s'interroger sur la contribution à la protection des personnes ; on verra que « l'avis éthique » est en fait requis, car devenu un critère de publication de résultats dans des revues scientifiques internationales. Cela conduit à un fondement mixte d'intervention des CPP, et une prétention discutable à garantir la *qualité* des études et donc des données, on le reverra *infra*.

L'expression « recherche impliquant » prétend ainsi réunir deux univers conceptuels différents, non sans confusions potentielles : cela a conduit le législateur à devoir préciser qu' « ***en cas de doute sérieux sur la qualification*** *d'une recherche au regard des trois catégories de (RIPH) définies à l'article L. 1121-1, le CPP concerné saisit pour avis l'Agence nationale de sécurité du médicament et des produits de santé* » (L. 1121-4).

Or, le doute s'est instillé, appelant de nouvelles précisions.

2. La porosité des catégories légales depuis 2012

a. L'introduction *praeter legem* de recherches interventionnelles « sans risque »

En avril 2018, un second arrêté précise les « actes ou procédures dénués de risques » pouvant bénéficier du cadre procédural allégé de ce 3°, à la condition d'être « décrits et justifiés dans le protocole de recherche » [530]. Or, ce faisant, il n'établit pas une liste de recherches « non interventionnelles sans risque ni contrainte » : il fait référence à des actes et procédures spécifiques à une recherche interventionnelle, **que L. 1121-1-3° était censé exclure.**

[530] Second arrêté du 12 avril 2018, NOR : SSAP1810240A.

En bref, cet arrêté introduit une quatrième catégorie de RIPH [531] : celle des recherches « interventionnelles sans risques » (car conformes à la pratique courante).

Or, cela **relève du tour de bonneteau juridique**, car l'article L. 1121-1-3° ne prévoyait pas une telle liste. En 2019, dans le cadre d'un contentieux de la légalité de l'action administrative, le Conseil d'Etat a tout aussi habilement jugé qu'il n'y avait pas là d'excès de pouvoir : il *« résulte nécessairement* (de l'article L. 1121-1-2°) *que le ministre est également compétent pour énumérer celles des recherches qui ne relèvent pas du 2° de cet article mais entrent dans le champ du 3° du même article* » [532].

Rendu nécessaire par les conséquences de la loi, **ce pragmatisme est certes à saluer. Mais**, si un doute pouvait déjà exister entre les catégories L. 1121-1-1° et 2°, le doute est désormais aussi possible entre les catégories L. 1121-1-2° et 3°. En tous cas, **la distinction recherche « interventionnelle » / recherche « observationnelle » ne départage plus les régimes** : le critère de rattachement aux procédures est devenu le risque pour la personne.

b. Le critère de rattachement est devenu l'appréciation du risque.

L'appréciation du risque ne va pas toujours de soi, les arrêtés de 2018 et l'arbitrage de l'ANSM l'établissent. En outre, elle est potentiellement polarisée pour des motifs tant économiques qu'idéologiques. On peut imaginer des doutes de CPP, quant à savoir si une recherche à « risque minime » peut être considérée comme « dénuée de risque », si le principe doit être le « consentement express » ou la « non-opposition » de la personne (L. 1122-1-1).

Certes, afin d'alléger les procédures en contexte de Covid19, l'Ordonnance d'avril 2020 a prévu une accélération de l'examen dans le cas de L. 1121-1-3° CSP [533]. Mais, depuis l'Ordonnance de juin 2020 qui s'en est suivie, cet accélération ne **semble** plus devoir bénéficier aux recherches interventionnelles **mêmes si « dénuées de risque** » [534].

---

[531] En ce sens, Th Roche, C Lauria : « Loi Jardé, le chantier continue encore et toujours : publication de deux nouveaux arrêtés » ; Blog sciences du vivant, Delsol Avocats (contrôlé sept. 2020).
[532] Selon CE 16 déc. 2019 n° 421582, saisi par la voie du REP, il « résulte nécessairement *(de l'article L. 1121-1-2°)* que le ministre est également compétent pour énumérer celles des recherches qui ne relèvent pas du 2° de cet article mais entrent dans le champ du 3° du même article ».
[533] Entre autres. Voir Ordonnance n°2020-460 du 20 avril 2020, article 17-II.
[534] Modifié par ordonnance n°2020-737 du 17 juin 2020, l'article 17 II engage les CPP à s'assurer que la recherche n'est pas interventionnelle. V. arrêté 3 juil. 2020 fixant le format du questionnaire d'auto-évaluation mentionné au II de l'article 17 de l'ordonnance 22 avril 2020 préc.

Panorama rectifié du droit de la RIPH

Régime	Interventionnelle		Non interventionnelle (observationnelle)	
RBM 1988-2012	• Bénéfice direct pour la personne • Bénéfice indirect pour la personne • Avis consultatif des CCPPRB		(sans objet)	
RIPH 2012-2018	Catégorie I	Catégorie II	Catégorie III	
RIPH dep. 2018	Interventionnelle	Interventionnelle à risque minime (arrêté 2018)	**Interventionnelle dénuée de risque** (arrêté 2018 et jurisprudence 2019)	Non interventionnelle
Saisine des CPP depuis 2012	Approbation obligatoire (régime propre pour les médicaments) depuis 2020)	Approbation obligatoire	Approbation obligatoire	Approbation obligatoire

Quid juris ? quel est le critère d'application : la catégorisation selon le type de recherche, selon le niveau de risque ?

L'Ordonnance de 2016, le décret de 2017, les arrêtés de 2018, la jurisprudence de 2019, les Ordonnances de 2020, sans compter en 2022 d'autres compléments [535] révèlent progressivement la faiblesse systémique de la loi de 2012 dans sa prétention à créer un droit de la recherche « impliquant la personne humaine », **à l'égard duquel des situations seront en outre autonomes quant au régime de recueil des données**, ce qui nous intéresse ici.

B. LE DROIT DE LA RECHERCHE « N'IMPLIQUANT PAS » LA PERSONNE HUMAINE

Le champ d'application de la loi est **défini par un critère matériel** : « *les recherches organisées et pratiquées sur l'être humain **en vue du développement des connaissances biologiques ou médicales** sont autorisées dans les conditions prévues au présent livre et sont désignées ci-après par les termes (RIPH)* », L. 1121-1 CSP. On peut s'étonner de ce que le

[535] Les exceptions se sont encore multipliées et les textes alourdis en 2022, notamment pour les dispositifs médicaux : Ord. n° 2022-582 du 20 avril 2022 (art 2) et ord. n° 2022-1086 du 29 juill. 2022 (art 3).

champ d'application de la loi « Jardé » de 2012, soit explicité dans la partie réglementaire, par le critère qui était l'exact fondement de la loi « Huriet-Sérusclat » de 1988.

Ce qui nous intéresse ici est qu'il a fallu conceptualiser des recherches « n'impliquant pas », pour les faire échapper au treillage précité (1) ; et que la CNIL **a ajouté en ce sens le critère de la simple « participation »**, pour changer encore de régime du traitement des données (2).

1. L'autonomie de la recherche « n'impliquant pas » selon le décret de 2017

Du fait des difficultés conceptuelles et méthodologiques rencontrées, le pouvoir réglementaire est intervenu pour d'une part, changer de façon audacieuse (aux limites des prérogatives réglementaires) la définition du champ d'application de la loi (a) ; d'autre part, restreindre ce champ d'application sans, au demeurant, que la loi le prévoie (b).

a. Changement de la définition du champ d'application du droit de la RIPH

Dans la partie réglementaire, l'article R. 1121-1 tel que modifié en 2016, **explicitait la signification des recherches « impliquant la personne humaine »,** selon qu'elles portaient sur un médicament (al. 1), ou un dispositif médical (al. 2), pour *in fine* disposer que « *Les autres catégories de recherches mentionnées au 1° de l'article L. 1121-1 font l'objet, en tant que de besoin, d'une définition prise par décision du directeur général de l'Agence nationale de sécurité du médicament et des produits de santé* » (al. 3) [536].

Par cet article, la recherche interventionnelle au sens du 1° était bien couverte, mais pas celle relevant du 2° (qui s'est subdivisée avec le décret de 2018 confirmé par la jurisprudence de 2019 préc.), ni celle dite non interventionnelle relevant du 3°. Les 2° et 3° relevaient donc d'une décision du directeur de l'Agence, ce qui est **à la fois pragmatique et insécurisant**, compte tenu de la porosité précitée des catégories résultant de la loi de 2012 (on rappellera que la loi avait déjà prévu l'arbitrage de l'Agence, en cas de difficulté).

En 2017, un décret modifie profondément l'article R. 1121-1 CSP, pour définir **concrètement et de façon unifiée** ce qui relève des recherches impliquant la personne humaine [537] : relèvent

[536] Décret n° 2016-1537 du 16 novembre 2016 relatif aux recherches impliquant la personne humaine.
[537] Décret n° 2017-884 du 9 mai 2017 modifiant certaines dispositions réglementaires relatives aux recherches impliquant la personne humaine.

de ce droit les recherches « *organisées et pratiquées sur des personnes volontaires saines ou malades, en vue du développement des connaissances biologiques ou médicales qui visent à évaluer : 1° Les mécanismes de fonctionnement de l'organisme humain, normal ou pathologique ; 2° L'efficacité et la sécurité de la réalisation d'actes ou de l'utilisation ou de l'administration de produits dans un but de diagnostic, de traitement ou de prévention d'états pathologiques* ». Il n'y a **plus ici de distinction par technologies** (qu'avait promue le décret de 2016), mais une **heureuse approche unifiée par le but scientifique de la recherche**.

Le décret de 2017 ne va pas jusqu'à retrouver les termes de la loi de 1988, laquelle distinguait selon que la recherche présentât pour la personne y concourant, un « bénéfice direct » (cas du patient) ou non (sujet sain), caractérisant ainsi un enjeu éthique différencié. Surtout, le décret va sur la base de cette clarification du but scientifique, **écarter du champ d'application de la loi nombre de recherches** au motif qu'elles « n'impliquent pas ».

b. Restriction réglementaire du champ d'application de la RIPH

Sans que la loi ne lui offre de fondement explicite (mais n'est-il pas constitutionnellement de la compétence du législateur qui a institué une protection légale des personnes, **le soin d'en déterminer lui-même les cas d'exclusion ?**), le décret de 2017 introduit une distinction interne majeure. Il s'agit d'une nouvelle illustration du pragmatisme rendu nécessaire par la loi de 2012, et son critère trop lâche de l'« *implication* ».

Le même article R. 1121-1 CSP dispose ainsi, dans un II, que : « ***Ne sont pas des recherches impliquant la personne humaine au sens du présent titre*** *les recherches qui, bien qu'organisées et pratiquées sur des personnes saines ou malades* (sic)*, n'ont pas pour finalités celles mentionnées au I, et qui visent R. 1121-1-II-1° a) à évaluer les prétentions des produits cosmétiques* (au sens de L. 5131-1 CSP) *; b) à effectuer des enquêtes de satisfaction du consommateur pour des produits cosmétiques ou alimentaires* » [538] , ces activités ne relevant pas du champ de la recherche biomédicale (RBM), qui était l'objet exclusif de la loi Huriet.

Le même article R. 1121-1-II CSP écarte les recherches qui visent c) à effectuer « *toute autre enquête de satisfaction auprès des patients* » ; d) « *à réaliser des expérimentations en*

[538] Il est étonnant que les produits alimentaires soient ici impliqués ; on rappellera que les « compléments alimentaires » ne sont pas définis dans le Code de la santé publique, mais par un décret distinct. Ils n'en sont pas moins un enjeu de santé publique.

sciences humaines et sociales dans le domaine de la santé ». Cela est frappant, dans la mesure où l'inclusion des recherches **non interventionnelles** dans le champ de la RIPH avait été fondée sur l'invocation d'un risque de perturbation psychologique.

De même, il écarte du champ de la RIPH, mais par alinéas cette fois séparés et donc avec emphase, les recherches « *qui visent à évaluer des modalités d'exercice des professionnels de santé ou des pratiques d'enseignement dans le domaine de la santé* » (2°). Une dernière exclusion retient l'attention : « *3° Ne sont pas des recherches impliquant la personne humaine au sens du présent titre les recherches ayant une finalité d'intérêt public de recherche, d'étude ou d'évaluation dans le domaine de la santé* ***conduites exclusivement à partir de l'exploitation de traitement de données à caractère personnel*** *mentionnées au I de l'article 54 de la (LIL de 1978 modifiée)* ***et qui relèvent de la compétence du comité d'expertise pour les recherches, les études et les évaluations*** *prévu au 2° du II du même article* ».

On voit ici apparaître la question de l'utilisation secondaire (infra) ; l'article R. 1121-1-II-3° spécifie que cette utilisation peut concerner des données à caractère personnel ; mais même quand ces données ne possèdent pas de caractère personnel, nous verrons **qu'un dispositif de filtrage actif** est mis en place par le comité ad hoc sous l'égide de la CNIL, lequel en 2021 a changé de nom : les termes « de la compétence du comité d'expertise pour les recherches (etc.) » ont été remplacés par « *de la compétence du comité éthique et scientifique pour les recherches (etc.)* » par le décret de 2021 relatif au SNDS [539].

2. L'autonomie de la simple « participation » selon la doctrine de la CNIL

Le critère de la « participation » de la personne **n'est pas d'origine réglementaire, mais doctrinale :** il s'agit du terme choisi par la CNIL pour désigner l'hypothèse de traitements réglementairement exclus du champ de la RIPH (sur cette exclusion réglementaire en 2017 et la variété des hypothèses dans l'article R. 1121-1-II, *supra*). Ce terme s'imposait.

[539] Décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

En effet, la CNIL élabore des « méthodologies de référence » relatives au consentement des personnes notamment, **lesquelles MR sont différenciées selon le type de recherches auxquelles elles s'appliquent**, nous l'avons vu. La conséquence de la distinction précitée est l'applicabilité de la MR004. Or, selon la CNIL, celle-ci recouvre deux types de recherches :

* D'une part, les recherches « *sur des **données déjà collectées**, lors du soin ou de recherches antérieures (**réutilisation de données**) ou des données collectées dans le cadre de la prise en charge médicale, au fil de l'eau* ». C'est ce qui relève de l'utilisation secondaire des données de santé, que nous traiterons *infra*, selon les modalités de cet utilisation secondaire (données personnelles, données anonymisées, données pseudonymisées).
* D'autre part, les recherches « *dans lesquelles la personne participe (sic) et pour lesquelles des **données spécifiques liées à la recherche sont collectées sans répondre à la définition juridique de (RIPH) et notamment à la finalité précisée** dans le code de la santé publique (articles L. 1121-1 et R. 1121-1 CSP)* » [540].

Cette doctrine est intéressante sur un double terrain : son contenu est clair, sa rédaction moins : ses circonvolutions ont appelées par une loi mal conçue, dont il aura fallu du préciser le but et le champ **du fait de l'incongruité des catégorisations de 2012**.

On notera qu'en 2016, la loi a institué une procédure d'avis du Comité d'Expertise pour les Recherches, les Etudes et les Evaluations dans le domaine de la Santé (CEREES) pour les études **«** n'impliquant pas » la personne humaine [541]. Cet avis est demandé par la CNIL avant l'autorisation de telles études. Sur la base d'un tel avis, son refus en 2022 d'autoriser l'étude visant à un « Palmarès des hôpitaux » (appréciation de performance des organisations), a conduit à invoquer « l'intérêt public » dans des conditions contestées [542].

[540] CNIL, « Recherches dans le domaine de la santé », préc.
[541] Article 193, loi du 26 janvier 2016 de modernisation de notre système de santé.
[542] Conseil d'État 30 juin 2023, n° 469964, suite à la décision de la CNIL rendue dans l'affaire « Palmarès des hôpitaux » : la CNIL précise les raisons de son refus d'autoriser le Point à accéder à la base de données des hôpitaux, 10 nov. 2022 (site CNIL). Saisi par la CNIL qui a suivi son avis, le Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé avait considéré que « *la construction des indicateurs retenus dans le palmarès peut conduire à diffuser une information erronée sur les performances relatives réelles des établissements de santé pouvant induire en erreur les patients et être par conséquent contraire à l'intérêt public* ». Pour une critique avertie, J. de Kervasdoué, « Palmarès des hôpitaux : la réponse d'un expert aux critiques de la CNIL », in Le Point 18 nov. 2022.

§2. CATEGORISATION JURIDIQUE DES DONNEES ISSUES DE LA RECHERCHE MEDICALE ?

Après avoir vu la catégorisation des études participant de la recherche biomédicale, et leurs conséquences sur le régime de celle-ci quand au cadre juridique du recueil des données, nous examinons maintenant la catégorisation juridique des données qui en sont issues.

Là encore, nous constatons **qu'il n'existe pas de régime unifié de catégorisation**. S'il est possible, de façon parfois laborieuse, de distinguer les catégories selon le mode de recueil des données en droit commun (A), le recueil des données dans l'hypothèse notamment des autorisations d'accès précoces aux médicaments, relève d'un régime autonome (B).

B. DISTINCTION SELON LE MODE DE RECUEIL DES DONNEES EN DROIT COMMUN

Après l'examen du droit applicable à l'hypothèse de « l'implication » du patient, notion qu'il va falloir clarifier du fait de l'ambiguïté législative (1), nous esquissons quelques considérations sur la portée du droit français applicable (2), car seul ce droit le prévoit.

1. Droit applicable à l'hypothèse de l'« implication » du patient

Relevons d'abord que la porosité des catégories de recherche impacte l'application des méthodologies de référence (MR) de la CNIL (a), avant de voir comment l'ambiguïté a imposé de distinguer la « *participation* » et de l'« *implication* » du patient (b).

a. La porosité des catégories impacte l'application des méthodes.

Elaborées par la CNIL, **les MR déterminent la conformité du traitement informatique des données** selon les catégories de recherches en santé [543]. Parmi les objectifs des MR, outre l'accompagnement des professionnels et l'aide à al réalisation de l'analyse d'impact, figure celui de leur permettre de **mettre en œuvre les traitements de données impliquées par leurs actes thérapeutiques sans autorisation préalable, sous réserve d'une déclaration de conformité au regard des** règles et principes prévus par ces référentiels.

[543] CNIL, « Recherches dans le domaine de la santé : ce qui change avec les nouvelles méthodologies de référence », 16 juillet 2018, cnil.fr (contrôlé sept. 2020).

En 2016, la CNIL a refondu ces MR : leur application est en principe déterminée par la distinction entre recherches « interventionnelles » et « non interventionnelles ». Les premières relèvent de la MR001 (pour rappel, il s'agit des interventions sur la personne non justifiées par sa prise en charge habituelle, ou ne comportant que des risques et contraintes minimes, L. 1121-1-1° et 2°). Les secondes relèvent de la MR003.

Mais depuis l'arrêté de 2018 et les Ordonnances de 2020, on peut se demander à quelle MR se rattachent les **recherches interventionnelles dénuées de risque** [544], car le site de la CNIL ne le précise pas : à la MR001, en raison de leur caractère interventionnel ? à la MR003, par attraction réglementaire dans le champ de L. 1121-1-3° (*supra*) ? Les contours des études « non interventionnelles », ou relevant de ce régime, apparaissent difficiles à tracer.

Types de recherche		**Catégorie CSP**	**Approbation CPP**	**Méthode CNIL**
« impliquant » (loi 2012)	**interventionnelle « non justifiée par [la] prise en charge habituelle »**	catégorie I (L. 1121-1-1°)	obligatoire (nouveau régime depuis 2020 pour les médicaments)	MR 001
	interventionnelle à « risques et contraintes minimes »	catégorie II (L. 1121-1-2°)	obligatoire	MR 001
	non interventionnelle	catégorie III (L. 1121-1-3°)	obligatoire depuis 2012	MR 003
	doute quant à la qualification	arbitrage ANSM (L. 1121-4)	selon l'arbitrage	selon l'arbitrage
« n'impliquant pas » (décret 2017)	**« bien qu'organisées et pratiquées sur des personnes saines ou malades »**	R. 1121-1-II (1°, 2° et 3°)	sans objet	MR 004

Si la CNIL met ici en exergue la finalité de la recherche, c'est pour distinguer selon que la personne est « **impliquée** » (MR001 et MR003), ou seulement « **participe** » (MR004).

[544] Notamment, *selon les technologies,* dans les hypothèses de recherches fondées sur des senseurs/capteurs connectés non invasifs anodins (*fit bit* etc) et/ou les applications logicielles, embarquées ou à distance etc. Cela ne se limite pas aux technologies citées dans l'arrêté de 2018.

b. La notion de « participation » est distinguée de la notion d'« implication ».

Nous avons précédemment relevé que la MR004 recouvrait selon la CNIL deux types de recherches, écartées du champ légal de la RIPH par le décret de 2017 précité. Il s'agit pour rappel d'une part, des recherches « *sur des données déjà collectées, lors du soin ou de recherches antérieures (**réutilisation de données**) ou des données collectées dans le cadre de la prise en charge médicale, au fil de l'eau* » ; d'autre part, des recherches « *dans lesquelles la personne participe (sic) et pour lesquelles des **données spécifiques liées à la recherche sont collectées sans répondre à la définition juridique de (RIPH) et notamment à la finalité précisée** dans le code de la santé publique (articles L. 1121-1 et R. 1121-1 CSP)* » [545].

Cette dernière nous retient seule ici, sachant que les dispositifs connectés et/ou applications ne sont tributaires de ce droit **que s'ils proposent des services à distance** (à la différence d'un usage exclusif par l'utilisateur), ou s'ils **comportent une connexion pour la sauvegarde externe continue de données** (à la différence d'un stockage local non partagé) etc. [546].

Or, le défi naît ici de l'absence de prétention explicite en santé de certains objets connectés et/ou applications. Nous avons relevé que des fabricants de technologies évitaient soigneusement leur qualification « médicale » (L. 5211-1) [547], pour écarter les contraintes de certification dans ce domaine mais aussi et plus probablement surtout, **éluder la qualification « de santé » des données qui, par inférence, en découlerait** [548].

Il en résulte que dans ce cas, les « recherches » entreprises par ces opérateurs **ne relèvent ni de la catégorie des recherches « impliquant », ni de la catégorie des recherches « n'impliquant pas »**, et rejoignent malgré leur sensibilité en santé le droit commun de la protection des données personnelles, soustrait à l'application de la MR004.

---

[545] CNIL, « Recherches dans le domaine de la santé », préc.

[546] CNIL, « Les applications mobiles en santé sont-elles soumises à la réglementation sur la protection des données personnelles ? » août 2018, cnil.fr (contrôlé sept. 2020). Sur les applications mêmes, HAS, « Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (*Mobile Health ou mHealth*) », oct. 2016 .

[547] *Comp*. contenu de l'arrêté d'avril 2018.

[548] E. Pinilla, F. Megerlin, « Des données de santé par qualification de la loi etc. » RGDM janv. 2018 préc.

2. Considérations sur la portée du droit français applicable

a. La compétence territoriale

L'applicabilité du texte est territoriale, indifféremment quant à la nationalité et au statut des personnes « impliquées ». **A titre optionnel, la procédure peut cependant** s'appliquer à des RIPH conduites hors de l'Union européenne, selon l'intention d'un promoteur ayant son siège en France (L. 1123-7-1) : le but est alors aussi de faire connaître le principe de sa recherche et d'en faire valider les conditions, permettant le rapatriement des résultats pour une valorisation nationale / européenne. Mais si le but n'est pas le rapatriement formel des résultats pour une valorisation **explicite** en Europe ?

En outre, **le droit européen et la loi française prévoient la publicité des RIPH.** Restons en ici à la loi française : elle prévoit que « *les recherches impliquant la personne humaine et leurs résultats, à l'exception de ceux relevant du secret de la défense nationale, sont inscrits dans un répertoire d'accès public selon des règles déterminées par décret* » (L. 1121-15).

Les RIPH **sont alors distinguées selon un critère transverse, selon que leur finalité est commerciale ou non** (L. 1121-16-1-II). Dans le cas où la recherche n'a pas de finalité commerciale, est financièrement soutenue par les assureurs obligatoires en santé, et ne relève pas de la défense nationale, « *le promoteur de la recherche s'engage à rendre publics les résultats de sa recherche* » (L. 1121-16-1).
Mais ce dernier peut aussi, en cours de route, la requalifier en recherche « commerciale », et se libérer de l'obligation d'en publier les résultats, contre reversement financier [549]. La confidentialité des recherches et la protection spécifique des données (*data protection,* etc.) puis des éventuelles applications ultérieures (*sous brevet etc.*) relèvent alors de mécanismes divers, qu'il n'est pas lieu de détailler ici.

Quoiqu'il en soit, ces textes sont conçus pour des promoteurs de RIPH **opérant selon la légalité française**, avec une intention de valoriser leurs résultats en Europe, auprès notamment des instances publiques [550].

---

[549] L. 1121-16-1- III, 2°, 3ème alinéa.
[550] Par publication scientifiques ou didactiques multi-supports, argumentation devant les instances d'autorisation des produits de santé (EMA, ANSM), en charge de leur évaluation (CT, CNEDIMTS, CEESP), de la négociation des prix remboursables (CEPS) etc. ; à l'appui aussi de promotions sélectives, de recherches de capitaux ou partenariats, etc. mais également d'études de marché etc… selon l'art des présentations devant les CPP.

b. la compétence matérielle

Nous avons vu que la notion légale d'« implication » était suffisamment vague pour que le pouvoir réglementaire ait du la cerner en 2017, et pour que la CNIL invoque, outre la définition légale des RIPH, l'argument surabondant de leur « finalité », pourtant explicitée dans les textes. Nous avons aussi vu que l'article R. 1121-1-II détaillait les recherches à la frontière de cette qualification, pour les en écarter expressément (*supra*).

Mais des recherches observationnelles **se développent parfois dans l'ombre-portée et hors portée des textes, par des acteurs d'assise extraterritoriale**, recourant à des outils dématérialisés aux applications mixtes. Ils peuvent laisser les personnes « impliquées » dans l'ignorance qu'elles sont scrutées, et se soucient peu des CPP.

Nous avons vu ce fait en filigrane dans l'avis, non suivi en la forme dans le RGPD, du groupe de travail de l'article 29 rendu en 2015. Cet avis proposait que fussent qualifiéee « de santé » dès lors que « *a) Les données traitées par l'application ou le dispositif sont intrinsèquement / clairement des données médicales. En d'autres termes, les données fournissent des informations sur l'état de santé physique ou mentale d'un individu généré dans un contexte professionnel de la santé (par exemple, les fournisseurs de soins de santé) ; b) les données brutes du capteur traitées par l'application ou dispositif peuvent être utilisés indépendamment ou en combinaison avec d'autres données, pour tirer des conclusions sur l'état de santé ou des risques réels pour la santé d'un individu ;* ***c) les données permettant de tirer des conclusions à propos de l'état de santé d'un individu (indépendamment du fait que ces conclusions sont exactes ou inexactes, légitimes ou illégitimes, suffisantes ou insuffisantes)*** » [551].

Si donc la recherche fondée sur des données de santé ne relève pas de ce II, sans viser l'évaluation des « mécanismes de fonctionnement de l'organisme humain normal ou pathologique » (I-1°), ni viser les buts du I-2°, quel droit applicable ? Le développement des technologies et services marchands dans ce champ est exponentiel – une aubaine, pour les fournisseurs et utilisateurs, à toutes fins, des mégadonnées de santé « par destination ».

Les conséquences en santé **en termes de puissance descriptive, prédictive voire inductive de comportements / vulnérabilités** (à l'échelle des individus et populations), par des outils dits d'« intelligence artificielle », sont considérables.

[551] Annexe à la lettre du 5 février 2015 du groupe de l'article 29, préc.

B. AUTONOMIE DU « RECUEIL DE DONNEES » DANS LE CAS DES AUTORISATIONS D'ACCES PRECOCE

Il s'agit là d'un autre exemple de données d'intérêt stratégique. Le droit français permet l'utilisation exceptionnelle de médicaments sans / hors autorisation de mise sur le marché (AMM), lorsque l'état des connaissances constitué lors d'essais en cours ou de façon empirique nourrit un espoir suffisant dans une situation clinique critique. Depuis 2021, les entreprises qui demandent cet accès anticipé pour leurs produits innovants **doivent systématiquement recueillir ces données issues de soins** (patients traités hors des essais) **pour compléter les données qu'elles produisent** (patients inclus dans les essais), afin d'une évaluation élargie pour le remboursement et le prix.

Nous relevons ici les frontières conceptuelles donc opérationnelles, entre le droit de l'accès précoce et le droit de la recherche « impliquant » les personnes, **en ce qu'il intéresse le recueil et traitement des données** résultant de la mise en œuvre des Protocoles d'utilisation temporaire – recueil de données (PUT-RD) imposés par la loi. Les développements suivant reprennent notre publication de 2022, et l'actualisent [552]. Nous verrons la notion et son autonomie à l'égard de la RIPH (1), puis la vocation des données ainsi recueillies (2).

1. Notion d'accès précoce subordonnés au protocoles incluant le recueil de données

Le législateur a refondu le système des Autorisations Temporaires d'Utilisation (ATU) nominative (ATUn) et de cohorte (ATUc) et des Recommandations Temporaires d'Utilisation (RTU), et les modèles de prise en charge temporaire (PEC-T) qui était juridiquement explicite, mais qui s'était complexifié [553]. Depuis lors, une nouvelle terminologie et de nouveaux régimes y ont été substitués, non sans discussion quant aux chevauchements conceptuels.

a. Refonte en 2021 du cadre de l'accès anticipé des patients

Le législateur a réarticulé les rôles de l'Agence Nationale de Sécurité du Médicament et de la Haute Autorité de Santé, mis en exergue la notion d'« accès », et convoqué des catégories

[552] Megerlin F, Pinilla E, Huriet Cl, Recueil de données sur les médicaments en accès précoce : quel lien avec la recherche « impliquant » les personnes humaines ? Rev Gen Dr Méd 2022 (1), 375-388.
[553] Loi n° 2020-1576 du 14 déc. 2020 de financement de la sécurité sociale (article 78).

morales [554] : il a ainsi institué des procédures d'accès « précoce » et « compassionnel », ces dernières recouvrant l'autorisation d'accès compassionnel comme les cadres de prescription compassionnelle. Désormais, la HAS décide de l'accès précoce **(tableau)**.

Pour cela, la prescription médicale doit répondre à des conditions cumulatives : « traiter des maladies graves, rares ou invalidantes », dans des « indications thérapeutiques précises », si « 1° Il n'existe pas de traitement approprié ; 2° La mise en œuvre du traitement ne peut pas être différée ; 3° L'efficacité et la sécurité de ces médicaments sont fortement présumées au vu des résultats d'essais thérapeutiques ; 4° Ces médicaments sont présumés innovants, notamment au regard d'un éventuel comparateur cliniquement pertinent » (L. 5121-12-I CSP).

Régimes successifs des utilisations de médicaments sans ou hors AMM

Régime	Avant juin 2021	Depuis juin 2021	Initiative	Décideur
Pré AMM	ATU nominative	Accès compassionnel	ANSM entre autres	ANSM
	ATU de cohorte	Accès précoce	Laboratoire	HAS
Post AMM	PEC-T	Accès précoce	Laboratoire	HAS
	RTU	Accès compassionnel	ANSM entre autres	ANSM

La procédure a été concrétisée en juin 2021 par décret [555], et détaillée par des doctrines de la HAS [556]. Son guide d'accompagnement éclaire notamment l'élaboration des protocoles d'utilisation temporaire (PUT) et de recueil de données (RD), qui centralisent les informations disponibles sur le médicament, les conditions de son utilisation, et organisent le recueil des données (R. 5121-70 CSP). Par définition, ces protocoles visent des patients non inclus dans les essais, que ces derniers soient en cours (demandes pré-AMM) ou finalisés (post-AMM).

Le système appelé désormais « autorisation d'accès précoces / compassionnel », **jouit d'une autonomie bien établie**. D'une part, le Code de la santé publique prévoit un régime dédié (Ve Partie du CSP), distinct du droit de la recherche impliquant les personnes humaines (Ière Partie du CSP), sans renvois légal ni réglementaire de l'un à l'autre. Le but est en effet l'usage du médicament à titre exceptionnel dans un but de soin, en cas d'espoir suffisant face

[554] Dans le sillage de la notion de « *compassionate use* » introduite par l'article 83 du Règlement (CE) n° 726/2004 sans pour autant établir un cadre juridique européen, car la compétence en la matière est nationale.
[555] Décret n° 2021-869 du 30 juin 2021 relatif aux autorisations d'accès précoce et compassionnel.
[556] HAS (guide) « Autorisation d'accès précoce aux médicaments : doctrine d'évaluation de la HAS », adopté le 17 juin 2021 ; HAS (guide), « Accès précoce des médicaments : accompagnement des laboratoires », adopté le 8 juillet 2021 ; Site HAS (vérifié nov. 2021).

à une situation clinique critique ; mais les circonstances et les effets doivent être parfaitement documentés : tel est le but des PUT-RD.

Le recueil de données désormais obligatoirement lié au PUT doit être mené *en parallèle* d'une recherche qui implique la personne humaine (RIPH), ce qui conduit à une méthodologie CNIL différente du fait de la qualification hors droit RIPH, de ces données. Pour autant le recueil ne semble pas présenter la même impérativité : l'autorisation d'accès précoce est « subordonnée » [557] ; tandis que dans que l'autorisation est seulement « assortie » dans le cas de l'accès compassionnel [558], lequel pourtant à titre d'exception recouvre l'accès pré-précoce (CSP, L. 5121-12-1, II, 2ème alinéa, par dérogation).

b. Recueil des données de santé : quelle méthodologie CNIL ?

En 2014, la CNIL avait pour le système des ATU/RTU **institué un régime d'autorisation unique** (AU-041) [559] ; ce régime n'a pas été affecté par l'adoption en 2015 puis 2016 des « méthodologies de référence » propres à la RIPH (*supra*) : si des aspects convergent, leur objet est autre. L'autonomie est confirmée, à titre superfétatoire, par un troisième élément. L'avènement du Règlement général de protection des données en Europe **a en 2018 abrogé les systèmes nationaux d'autorisation,** dont l'autorisation unique précitée [560]. Quel impact ?

Selon la CNIL, « *dans l'attente de l'adoption d'un référentiel* (sous-entendu d'un référentiel dédié)*, les fichiers relatifs au patient, nécessaires à l'initiation, au suivi et à l'arrêt de prescription particulière de médicaments concernés par une ATU ou une RTU n'ont plus à être déclarés à la CNIL* ». En outre, elle « *considère, **à titre dérogatoire et strictement temporaire*** (mots soulignés par elle) *qu'il n'est pas nécessaire de déposer une demande d'autorisation* (…) *si le traitement de données considéré est conforme à toutes les exigences*

[557] L. 5121-12- « *IV. - L'autorisation d'accès précoce **est subordonnée au respect**, par l'entreprise qui assure l'exploitation du médicament, d'un protocole d'utilisation thérapeutique et de recueil des données* ».
[558] L. 5121-12-1- « *V. - Les autorisations et les cadres de prescription au titre de l'accès compassionnel **sont assortis d'un protocole** d'utilisation thérapeutique et de suivi des patients qui précise les conditions de recueil des informations (...)* ».
[559] Délibération n° 2014-501 du 11 décembre 2014 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel par les entreprises ou organismes exploitant ou important des médicaments dans le cadre des autorisations temporaires d'utilisation (ATU) et recommandations temporaires d'utilisation (RTU).
[560] Abrogation à effet du 25 mai 2018, cf. Règlement (UE) n° 2016/679 du Parlement et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, etc. et abrogeant la directive 95/46/CE.

prévues par l'AU-041 » [561]. Depuis 2021, les termes ATU et RTU sont simplement à remplacer par AAP et AAC/CPC.

La CNIL souligne que, en dépit de l'abrogation du système des autorisations uniques, et « dans l'attente de la production de référentiels RGPD, [elle] a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité » [562]. De son côté, la HAS rappelle que l'entreprise doit accomplir les formalités nécessaires auprès de la CNIL [563], et a pris l'heureuse initiative d'une notice d'information du patient sur le traitement de ses données personnelles [564].

En conséquence, la partie « recueil des données » à visée observationnelle dans les PUT-RD ne relève d'aucune des méthodologies de référence existantes de la CNIL ; à titre transitoire, ce recueil ne requiert pas de demande d'AU, laquelle reste toutefois possible sachant que ses critères doivent être virtuellement satisfaits. Le tout valait dans l'attente d'un référentiel spécifique aux procédures d'accès précoce, **lequel a été adopté en novembre 2022** [565].

Notons la finalité exclusive du système abrogé en 2022 de l'autorisation unique AU-041, dont la philosophie demeure, à défaut de l'outil : il s'agit de « *la collecte, l'enregistrement, l'analyse, le suivi, la documentation, la transmission et la conservation des données relatives à l'accès, à l'initiation, au suivi et à l'arrêt de prescription de spécialités pharmaceutiques dans le cadre défini par les articles L. 5121-12 et L. 5121-12-1 du Code de la Santé Publique* » et par ailleurs de *« la gestion des contacts avec les médecins prescripteurs et les pharmaciens dispensateurs d'un médicament sous ATU ou RTU* ». **Toutes autres finalités sont exclues** [566].

---

[561] CNIL, « Autorisation temporaires d'utilisation (ATU) et recommandations temporaires d'utilisation (RTU) : faut-il faire des formalités auprès de la CNIL ? », site CNIL (vérifié oct. 2021).
[562] CNIL, Déclaration n°41 « Autorisations temporaires d'utilisation et recommandations temporaires d'utilisation », synthèse, site CNIL (vérifié oct. 2021).
[563] HAS, (Guide) Accès précoce des médicaments : accompagnement des laboratoires préc.
[564] HAS, (information) Accès précoce à un médicament – Traitement des données personnelles, juillet 2021, site HAS (vérifié oct. 2021).
[565] Référentiel relatif aux traitements de données à caractère personnel mis en œuvre par le laboratoire titulaire des droits d'exploitation d'un médicament bénéficiant d'une autorisation d'accès précoce, 16 nov. 2022 ; référentiel relatif aux traitements de données a caractère personnel mis en œuvre par le laboratoire titulaire des droits d'exploitation d'un médicament bénéficiant d'une autorisation d'accès compassionnel, 16 nov. 2022.
[566] CNIL, Déclaration n° 41 préc.

2. La vocation des données de santé recueillies dans le cadre des PUT-RD

Il n'est pas lieu d'analyser ici le décret de 2021 qui concrétise le cadre des accès précoce, ni les procédures de décision selon les cas visés. Rappelons seulement que le PUT-RD ne vise que les patients traités en parallèle d'essais, ou hors d'indications validées. Les essais peuvent donc être en cours ou finalisés (R. 5121-68-II-1°, b). Leur avancement doit en tous cas laisser « fortement présumer » la sécurité et l'efficacité du médicament (idem II-2°, c) dans des indications précises et pressantes (L. 5121-12-I préc.).

a. le but du recueil obligatoire de données dans le cadre du protocole

En juin 2021, la HAS a publié sa doctrine d'évaluation spécifique en la matière [567]. Elle y souligne notamment que le PUT-RD « permet de recueillir des données observationnelles/en vie réelle chez les patients bénéficiant d'un médicament en autorisation d'accès précoce », sachant que « *les patients éligibles à un essai clinique en cours dans l'indication considérée doivent prioritairement être inclus dans celui-ci* » ; que **les données de PUT-RD n'ont pas vocation à remplacer les essais cliniques, ni ne modifient les attentes de la Commission de la transparence** en vue de l'inscription éventuelle sur la liste des médicaments remboursable ; « *ces données sont complémentaires et contribuent donc à l'évaluation du médicament par la HAS pour le renouvellement de l'autorisation d'accès précoce et, à terme, pour l'évaluation en vue du remboursement* ».

En outre, elle **encourage le stockage des données dans le système national des données de santé** (SNDS) ; à tout le moins, préconise une harmonisation des codage pour permettre le chaînage des données PUT-RD/SNDS [568], « notamment **en vue de leur réutilisation pour une éventuelle étude post-inscription** » [569].

Le guide poursuit, en saluant le fait que « pour un nouveau médicament ou une nouvelle indication, les accès précoces *représentent la* ***première opportunité de collecte de données observationnelles/en vie réelle en France*** ». La HAS y souligne notamment que « la collecte devra pouvoir *s'intégrer dans la pratique clinique courante* sans nécessiter de visites ou d'examens supplémentaires ou complémentaires ». Cette doctrine s'inscrit dans une dynamique mondiale de l'évaluation en vie réelle : l'opportunité de progrès en France a été

[567] HAS (Guide) « Autorisation d'accès précoce aux médicaments : doctrine d'évaluation », préc. Cette doctrine est spécifique car, bien distincte de HAS (Guide), « Études en vie réelle pour l'évaluation des médicaments et dispositifs médicaux » validée le 10/06/2021, site HAS (vérifié oct. 2021).
[568] Ibid, page 13.
[569] HAS (Guide) « Accompagnement des laboratoires » préc., p 34.

soulignée en 2017 dans un rapport public [570] ; elle y a fait l'objet en 2021 d'une doctrine générale de la HAS, distinctement de la doctrine d'évaluation des accès précoce [571].

b. Absence de lien juridique entre les PUT-RD et la RIPH

Nous avons souligné **l'autonomie du droit des accès précoce et des obligations afférentes de recueil de données**. Si l'on voulait rapprocher les PUT-RD du cadre des RIPH, une nouvelle catégorie devrait être conceptualisée **(tableau 4)**. En miroir de la « recherche interventionnelle dénuée de risque » (arrêté de 2018 et jurisprudence de 2019), il s'agirait d'une « **recherche non-interventionnelle non dénuée de risque** ».

Fin 2022, la CNIL a adopté deux référentiels distincts, concernant les accès précoces et les accès compassionnels après les retours reçus dans le cadre des consultations publiques lancées en février de la même année, après une légère modification de périmètre pour la consultation. Ces référentiels sont autonomes à l'égard de ceux valant pour la RIPH [572].

Droit	**RIPH**				**Hors RIPH**
Type	**« impliquant »**			**« non impliquant »**	**autonomes**
Mode	**Interventionnel**		**observationnel**	**principalement observationnel**	**Observationnel**
CSP	L.1121-1-1°	L.1121-1-2° Arrêté 2018	L.1121-1-3° Arrêté 2018 Jurispr 2019	R.1121-1-II (1°, 2° et 3°)	L.5121-12-IV Décret 2021
Catég.	Catégorie I	Catégorie II	Catégorie III	-	PUT-RD
Risque	Oui	Oui	Non	Non	Oui
CPP	Obligatoire	Obligatoire		Non	Non
CNIL	MR001	MR001	MR003	MR004	(*ad hoc*, nov 2022)
Données	Données d'essais		Données « de vie réelle »		

[570] B. Bégaud, D. Polton, F. von Lennep, « Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé - L'exemple du médicament », juin 2017 ; C. Le Gal Fontes, G. Leguinel, « De l'importance des données en vie réelle en matière de fixation de prix des médicaments » *RGDM*, n° 24, 2017, p. 33-48. *Comp*. F. Megerlin (dir.), Contrat de performance et accès au marché de l'innovation thérapeutique, Paris : Elsevier ; 2014.

[571] HAS (Guide), « Études en vie réelle pour l'évaluation des médicaments et dispositifs médicaux » (validé le 10/06/2021), site HAS (vérifié oct. 2021).

[572] Référentiel relatif aux traitements de données à caractère personnel mis en œuvre par le laboratoire titulaire des droits d'exploitation d'un médicament bénéficiant d'une autorisation d'accès précoce, 16 nov. 2022 ; référentiel relatif aux traitements de données a caractère personnel mis en œuvre par le laboratoire titulaire des droits d'exploitation d'un médicament bénéficiant d'une autorisation d'accès compassionnel, 16 nov. 2022.

En pratique, les PUT mis en place en 2021 n'ont rien à envier dans leur rigueur scientifique et éthique (consentement informé etc.) au cadre de la RIPH. En revanche, **l'abondement du système national des données de santé par tout type d'étude observationnelle** laisse songeur, quant à la qualité des données, et donc quant à la valeur de leur exploitation.
L'acronyme anglo-saxon « *garbage in, garbage out* » est ici suffisamment explicite : la pertinence des systèmes d'intelligence augmentée dépendra du volume certes, mais aussi de la qualité des donnée de santé qui feront l'objet du traitement statistique.

La question ne se pose *a priori* pas pour les données d'accès précoce, vu la qualité de la réflexion structurée par la HAS quant aux PUT-RD – sous réserve de leur due mise en œuvre par les entreprises et au sein des établissements de santé [573]. Elle se posera pour les données recueillies hors du contexte PUT-RD, pour des données « en vie réelle ».

Mais deux point sont ici parfaitement explicites :

* les référentiels **ne couvrent pas la réalisation d'un contrôle de la qualité des données** par une personne ne relevant pas de l'équipe de soins (généralement ARC, attaché de recherche clinique).

* la CNIL signale en nov. 2022 que des modifications sont intervenues, au regard du projet soumis à consultation en février 2022, quant aux conditions dans lesquelles **une réutilisation des données collectées (utilisation secondaire) peut être envisagée**. Dès lors que la finalité d'un traitement ultérieur n'est pas celle de sa collecte, il est soumis à formalités distinctes [574].

***

[573] Le décret n° 2021-869 préc. soulève nombre de questions d'organisation pratique et conséquences juridiques.
[574] Site CNIL, « Santé : la CNIL adopte deux référentiels concernant les accès précoces et les accès compassionnels ».

SECTION II. DYNAMIQUE DE LA DONNEE PAR L'AVENEMENT DES UTILISATIONS SECONDAIRES

Nous venons de voir comment le droit français de la recherche biomédicale avait conduit à catégoriser les recherches et les méthodologies CNIL afférentes ; mais que **la distinction entre recherche « impliquant » et « non impliquant »** la personne **n'altérait pas le caractère « personnel » de la donnée de santé qui en découle**, seulement le régime de sa réutilisation.

Nous avons pu y distinguer **au sein de la catégorie « impliquant »**, les études **interventionnelles, qui visent à générer** des données inédites pour la recherche scientifique et clinique ; les études **observationnelles, qui visent à recueillir** des données générées par les activités de soins dans des conditions réelles de prescription (à distinguer des « essais cliniques pragmatiques » [575], non purement observationnels [576]) pour diverses finalités. Nous avons relevé l'autonomie des dispositions relatives aux accès précoces et compassionnels.

Nous voyons maintenant ici, toujours dans une dynamique de recherche élargie, l'effet sur la notion de « donnée de santé », du développement des « utilisations secondaires ».

Si des données d'essais cliniques protocolisés peuvent certes donner lieu à un ré-usage, « l'utilisation secondaire » s'entend essentiellement des données hors de tels essais ; il s'appuie sur la **conceptualisation de la donnée de « vie réelle »** et ses subdivisions (§1). A l'opposé, nous constaterons l'avènement de la **donnée de santé « synthétique »**, catégorie non juridique qui prétend pallier certaines difficultés rencontrées avec la précédente (§2).

---

[575] Les essais cliniques pragmatiques sont pratiqués dans le système de santé hors d'un contexte d'essais cliniques protocolisés. Ils visent l'étude de la corrélation entre les traitements et les résultats en pratique de soins, non sur la démonstration d'explications causales des résultats. Mais ils visent souvent aussi à une démonstration : cela dépend du périmètres de l'étude et des paramètres retenus. V. l'article souche, D. Schwartz et J. Lellouch, « *Explanatory and pragmatic attitudes in therapeutical trials* », *Journal of Chronic Diseases*, vol. 20, nº 8, août 1967, p. 637–648 ;

[576] En droit français, de tels « essais pragmatiques » relèvent des RIPH de catégorie III (non interventionnel). Sur la finalité dominante de ces essais, voir l'article de référence de C.D. Mullins, D. Whicher, E.S. Reese et S. Tunis, « *Generating Evidence for Comparative Effectiveness Research Using More Pragmatic Randomized Controlled Trials:* », *PharmacoEconomics*, vol. 28, nº 10, octobre 2010, p. 969–976 ;

§1. LA SUBDIVISION DE LA NOTION PAR LES UTILISATIONS SECONDAIRES

Les **notions d'utilisation « primaire » / « secondaire »** n'étant pas définies en droit français, c'est dans la proposition en mai 2022 de règlement relatif à l'espace européen des données de santé, qu'on les trouvera [577].

*** La notion « d'utilisation primaire »** est explicite et tient dans une unique définition [578], à la différence de l'utilisation secondaire qui nécessitera un renvoi. Cela, bien que sa proposition de définition européenne (article 2§2, d) ne recouvre pas les activités de R&D précitées notamment – mais l'article 33§3 rattrape ce point [579] et son §4 couvre les données d'une protection spécifique.

On retrouve ici les données de santé « par qualification de la loi », et « par destination », dès lorsqu'elles trouvent une **application et non seulement une signification médicale** (*supra*) : le critère de qualification est ici **l'usage, non la nature**. L'article 5 établit même des « *catégories prioritaires* » de données à fin d'utilisation primaire, qu'il n'est pas lieu de développer ici, mais que l'on retrouvera dans la seconde partie de notre thèse.

***** En contraste, l**a notion d'utilisation « secondaire » aboutit à une sous-catégorisation des données de santé**, par paramétrage de leur champ. Ainsi, la définition des buts légitimes en la matière (encore absente du droit français), est l'objet de l'article 34 de la proposition précitée. Cet article énonce les « *Finalités pour lesquelles* ***des données de santé électroniques peuvent être traitées à des fins d'utilisation secondaire*** **»** [580] (l'article 35 énonce quant à lui les

---

[577] *Proposition de Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final 2022/0140 (COD).*

[578] Il s'agit du « *traitement de données de santé électroniques à caractère personnel* ***pour la fourniture de services de santé*** *visant à évaluer, maintenir ou rétablir l'état de santé de la personne physique à laquelle ces données se rapportent, y compris la prescription, la dispensation et la fourniture de médicaments et de dispositifs médicaux,* ***ainsi que pour les services de sécurité sociale,*** *administratifs ou de remboursement pertinents* »;

[579] Ainsi, « *Les données de santé électroniques énumérées au paragraphe1 englobent les données traitées à des fins de fourniture de soins de santé ou de soins,* ***ou à des fins de santé publique, de recherche, d'innovation, d'élaboration des politiques, de statistiques officielles, de sécurité des patients ou de réglementation****, collectées par des entités et organismes du secteur de la santé ou des soins* (…) ».

[580] Lequel dispose que « *Les organismes responsables de l'accès aux données de santé* ***ne donnent accès aux données de santé*** *électroniques énumérées à l'article 33* ***que si la finalité prévue du traitement poursuivi par le demandeur est conforme*** *: a) aux activités* ***pour des raisons d'intérêt public*** *dans le domaine de la santé publique et de la santé au travail, telles que la protection contre les menaces transfrontières graves pour la santé, la surveillance de la santé publique ou la garantie d'un niveau élevé de qualité et de sécurité des soins de santé et des médicaments ou dispositifs médicaux; b) au fait* ***d'aider les organismes du secteur public*** *ou les institutions, organes et organismes de l'Union, dont les autorités réglementaires, dans le secteur de la santé ou des soins, à accomplir les tâches inscrites dans leur mandat; c) au fait de* ***produire des statistiques officielles*** *à l'échelon national, plurinational et de l'Union en rapport avec les secteurs de la santé ou des soins; d) aux* ***activités d'éducation ou d'enseignement*** *dans les secteurs de la santé ou des soins; e) à la* ***recherche***

finalités interdites). En outre, il est précédé d'un article 33, lequel définit de façon exhaustive les « ***Catégories minimales de données*** *électroniques destinées à un utilisation secondaire* » (33§1), adaptable par actes délégués de la Commission européenne, on le reverra en Partie II.

Le champ d'utilisation secondaire des données de santé et les catégorisations à venir n'est pas celui de notre recherche, laquelle porte sur la dynamique de la notion, non du paramétrage fin des utilisations. Mais c'est l'occasion d'examiner les doctrines et droits qui **ont auparavant conceptualisé la notion de « donnée de santé de vie réelle »** pour promouvoir son emploi (A). Puis nous relèverons les conditions posées en 2016 par le RGPD, qui subdivise les catégories de données selon les buts (B).

B. DYNAMIQUE CONCEPTUELLE DES « DONNEES DE VIE REELLE »

L'utilisation massive à titre secondaire des données de « vie réelle » est l'objet en France d'un rapport en 2017, dans le sillage de la création du SNDS (supra).

Ce rapport théorise le potentiel d'emploi de ces données « *pour la qualité des soins et la régulation du système de santé* » [581]. Nous voyons ici rapidement les difficultés rencontrées dans la caractérisation de la notion (1), avant d'en citer quelques applications juridiques (2).

1. La caractérisation de la notion de « donnée de vie réelle »

Nous traitons ici des contours, plutôt que du contenu, car ce dernier est *a priori* acquis et ici limitatif : il s'agit ici des données de santé **par qualification de la loi** (résultat de l'activité organique des systèmes de santé), non de la production périphérique qui ne s'intègre pas dans les bases de données institutionnelles (SNDS) ni personnelle (ENS).

---

scientifique *ayant trait aux secteurs de la santé ou des soins;* [SEP]*f)* ***aux activités de développement et d'innovation*** *pour les produits ou services contribuant à la santé publique ou à la sécurité sociale, ou à la garantie d'un niveau élevé de qualité et de sécurité des soins de santé, des médicaments ou des dispositifs médicaux;* [SEP]*g) à la* ***formation, au test et à l'évaluation des algorithmes****, entre autres dans les dispositifs médicaux, les systèmes d'IA et les applications de santé numériques, à la contribution à la santé publique ou à la sécurité sociale, ou à la garantie d'un niveau élevé de qualité et de sécurité des soins de santé, des médicaments ou des dispositifs médicaux; h) à* ***la fourniture de soins de santé*** *personnalisés consistant à évaluer, à maintenir ou à rétablir l'état de santé des personnes physiques, sur la base des données de santé d'autres personnes physiques* ».

[581] B. Bégaud, D. Polton, F. von Lennep, « Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé - L'exemple du médicament », juin 2017.

Mais, même entendue de façon ainsi restrictive, la notion de « *donnée de vie réelle* » possède du fait de la disparité des modes de production et des enjeux stratégiques, une **signification équivoque au plan international** (a) ; cela appelle un positionnement national (b).

a. Equivoque internationale de la notion

L'invocation des « données de vie réelle » (en anglais, « *real world data* ») **croît de façon exponentielle**. Alors qu'en 2004 on comptait 207 publications contenant ces mots parmi celles référencées par le site américain PubMed [582], on en compte 9851 référencées en 2022 ; déjà 1423 pour les seuls deux premiers mois de l'année 2023. Naturellement, ces statistiques doivent leur dynamique tout autant à leur production abondante et exploitation pratique, qu'à la motivation doctrinale dans le monde académique (« *publish or perish* ») et le potentiel anticipé. Il n'est pas lieu ici de citer et classer une très abondante bibliographie [583].

Distinctement des applications épidémiologiques et de gouvernance, le but est **fréquemment que les « données de vie réelle » servent de « preuves en vie réelle »**. Le rôle est alors critique pour la régulation des marchés [584] (la pharmacovigilance s'appuie depuis longtemps sur de telles données) ; mais aussi en amont, dans le développement des technologies [585], au point que certains s'interrogent sur les cas dans lesquelles les « données de vie réelle » **sont complémentaires, peuvent être substitutives, voir être sources uniques** par rapport aux données issues des essais cliniques [586], questions qui échappent au champ de notre recherche.

Ce qui nous intéresse ici, est que la ressource des « données de vie réelle » **met immédiatement en exergue le périmètre observé, la qualité des sources et méthodes de recueil**, alors que ces points peuvent devenir décisifs. Certes, il des cas nous le verrons *infra*, dans lequel la « donnée de vie réelle » recherchée se limite à un résultat rapporté sur registre, sur la base d'un indicateur simple. Mais hors de cette hypothèse, les « données de vie réelle » participent d'un large set de données, et seront livrées à l'étude observationnelle statistique « multivariée » (c'est à dire une analyse considérant de multiples variables). **Leur périmétrage et paramétrage sont dès lors un enjeu considérable, voire décisif.**

---

[582] Emanation du NIH américain, National Library of Medicine

[583] Il suffit de taper les mots « real world data » sur le moteur de recherche du site PubMed.

[584] A. Dang, « Real-World Evidence: A Primer », Pharmaceut Med. 2023 Jan;37(1):25-36.

[585] P. Naidoo, C. Bouharati, V. Rambiritch, N. Jose, S. Karamchand, R. Chilton, R. Leisegang, « Real-world evidence and product development : Opportunities, challenges and risk mitigation », Wien Klin Wochenschr. 2021 Aug;133(15-16):840-846 ; auparavant l'article matrice de A. Baumfeld, R. Reynolds, P. Caubel, L. Azoulay, N.A. Dreyer, « Trial designs using real-world data: The changing landscape of the regulatory approval process », Pharmacoepidemiol Drug Saf. 2020 Oct;29(10):1201-1212.

[586] G. de Pouvourville, X. Armoiry, A. Lavorel, P. Bilbault et al. « Données et preuves en vie réelle dans l'évaluation des technologies de santé : dans quels cas sont-elles complémentaires, substitutives, ou les seules sources de données par rapport aux essais cliniques ? » Ther. Vol 78 (1) janvier 2023, 66-80

Dès que l'on ne raisonne plus en termes de résultat prédéfini (selon un indicateur cliniquement pertinent), **expertise scientifique interne et statistique externe peuvent dialoguer, se pondérer ou s'affronter** dans les nébuleuses statistiques [587]. Cela renouvelle plusieurs débats : sur les conflits d'intérêts (qu'est-ce qui explique la statistique issue de la vie réelle ?) ; sur le principe de précaution (quelle significativité statistique de la vie réelle ?) ; sur l'incorporation des sciences sociales (ma vie réelle est elle statistiquement la vôtre ?) etc. Ceci sans compter selon les « conséquences anticipées » qui peuvent déterminer des choix de méthodes et de variables, les échantillons observés, les échelles et délais d'observation, etc.

Ces paradigmes ont induit une tension quasi idéologique : certains auteurs, comme monsieur Anderson, vont jusqu'à prophétiser **l'obsolescence des méthodes scientifiques sous le déluge des données** [588] , alors qu'observation même très fine (de corrélation) et compréhension (de causalité) ne sauraient être confondues, et que l'intelligence dite « artificielle » ne connaît de vraisemblance et de cohérence que statistique.

Dans ce contexte, des auteurs ont cherché la signification internationale des termes « données de vie réelle ». Ils ont rapporté 38 définitions différentes : 20 se rapportaient à des données collectées hors d'un cadre d'essais randomisés contrôlés ; 9 à des données hors d'un cadre interventionnel / contrôlé ; 5 à des données dans un cadre non expérimental ; 4 relevaient d'une catégorie que son hétérogénéité rend non caractérisable. Les auteurs concluent à la difficulté potentielle de dialogue [589] en l'absence de définition univoque. **Il est douteux qu'une telle définition soit possible au plan international**.

Il ne nous a pas semblé nécessaire d'actualiser ce constat de 2017. Depuis cette étude sur le concept (étude qui constate en fait l'absence de concept, et démontre une notion à contenu très variable), six années se sont écoulées de développement exponentiel de la littérature : pour les seules années 2018 à 2022 incluses, on compte un total de 32.739 publications référencées qui incorporent les mots « *real world data* » [590].

---

[587] Baumfeld E, Reynolds R, Caubel P, Azoulay L, Dreyer NA. « Trial designs using real-world data : The changing landscape of the regulatory approval process ». Pharmacoepidemiol Drug Saf. 2020 Oct;29(10):1201-1212 ; comp. Franklin JM, Schneeweiss S. « When and How Can Real World Data Analyses Substitute for Randomized Controlled Trials ? » Clin Pharmacol Ther. 2017 Dec;102(6):924-933.

[588] Anderson C, « The end of theory: The data deluge makes the scientific method obsolete », Wired 2008, Corpus ID: 53810729. https://www.wired.com/2008/06/the-end-of-theo/ (accédé juillet 2021).

[589] Makady A, de Boer A, Hillege H, Klungel O, Goettsch. « What Is Real-World Data? A Review of Definitions Based on Literature and Stakeholder Interviews ». Value Health Jul-Aug 2017;20(7):858-865.

[590] Selon les statistiques du site PubMed préc., qui ne signalent que les publications majoritairement anglophones référencées par le NIH. Par ailleurs, nous n'avons pas intégré dans notre calcul l'année 2017 (2863 publications) et le début d'année 2023 (1423 publications, actualisé à la mi-février).

b. Cadrage méthodologique national de la notion : approche française en 2021

Dans ce contexte d'effervescence et d'imprécision, alors que les enjeux sont proprement stratégiques (si l'on assigne à la « donnée de vie réelle » la valeur de « preuve de vie réelle », quand sont en jeu des politiques de santé publique, ou d'acquisition nationale de technologies dont la négociation de leurs prix), il est nécessaire d'établir une doctrine **qui permette d'homogénéiser les données considérées, et de les rendre recevables** dans une optique d'aide à la décision. Ainsi seulement peut-on passer de la « *notion* », au « *concept* ».

Tel est l'apport en 2021 en France de la doctrine de la Haute Autorité de Santé (HAS), titrée « *Guide méthodologique - Études en vie réelle pour l'évaluation des médicaments et dispositifs médicaux* » [591], laquelle actualise sa doctrine de 2011. De façon emblématique, cette dernière était titrée guide méthodologique des « études post-inscription » [592] (sous-entendu post-inscription des technologies de santé sur la liste remboursable par l'assureur obligatoire). Ce guide a pour objectif de « *soutenir et accompagner les études en vie réelle des produits de santé évaluées par les commissions d'évaluation de la HAS. Il vise à proposer des points de repère pratiques sur les aspects méthodologiques pour* ***optimiser le niveau de preuve de ces études et la confiance dans leurs résultats*** » [593].

La HAS souligne que ses commissions internes, en charge d'élaborer les avis pour l'aide à la décision publique [594], ont « *une longue histoire d'utilisation des données observationnelles également appelées « en vie réelle »,* ***c'est-à-dire les données concernant l'utilisation, l'efficacité ou la tolérance d'un produit de santé en pratique courante****. Afin de réaliser sa mission, d'enrichir et d'accompagner l'évaluation des produits de santé, la HAS analyse régulièrement des données observationnelles et sollicite également des données en vie réelle complémentaires aux essais cliniques lorsqu'elles sont indispensables à une réévaluation* » [595]. **Le recours aux données de vie réelle n'est donc pas nouveau : c'est désormais la pétition d'une approche systématique, qui l'est.**

---

[591] HAS (Guide), « Études en vie réelle pour l'évaluation des médicaments et dispositifs médicaux » (validé le 10/06/2021), voir le site de la HAS

[592] HAS (Guide). « Les études post-inscription sur les technologies de santé (médicaments, dispositifs médicaux et actes) Principes et méthodes » (2011), voir le site de la HAS.

[593] Ibid. (HAS 2021), 2.

[594] Pour l'évaluation des médicaments, la commission de la transparence (CT) ; pour les dispositifs médicaux, la commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (CNEDiMTS) ; pour les vaccins, la commission technique des vaccins ; dans certains cas autres selon notamment des seuils de coûts prévisionnels, d'évaluation économique et de santé publique (CEESP).

[595] Ibid. préc., 4.

Le guide de la HAS détaille ensuite les attentes auxquelles il doit être satisfait, nous ne les passerons pas en revue : **il n'y existe pas de définition de la donnée de « vie réelle », mais des critères de qualification des processus permettant de s'en prévaloir**.

La mise à jour du guide méthodologique en 2021 est justifiée par le fait que les données de santé sont de plus en plus accessibles, grâce notamment à la Plateforme des données de santé précitée (SNDS) ; que l'« *évolution des méthodes d'analyse augment(e) les possibilités d'études comparatives en vie réelle* » ; qu'il devient possible d'intégrer la perspective personnelle des patients et usagers, en termes d'expérience (*Patient-Reported Experience Measure, PREMs*) voire de résultat (*Patient-Reported Outcome Measure, PROMs*).

La HAS **de conclure la justification contextuelle, par le but fondamental** : l'importance de disposer de « *données complémentaires à celles des essais cliniques grâce aux études en vie réelle demandées par la HAS ou réalisées à l'initiative de l'entreprise du médicament ou du (dispositif médical)* », sachant cette tendance croissante en droit comparé [596]. On reviendra sur quelques applications emblématiques.

Mais ces principes d'emploi ne font que mettre en exergue le périmètre des données « de vie réelle exploitables ». Or, nous avons vu l'équivoque de la notion. Cela justifie l'effort en cours de la HAS (appel lancé en mai 2022 actualisé février 2023), de **recenser les sources de données de « vie réelle » (études/bases) mobilisables**, c'est-à-dire suffisamment fiables pour répondre à ses demandes à fin d'évaluation des technologies de santé notamment [597].

[596] Makady A, Ham RT, de Boer A, Hillege H, Klungel O, Goettsch W. « Policies for use of real-world data in health technology assessment : a comparative study of six HTA Agencies ». Value Health 2017;20(4):520-32 et Makady A, van Veelen A, Jonsson P, Moseley O, D'Andon A, de Boer A, et al. « Using real-world Data in Health Technology Assessment practice: A comparative study of five HTA agencies ». Pharmacoeconomics 2018;36(3):359-68.

[597] La HAS a émis un formulaire type titré « Fiche de recensement des études en vie réelle/bases de données pour la HAS », disponible sur sont site sur l'onglet Études en vie réelle - Recensement des sources de données mobilisables pour répondre aux demandes de la HAS.

2. Exemple d'applications stratégiques des « donnée de vie réelle »

En application de son programme de recensement des études/bases de données de vie réelle mobilisable pour son activité d'évaluation, la HAS publie et actualise en 2023 une liste des **sources de données qu'elle retient** [598]. Distinctement, mais dans le même sens de recherche de données de vie réelle exploitables, elle en 2022 publié un panorama des « *entrepôts de données de santé hospitaliers* », **distincts et complémentaires** des bases de données du Programme de médicalisation des systèmes d'information (PMSI) [599].

Il n'est pas lieu ici d'entrer dans le détail de toutes ces bases et applications, auquel ne se réduit pas l'usage des données de vie réelle [600]. Ce qui nous intéresse ici sont **quelques-unes des applications juridiques, au sens prévues, et non seulement autorisées** par le droit.

Le champ est si vaste que nous concentrerons l'attention sur l'usage de ces données, non à titre documentaire ou de pilotage (par exemple pour la conception et conduite de politiques de santé publique à l'échelle nationale ou régionale), mais pour le départage d'obligations portées par des contrats entre les industriels et l'Etat (a). Depuis 2023, elles sont dans certains cas même **non plus seulement prévues, mais imposées par le législateur** (b).

a. La donnée de santé de « vie réelle », appelée par le contrat

Les contrats dont il s'agit sont ceux liant l'Etat français et l'industriel du médicament ou du dispositif médical, par lequel ils conviennent d'un prix remboursable. La « fixation » [601] de ces prix relève d'une alchimie complexe. C'est la raison pour laquelle leur négociation, outre le fait qu'elle s'inscrive dans le cadre du droit de la sécurité sociale, est balisée par un cadre conventionnel, lequel est tracé par les Accords cadre précités entre l'Etat (au travers du Comité économique des produits de santé) et le syndicats des industriels du médicament, pour ne prendre que cet exemple [602]. La doctrine a montré comment ceux-ci « *depuis une décennie*

[598] **Son site n'indique pas quelles sont les sources proposées, mais qu'elle n'aura pas retenues**. Voir Partie « Liste des sources de données retenues par la HAS », sur l'onglet Études en vie réelle - Recensement des sources de données mobilisables pour répondre aux demandes de la HAS, actualisé février 2023.
[599] HAS, Rapport « Entrepôts de données de santé hospitaliers en France - Quel potentiel pour la Haute Autorité de santé ? » validé par le collège le 10 oct. 2022.
[600] Rapport Bégaud préc. 2017, Mission Bothorel 2020 préc.
[601] Négociation, et décision par défaut. Les prix convenu ou décidé est arrêté par les ministres, et publié au Journal officiel. Alors seulement, l'exploitation commerciale peut véritablement commencer.
[602] C. Le Gal Fontes, G. Leguelinel, « De l'importance des données de vie réelle en matière de fixation des prix des médicaments », Rev gen Dr Med 2017, 181s.

(…) mobilisent les données de vie réelle, de façon tâtonnante : ces approches ***visent à corréler le prix payé, à la performance en pratique de soins*** » [603].

Afin de donner une lisibilité réciproque aux parties, et en quelque sorte un **canevas aux négociations pour les structurer et orienter**, ces Accords-cadre posent des principes et méthodes de négociation, mais aussi des concepts propres aux opérations commerciales. Leur actualisation régulière est déterminée par le progrès des technologies, la transformation des marchés, et l'évolution des impératifs nationaux (dont récemment en sortie de crise Covid19, le besoin de « souveraineté sanitaire », lequel motive la recherche d'accords visant la sécurité d'approvisionnement [604]). Dans ce contexte d'obligations d'expression contractuelle, les « données de vie réelle » sont apparues dans plusieurs accords cadre successifs.

En décembre 2012, à l'appui du concept de **contrat de « prix conditionnel »**, porté par l'article 10 ter. Il s'agit « alors d'une voie optionnelle, dérogatoire », laquelle vise permet de convenir rapidement d'un prix facial (le prix publié, fondé sur la valeur perçue à l'issue des essais cliniques), lequel prix facial sera potentiellement modulé (pour aboutir au « prix réel » confidentiel) selon la performance rapportée en « vie réelle » [605].

En décembre 2015, le nouvel Accord-cadre fait apparaître pour la première fois la notion de **« contrat de performance »** [606]. Son article 12 toutefois mixe plusieurs mécanismes d'une façon critiquée par la doctrine [607] pour un résultat dénoncé dans un rapport du CEPS [608].

En mars 2021, le nouvel Accord-cadre [609] « *distingue les approches mêlées en 2015. Il ne les présente plus comme des voies optionnelles par défaut, mais comme des approches de première intention* » [610] : il introduit une **approche renouvelée du « contrat de performance »** (titre de l'article 15a), distinct du « **contrat portant sur la transposabilité en vie réelle** » (titre de l'article 16). Dans les deux cas réduit significativement le nombre de

[603] F. Megerlin, « Technologies de Santé : vers l'achat de 'résultats' » ? Actes du colloque, 40 anniversaire de l'AFDS « Les mouvements du droit de la santé », hors série Rev. dr. san. soc. 2022, Dalloz éd., 135-147.
[604] Idéalement par la relocalisation de production en France / en Europe, de la fabrication de produits parfois « matures ». La LFSS 2022 y incite expressément en prévoyant la prise en compte des lieux de production dans la fixation des prix.
[605] Article 10ter, Accord-cadre du 5 déc. 2012 entre le CEP et le LEEM, disponible sur le site du CEPS.
[606] Article 12, Accord cadre du 31 déc. 2015, entre le CEP et le LEEM, disponible sur le site du CEPS.
[607] F. Megerlin, « Médicaments innovants onéreux : vers le paiement de résultats contractualisés ? » n° *Prix des médicaments*, Rev. Fr. aff. Soc. / DREES 2018 (3) 129-146.
[608] Rapport d'activité 2019, publié en 2020, disponible sur le site du CEPS.
[609] Articles 15a et 16, Accord-cadre du 5 mars 2021 entre le CEP et le LEEM, disponible sur le site du CEPS.
[610] Megerlin F., RDSS 2022 préc., page 142.

variables (c'est-à-dire donc de « données de vie réelle ») à considérer pour caractériser la performance contractualisée, ou à observer.
Un nouvel Accord cadre devra être adopté en 2024, à moins d'une prorogation du précédent.

Il n'est pas lieu ici de tenter une explication de ces mécanismes complexes. Notons simplement que, après une période marquée par le paradigme de variables multiples à considérer, semble succéder un paradigme de variables réduites en nombre voire très limitées. A quel point ? dans son extension conceptuelle maximale, « *dans le contrat qui n'a pas pour objet une évaluation à terme par statistique multivariée, une donnée unique de 'vie réelle' peut être considérée : le résultat, tel que prédéfini* » [611]. Cela **réduit sensiblement la problématique de la définition de la « donnée de vie réelle », du moins pour cette négociation des prix** fondée sur les registres de résultat. Encore faut-il identifier un indicateur de performance qui soit cliniquement pertinent ; et que le registre soit renseigné.

Dans ce cadre toujours de fixation des prix, l'obligation de considérer une « donnée de vie réelle » n'est plus seulement portée par des figures contractuelles : elle est **depuis 2023 imposée par la loi.**

b. La donnée de santé de « vie réelle », convoquée par la loi

Sur les 3 dernières années, on peut à nouveau relever une dynamique très forte en ce sens, que cela relève du nouveau régime des accès dérogatoires aux médicaments (i), ou du cadre légal autonome d'accès au marché de médicaments de thérapie innovante (ii).

i. l'exemple des modèles d'accès dérogatoires : organiser la stéréoscopie des données

En 2020, le législateur a refondu l'ex-système des autorisations temporaires d'utilisation nominative (ATUn) et de cohorte (ATUc), des prises en charge temporaires (PEC-T), des recommandations temporaires d'utilisation (RTU), lequel s'était complexifié [612]. Il en résulte un nouveau cadre dérogatoire d'accès aux médicaments, modifié encore en 2021 et 2022 : les

[611] Ibid., page 144. *Comp*. en faveur de l'analyse statistique multivariée, R. Launois, O. Ethgen, « Contrats de risk-sharing : choix des schémas d'étude et des critères de jugement », Ann. Pharm. Fr. n°5, 2013, pp. 346-357.
[612] Loi n° 2020-1576 du 14 décembre 2020 de financement de la sécurité sociale pour 2021, modification par Loi n° 2021-1754 du 23 décembre 2021 de financement de la sécurité sociale pour 2022, puis encore par Loi n° 2022-1616 du 23 décembre 2022 de financement de la sécurité sociale pour 2023.

autorisations accès précoce (AAP, pré- ou post-AMM), les autorisations d'accès compassionnels (AAC), et cadres de prescription compassionnelle (CPC) [613].

A l'avènement de ce nouveau cadre, nous avons contribué à une étude **portant spécifiquement sur le régime de production des données,** qui s'est avéré autonome à l'égard du droit de la recherche impliquant la personne humain malgré l'extension considérable de celui-ci depuis une dizaine d'années, dans le champ observationnel (*supra*) [614]. Ce qui nous intéresse ici est que pour chacun des cas d'accès dérogatoire, le législateur a imposé la production de données afin d'en documenter les circonstances et les effets.

Pour l'accès précoce, il s'agit d'une **obligation légale**, laquelle prévoit notamment que « *L'autorisation d'accès précoce est **subordonnée au respect**, par l'entreprise qui assure l'exploitation du médicament, d'un **protocole d'utilisation thérapeutique et de recueil des données**, défini par la Haute Autorité de santé et annexé à la décision d'autorisation* » (article L. 5121-12-IV CSP), que cet accès soit pré-autorisation de mise sur le marché du médicament, ou post-autorisation de mise sur le marché. Depuis 2023, la pertinence du recueil de données est dans ce dernier cas discutée [615].

Pour les accès compassionnels, la loi est moins stricte ; ils « ***sont assortis d'un protocole** d'utilisation thérapeutique et de suivi des patients qui précise les conditions de recueil des informations concernant l'efficacité, les effets indésirables et les conditions réelles d'utilisation du médicament (...)* » (article L. 5121-12-1-V. CSP). Cela est étonnant, car l'accès compassionnel recouvre également, nous l'avons souligné, l'accès pré-précoce.

L'application de cette distinction est nette au plan européen (Tableau X), avec également des conséquences différenciées par le droit européen adopté en 2021, lequel va progressivement unifier l'évaluation des technologies de santé en Europe [616].

---

[613] B. Juillard-Condat, L. Tribaudeau, F. Taboulet, « Articulation entre accès précoce et l'accès de droit commun aux médicaments : quels impacts peut-on attendre de la réforme de 2021 ? » Rev. Gen. Dr. Med. 2023 n°10, 9-28 ; auparavant, B. Juillard-Condat, L. Tribaudeau, F. Taboulet, « Accès précoce et compassionnel : quel impact de la réforme en matière de sécurité sanitaire et d'accessibilité ? » *ibid*. n°9, 2022, 347-374.

[614] F. Megerlin, E. Pinilla, Cl. Huriet, « Recueil de données sur les médicaments en accès précoce : quel lien avec la recherche 'impliquant' les personnes humaines ? » Rev Gen Dr Méd 2022 (1), 375-388.

[615] HAS Commission de la transparence, 25 janv. 2023, voir les propos de son président Mr. P. Cochat, quant à l'apport des PUT-RD.

[616] F. Megerlin, E. Pinilla, Cl. Huriet, « Règlement européen de 2021 sur l'évaluation des technologies de santé : place des données de 'vie réelle' ? » Rev Gen Dr Méd 2023(2), 281-294.

	Accès précoce	Accès compassionnel
Cadre	PUT - « Recueil des données »	PUT - « Suivi des patients »
But	Recueil de données précises sur le patient	Recueil d'informations sur le médicament
Impérativité	Accès « subordonné » au PUT-RD	Accès « assorti » d'un PUT-RD
Portée nationale	Contribue à l'évaluation / remboursement	Permet l'adaptation des autorisations / cadres
Extension de champ	Egalement applicable aux accès post AMM	Egalement applicable aux accès pré-précoces
Portée européenne	Obligation de partage des données (Règlement 2021, consid. 33, article 10.3)	Coopération volontaire en matière de données (Règlement 2021, article 23.1.d)

On note ici un cadre bien différent de génération, de granulométrie et de vocation de la donnée recueillie, qui se retrouve d'ailleurs dans les textes européens : en application du règlement européen de 2021 (*infra*), les données relatives aux « accès précoces » **devraient être partagées** (approche intégrative à compter de 2025), les données relatives aux « accès compassionnels » **peuvent ne pas l'être** (l'approche reste coopérative) (*infra, partie II*) ; ceci bien que les données relatives aux usages compassionnels ne soient pas de moindre intérêt, compte tenu des conséquences cliniques et des coûts associés [617].

Pour quel usage national ? la doctrine de la Haute Autorité de santé, publiée en la matière (2021), est explicite : il s'agit d'une « ***opportunité de collecte de données observationnelles / en vie réelle*** », qui permet de documenter l'utilisation des médicaments objet de l'AAP, mais aussi d'« *alimenter les futures étapes d'évaluation par la commission de la transparence* » [618]. Le but est ainsi de disposer d'une forme de vision stéréoscopique grâce à la conduite en parallèle d'études interventionnelles (essai clinique) et observationnelles (au titre AAP). En pratique, l'intérêt en 2023 apparaît nuancé, surtout pour le recueil de données post-AMM.

[617] F. Megerlin, E. Pinilla, Cl. Huriet, Règlement européen de 2021 sur l'évaluation des technologies de santé : place des données de « vie réelle » ? Rev. gen. dr. med. 2023 n°10, 281-294.
[618] Autorisation d'accès précoce aux médicaments : doctrine d'évaluation de la HAS, doctrine adoptée par le Collège le 27 avril 2022, spéc. p 13.

Mais la loi va parfois plus loin, lorsque la génération de données n'intéresse plus l'évaluation à venir, mais le paiement de certains médicaments.

ii. l'exemple de l'accès des médicaments de thérapie innovante

En 2022, la loi de financement de la sécurité sociale pour 2023 a introduit, non dans le Code de la santé publique, mais **dans le Code de la sécurité sociale**, des dispositions qui traitent spécifiquement de la fixation du prix et de la méthode de paiement des « médicaments de thérapie innovante » au sens du droit européen. De façon inédite, l'article L. 162-16-6 CSS est augmenté d'un V. qui introduit **un mécanisme de paiement subordonné à deux données de vie réelle**, et ceci de façon remarquable par voie légale, plutôt que par voie conventionnelle [619], en contraste de la pratique établie en la matière depuis une douzaine d'années (*supra*) [620].

Toutefois, cette approche de la « donnée décisive » ne vaut que dans le champ très spécifique des médicaments de thérapie innovante **au sens du droit européen** [621], **plus large que celui du droit français** : ce dernier (L. 5121-1-17° CSP [622]) n'englobe en effet pas la « préparation de thérapie génique » (L. 5121-1-12° CSP [623]). N'étant pas compétent pour distinguer ces produits, et cette distinction n'étant par ailleurs pas nécessaire ici à la démonstration, nous nous en tenons ici à constater la donnée requise et son application.

En effet, ce qui nous intéresse est que la LFSS 2023 subordonne la continuité du paiement au succès clinique revendiqué par correction d'une anomalie biologique [624]. Ainsi, le nouvel article L. 162-16-6-V-C. CSS prévoit qu'« *en cas d'échec du traitement pour un patient,*

[619] V. Daël, « Remboursement des médicaments innovants en France : la solution du contrat de performance individuelle à paiements étalés », préc. ; F. Megerlin, F. Lhoste, LFSS 2023 et « Médicaments de Thérapie Innovante » : consécration du contrat de résultat ? » Rev Gen Dr Méd 2023(2), 259-266.

[620] Megerlin F, « Technologies de santé : vers l'achat de « résultats » ? Rev. dr. san. soc. Dalloz, 2022, Hors série, Actes du 40ème anniversaire de l'AFDS – Paris La Sorbonne, 135-147.

[621] L'article L. 162-16-6 rappelle *in extenso* que les MTI sont définis « à l'article 2 du règlement (CE) n° 1394/2007 du Parlement européen et du Conseil, du 13 novembre 2007, concernant les médicaments de thérapie innovante et modifiant la directive 2001/83/ CE ainsi que le règlement (CE) n° 726/2004 ».

[622] On entend par « *17° Médicament de thérapie innovante préparé ponctuellement, tout médicament tel que défini dans le règlement (CE) n° 1394/2007 du Parlement européen et du Conseil, du 13 novembre 2007, concernant les médicaments de thérapie innovante et modifiant la directive 2001/83/CE ainsi que le règlement (CE) n° 726/2004, fabriqué en France selon des normes de qualité spécifiques et utilisé dans un hôpital en France, sous la responsabilité d'un médecin, pour exécuter une prescription médicale déterminée pour un produit spécialement conçu à l'intention d'un malade déterminé* (…) ».

[623] On entend par « *12° Préparation de thérapie génique, tout médicament autre que les spécialités pharmaceutiques et les médicaments fabriqués industriellement mentionnés à l'article L. 5121-8, servant à transférer du matériel génétique et ne consistant pas en des cellules d'origine humaine ou animale* ».

[624] Une doctrine de la Commission de la transparence incorporant ce point est à paraître en fin 2022/ 23.

notamment en cas de décès, ou en cas d'administration concomitante ou séquentielle d'un autre traitement de même visée thérapeutique*, les versements cessent* ».

Comment établir l'arrêt du traitement, ou l'administration concomitante ou séquentielle d'un autre traitement de même visée thérapeutique, **sinon en considérant les données de santé** ? La loi dispose (V-C. alinéa 4) que l'« *entreprise (concernée)* ***assure à sa charge le recueil des données.*** *Les prescripteurs lui transmettent à cette fin les données de suivi des patients traités, selon des modalités* ***assurant le respect du secret médical*** ».

On pourrait s'étonner de cette approche, calquée sur le recueil des données dans le cadre des protocoles d'utilisation thérapeutique : l'arrêt par décès, ou l'administration concomitante ou séquentielle d'un autre traitement, est facile à établir par le PMSI, sans besoin de transmettre de données de santé à l'entreprise, à l'égard duquel il n'y a en fait pas de secret médical, compte tenu de la nature très particulière des produits « sur mesure ». En revanche, d'autres données plus précises pourraient certes être sollicitées, mais hors des prévisions de la loi [625].

La clause légale de protection des données ne vaut donc en fait qu'à l'égard de tiers, alors que l'on est ici hors d'un cadre légal de RIPH : le but est la mise à disposition d'un traitement autorisé, non son expérimentation clinique par étude interventionnelle doublée d'une étude observationnelle à la faveur d'un accès précoce.

B. SUBDIVISION DU CONCEPT DE DONNEE DE SANTE « DE VIE REELLE » : POROSITE ENTRE CATEGORIES

Nous venons de relever la dynamique en droit français, **telle qu'elle est impulsée par la loi**, non plus seulement de la qualification et du stockage, mais, au-delà de la production classique des soins, de la pharmacovigilance, etc., de génération et d'exploitation de la donnée de vie réelle. **C'est un enjeu stratégique national.**

Cette approche est encore singulière en Europe ; une approche en droit comparé dépasserait l'objet de notre thèse [626], mais il est intéressant ici de relever **comment, en droit européen, le phénomène est qualifié,** car il en découle une subdivision des notions.

[625] Megerlin F, Lhoste F, « LFSS 2023 et « Médicament de thérapie innovante » : consécration du contrat de résultat ? » Rev. gen. Dr. Med. 2023, n°10, 259-266.
[626] Et serait d'intérêt temporel limité, du fait de l'avènement annoncé de l'EESD proposé le 3 mai 2022.

La stratégie européenne des données de santé distingue trois catégories de données : les données à caractère non personnel, les données à caractère personnel, les données dites « mixtes ». Or, dans son avis de 2020, le CEPD relève qu'une combinaison de données à caractère non personnel peut conduire à une ré-identification d'une personne [627] ; on reviendra abondamment *infra* sur cette question aux conséquences majeures.

Cette question critique a été envisagée par de nombreux actes du droit dérivé : directive de 1996, de 2002, puis en 2016 par le Règlement général de protection des données précités ; en 2022, par le règlement sur la gouvernance des données de santé, et par les proposition de règlements sur l'espace européen des données de santé et sur l'intelligence artificielle, nous le verrons en Partie II.

Ce qui nous intéresse ici est la **catégorisation juridique des données de santé** dans un but d'utilisation secondaire, que nous avons précédemment définie *supra* selon les termes de la proposition de règlement de mai 2022 sur l'EEDS [628]. Mais ceci selon un critère transverse : on les distinguera selon qu'il s'agit de données personnelles (1), ou présentées comme *devenues* non personnelles (2) ; la nuance n'étant pas anodine, dans un contexte de rapides progrès technologiques en matière de vitesse et de volume de traitements, et alors que les la combinaison des deux est parfois requise (3).

1. Dualité juridique des « données personnelles » susceptibles d'utilisation secondaire

Par données personnelles, on entend d'abord nous l'avons vu les données « nominatives », lesquelles par définition identifient la personne à laquelle elles se rapportent (en dehors des mesures de police sanitaire dont la pharmacovigilance et autres régimes autonomes) ; ce scénario a été consacré en 2023, mais reste isolé (a). La donnée « pseudonymisée » reste quant à elle une donnée personnelle, mais, de façon réversible, a cessé d'être nominative (b).

a. Utilisation de la donnée nominative, quelle dynamique ?

Nous avons vu que la LFSS 2023 avait modifié le Code de la sécurité sociale, pour fonder le paiement de certains médicaments selon (ou plutôt pour) la durée du résultat rapporté en « vie réelle », selon une donnée de santé légalement échangée sous couvert de secret médical. Cette

[627] CEPD, Avis 3/2020 sur la stratégie européenne pour les données (16 juin 2020), page 9 n° 30 et s.
[628] COM(2022) 197 final, 2022/0140 (COD) préc., voir spéc. article 2§d pour la définition de l'« utilisation primaire », vs. article 2§e pour la définition de « l'utilisation secondaire », lequel renvoi au chapitre IV (spéc article 33, pour le champ « minimal » des données concernées).

pratique de prise en considération de données personnelles pour l'évaluation en vie réelle des technologies est innovante dans son fondement légal, mais participe d'un courant précité : il vise essentiellement au management de l'incertitude économique (celle de ne pas retrouver en pratique de soins, le résultat clinique perçu à l'issu des essais, qui avait fait consentir au prix initial), l'incertitude clinique étant l'objet du suivi des soins.

Dans le contexte précité de RIPH et de AAP/ AAC/ CPC [629], **le traitement des données relève de méthodes dédiées ou d'un régime autonome**, qui n'excluent pas une utilisation secondaire, également prévu dans le futur droit européen [630]. Ainsi, dans le cadre de la mise en œuvre des Protocoles d'utilisation thérapeutique – recueil de données, la HAS présente, sur son site internet, un récapitulatif de « *l'ensemble des données collectées dans le cadre des autorisations d'accès précoces délivrées par la HAS dans l'objectif de* ***promouvoir leur réutilisation à des fins de recherche*** **»** [631].

Dans le cadre de « l'accès précoce », le guide HAS de 2021 spécifie que sont susceptibles de recueil, outre les données habituelles, des données d'ordre ethnique, génétique, d'habitudes de vie, « *si strictement nécessaires* » [632]. Surtout, il indique que, sauf opposition du patient, ces « *données personnelles pourront également être utilisées ensuite pour faire de la recherche, étude ou de l'évaluation dans le domaine de la santé (…) Dans ce cadre, elles* ***pourront être utilisées de manière complémentaire avec d'autres données vous concernant****. Cela signifie que vos données personnelles collectées au titre de l'accès précoce pourront être croisées* avec des données du (SNDS) » ; **en principe donc**, pas avec d'autres types de données [633].

Mais l'accès à la donnée de santé personnelle tend à se développer en dehors de ces cadres (recouvrant les études post-inscription demandées par la HAS et le CEPS), y compris en dehors des contrats de prix visés par l'accord-cadre de 2021 et la LFSS de 2023 précités.

---

[629] RIPH : recherche impliquant la personne humaine, AAP : Autorisation d'accès précoce ; AAC : autorisation d'accès compassionnel ; CPC : cadre de prescription compassionnelle.
[630] On le reverra dans l'article 33 du projet de règlement EEDS de 2022, notamment 33§4 : « *Les données de santé électroniques comportant des droits de propriété intellectuelle (PI) protégés et des secrets d'affaires d'entreprises privées protégés sont mises à disposition à des fins d'utilisation secondaire. Lorsque ces données sont mises à disposition à des fins d'utilisation secondaire, toutes les mesures nécessaires pour préserver la confidentialité des droits de PI et des secrets d'affaires sont prises ».*
[631] Voir de la HAS, Liste des protocoles d'utilisation thérapeutique et de recueil de données en cours et terminés, publié le 21 juin 2022.
[632] HAS, Accès précoce à un médicament –Traitement des données personnelles, juill. 2021, page 1.
[633] *Ibid.,* page 3.

En ce sens, relevons en exemple la plus récente délibération en 2022 de la CNIL en la matière (à la date de notre rédaction), sur le projet de création d'un entrepôt de données [634]. Ce projet vise à « *permettre la réalisation de recherches, d'études ou d'évaluations dans le domaine de la santé destinées notamment à : décrire des conditions d'utilisation des produits de santé en pratique courante dans le cadre du parcours de soins ; mesurer l'efficacité et les risques liés à l'utilisation d'une thérapeutique (médicament, dispositif médical, solution digitale, etc.) ; mesurer l'impact organisationnel d'un produit de santé ; mesurer la consommation de ressources et la performance médico-économique d'une thérapeutique en vie réelle* ». Bien que le projet soit porté par des acteurs privés, ces motifs permettent de **justifier l'intérêt public de traitements qui impliquent des données de santé**, et rattachent cet entrepôt de données de santé aux articles 44-3° et 66-III de LIL modifiée.

Dans cet exemple, il est spécifié que l'entrepôt sera abondé par des données nominatives **issues des dossiers médicaux des patients** qui bénéficient de médicaments au titre des autorisations d'accès précoce exploitées par le laboratoire pharmaceutique responsable conjoint du traitement ; et pour les patients concernés, **de leurs données personnelles issues du Système national des données de santé,** puisqu'un appariement des données nominatives est requis. On est là dans le cœur de la catégorie des données de santé nominatives.

Pour autant, la délibération souligne que « *le statut de membre du consortium* ***ne confère aucun droit à l'accès aux données du SNDS contenues dans l'entrepôt*** *; seul le membre du consortium désigné comme tiers de confiance* (la société X) *dispose d'un accès aux données du SNDS dans le respect des missions qui lui sont confiées* » [635]. Les vases ne sont donc pas complètement communicants, et l'usage de l'entrepôt est assorti par la CNIL de nombreuses restrictions, qu'il n'est pas lieu de développer [636] (article L. 4113-7 CSP).

Cette délibération montre à quel point le sujet est bien cadré en France, dans le respect du droit Européen. Signalons une situation beaucoup plus complexe aux Etats-Unis, quant à la recherche de résultats centrés sur les patients (*Patient-centered outcomes research, PCOR*),

[634] Délibération n° 2022-063 du 23 mai 2022 autorisant le consortium AGORIA SANTE composé des sociétés Docaposte, AstraZeneca et Impact Healthcare à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données de santé, dénommé « Plateforme Agoria santé » (demande d'autorisation n° 2225091).
[635] *Ibid*., c'est la CNIL qui souligne.
[636] Dont l'interdiction des fins de promotion de produits de santé vers des professionnels ou établissements, de modulation de primes d'assurance en santé, de prospection commerciale sur la base de fichiers qui permettraient d'identifier directement ou indirectement les prescripteurs, etc.

du fait de la dispersion et parfois de conflits entre droits applicables [637], et de comportements que nous évoquerons avec l'étude des données de santé « synthétiques ».

b. La donnée de santé « pseudonymisée »

Si dans le champ de recherche précité, le recours à la donnée de santé nominative (identifiant le patient) s'impose, il existe d'autres champs où **le recours à une donnée personnelle est nécessaire sans que l'identification de la personne concernée s'impose**. Cela justifie le procédé de pseudonymisation des données, qu'un tableau didactique de la CNIL permet de comprendre en miroir du procédé d'anonymisation que l'on évoquera *infra* [638].

Tableau de source CNIL *(distinction entre pseudonymisation et anonymisation*)

Processus	Pseudonymisation	Anonymisation
Statut des données	Personnelles (restent indirectement identifiantes et donc soumises au RGPD et à la loi Informatique et Libertés	Anonymes
Réutilisation des données	Sous conditions	Sans restriction
Utilité des Données	Préservée car pas d'altération du niveau de détail des données	Plus ou moins altérée en fonction des objectifs poursuivis et des méthodes appliquées
Méthodes à mettre en œuvre	Compteur, générateur de nombres aléatoires, fonction de hachage, chiffrement à clé secrète, etc.	Dépend des objectifs poursuivis : confidentialité différentielle, randomisation, k-anonymat, l-diversité, t-proximité, etc.
Complexité de la mise en œuvre	Simple à moyenne	Dépend des objectifs poursuivis : simple dans certains cas comme l'agrégation ou le comptage et complexe dans d'autres

Or, aucune de ces deux notions n'a fait l'objet d'une définition en droit français dans la LIL de 1978 modifiée, qui du fait de son objet aurait pu en être le véhicule naturel. Les termes « pseudonyme », « pseudonymisation », « anonyme » en sont absents ; « anonymisation » présente une unique occurrence, lorsque la loi énonce depuis 2016 parmi les missions de la CNIL (article 8-I, i.) qu'elle peut « *certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification, par des tiers agréés ou accrédités selon les*

[637] Office of the National Coordinator for Health Information Technology, « Privacy and Security Framework for Patient-Centered Outcomes Research (PCOR) » FINAL REPORT July 2020 (site de l'ONC).
[638] Voir l'onglet titré « *Recherche scientifique (hors santé) : enjeux et avantages de l'anonymisation et de la pseudonymisation* » Site de la CNIL, mise à jour au 31 janvier 2022.

modalités mentionnées au h du présent 2°, de la conformité à la présente loi ***de processus d'anonymisation des données à caractère personnel*** (…) » [639].

De façon purement doctrinale donc, la pseudonymisation est définie par la CNIL comme « *un* ***traitement de données personnelles*** *réalisé de manière à ce qu'on ne puisse plus attribuer les données à une personne physique identifiée* ***sans information supplémentaire*** » [640]. Mais, dès lors que l'on dispose de l'information supplémentaire conservée séparément, il est possible par cette clef de reconstituer l'identité de la personne dont les données sont détenues [641].

En conséquence, comme l'énonce la CNIL, les « *d****onnées résultant d'une pseudonymisation sont (…) considérées comme des données personnelles et leur traitement reste intégralement soumis aux obligations du RGPD*** **». Il n'en va pas de même des données anonymisées, réputées de ce fait non personnelles.**

2. L'utilisation secondaire de « données de santé » devenues « non personnelles »

Comment, lorsqu'une donnée de santé est **nativement personnelle, devient-elle « non personnelle » ?** L'anonymisation de données de santé réelles est la stratégie de référence, qui permet dans l'intérêt général, d'exploiter des données ouvertes en limitant les risques pour les personnes [642]. Elle est définie par la norme ISO 29100:2011 comme le « *processus par lequel des informations personnellement identifiables (IPI) sont irréversiblement altérées de telle façon que le sujet des IPI ne puisse plus être identifié directement ou indirectement, que ce soit par le responsable du traitement des IPI seul ou en collaboration avec une quelconque autre partie* » [643] ; l'ISO souligne que cette norme n'a de prétention que technique, pas vocation de « modèle mondial de politique, ni (de) cadre législatif » [644].

Mais la donnée anonyme qui en résulte n'est pas une catégorie en droit national, ni européen, lesquels droits ne connaissent que des « données personnelles », pour les soumettre à leur

[639] Apport de la Loi n° 2016-1321 du 7 octobre 2016 « pour une République numérique ».
[640] *Ibid*. doctrine de la CNIL.
[641] Tables de correspondances avec les pseudonymes, données tierces permettant de ré-identifier les individus à partir de connaissances préalables, etc.
[642] Sur la « donnée synthétique », *infra.*
[643] Première édition en 2011-12-15 ; dernier examen en 2017 par L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale).
[644] Même si « des juridictions peuvent exiger la conformité avec un ou plusieurs documents référencées dans l'ISO/IEC/ JTC 1 :SC 27 WG 5 Standing Document 2 (WG 5 SD2) *Officially Privacy Documents Références* », la norme dixit (page v).

protection [645] (sous réserve du *Data Governance Act* de 2021, sur lequel on reviendra). Ainsi, la notion même de donnée anonyme **n'a pas de définition en droit, et *a priori* n'en a pas besoin** (a). Elle est définie comme le résultat d'un processus ; mais cela pose la question de savoir à quel point la donnée **initialement personnelle est devenue « anonyme »** (b).

a. La donnée personnelle de santé « anonymisée »

Nous venons de voir que la « pseudonymisation » d'une donnée lui laissait son caractère de donnée personnelle, **afin d'en préserver la précision granulométrique** : c'est une condition de sa valeur selon les exigences des usages secondaires envisagés, *supra*. Ainsi, la notion de « pseudonymisation » connaît de nombreuses occurrences dans les droits applicables : notamment dans le règlement 2016/679, avec 8 occurrences dans les considérants, et 6 occurrences dans le *corpus* normatif dont sa définition dans l'article 4 point 5.

Mais **tel n'est pas le cas de l'« anonymisation », ni de la notion de « donnée anonyme ».** Ces notions ne sont pas définies dans la directive 95/46/CE, où la notion « anonymisation » n'est paradoxalement évoquée que dans un unique considérant [646]. Pas plus, elles ne sont définies dans le règlement RGPD, où la notion elle connaît le même sort, dans un considérant qui d'ailleurs porte le même numéro [647]. En revanche, une **définition conceptuelle stable** en a été présentée en 2014 par le groupe de travail européen dit « de l'article 29 » (à statut d'organe consultatif européen, distinct du CEPD), qui a éclairé l'élaboration du RGPD [648].

En substance, le considérant 26 signifie, selon le GT 29, qu'une donnée devient anonyme lorsqu'elle est expurgée des éléments qui rendaient identifiable la personne concernée. Les données ainsi rendues anonymes ne doivent plus pouvoir être utilisées pour l'identifier par « *l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre* » par qui que ce soit, **et cela de façon irréversible**. Dans plusieurs textes européens, le caractère irréversible

[645] Sans préjudice toutefois, pour les données non personnelles, d'autres droits protecteurs comme celui de la confidentialité des communication etc.
[646] Considérant n° 26 de la directive 95/46/CE, pour signaler que « *les principes de la protection ne s'appliquent pas aux données rendues anonymes* ***de telle manière que la personne concernée n'est plus identifiable*** »
[647] Considérant n° 26 du RGPD de 2016, où le mot présente trois occurrences.
[648] Avis 05/2014 du 10 avril 2014 sur les techniques d'anonymisation (0829/14/FRWP216), rendu par le GT sur la protection des personnes à l'égard du traitement des données à caractère personnel de l'article 29,; ce GT a été institué par l'article 29 de la directive 95/46/CE (qui donc a précédé le RGPD de 2016) ; ses missions sont définies à l'article 30 de cette directive.

s'assimile à l'« *effacement* » [649] ; il n'existe donc pas de clefs (table de correspondance, marqueur) pour un retour à l'état *ex ante*. Mais le critère du « raisonnable » est en question.

Ceci est en effet une **définition, non par le processus, mais par le résultat**. Or, une telle définition n'a pas besoin de détailler ni même d'évoquer les techniques (évolutives) qui obligeraient les opérateurs, ni d'exposer les méthodologies de validation, dont nous avons vu que, depuis la loi de 2016, la CNIL « peut » les certifier. Mais il reste surprenant que le processus d'anonymisation **censé être irréversible ne donne pas lieu à une définition** dans le corpus normatif du règlement de 2016, malgré les trois occurrences du mot « anonyme » (concentrées dans le considérant n°26) – alors que tel est en revanche le cas pour le processus de « pseudonymisation » (article 4, point 5) [650] : cela renvoi au droit national, le soin d'énoncer les obligations des opérateurs et leur sanction.

Pas plus, le processus d'anonymisation n'est défini **dans la proposition de règlement de 2022 sur l'intelligence artificielle** : il y est seulement évoqué de façon incidente, pour une finalité « *de la surveillance, de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque* », que le recours à la pseudonymisation ou au cryptage peut être préférés « ***lorsque l'anonymisation peut avoir une incidence significative** sur l'objectif poursuivi* » [651], donc la perte d'intérêt par le floutage d'éléments décisifs des sets de données.

Si l'IA peut consommer des données avec une appétence pour les données les plus précises (et le risque de ré-identification induit), nous verrons qu'elle pourrait aussi générer des données de santé anonymes (?) au sens de « données synthétiques », *infra*. En revanche, le processus d'anonymisation est évoqué dans le considérant n° 40, lequel traite de la matière judiciaire, pour reconnaître ou dénier la qualification d'IA « à haut risque » [652].

---

[649] Toujours dans un considérant n° 26, mais de la directive cette fois 2022/58/CE sur vie privée et communications électroniques : « *Il **convient également d'effacer ou de rendre anonymes** les données relatives au trafic utilisées pour la commercialisation de services de communications ou pour la fourniture de services à valeur ajoutée, lorsque les services en question ont été fournis* » ; on retrouve l'idée dans l'article 6§1 : « *Les données relatives au trafic (…) doivent être **effacées ou rendues anonymes** lorsqu'elles ne sont plus nécessaires à la transmission d'une communication* (…) ».

[650] On entend par « *5) « pseudonymisation », le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;* »

[651] Préc., voir article 10.5

[652] Ainsi, cette qualification **ne devrait « *pas s'étendre** aux systèmes d'IA destinés à être utilisés pour des activités administratives **purement accessoires** qui n'ont aucune incidence sur l'administration réelle de la*

En santé, la distinction est **sensible** également pour les entreprises en compétition, qui **s'affrontent sur le terrain de l'irréversibilité des processus.** Ainsi l'une (IMS Health) n'hésite pas à attaquer en recours pour excès de pouvoir une délibération de la CNIL autorisant un traitement de données à l'autre (Celtipharm) ; le Conseil d'Etat de juger en 2014 que, « ***dès lors que ces données font l'objet d'une anonymisation irréversible,*** *le traitement autorisé par la délibération attaquée ne saurait avoir pour effet de porter atteinte au secret professionnel et au respect de la vie privée des patients* » [653]. L'invocation par le Conseil d'Etat d'un concept d'« anonymisation irréversible » **est frappante, car, par définition, le concept d'« anonymisation » devrait être irréversible.** Cela peut néanmoins laisser habilement une porte ouverte à la démonstration du contraire, afin d'éclairer la police du marché sur l'évolution technologique et le potentiel de réversibilité.

b. L'irréversibilité de l'anonymat de la donnée : à quel point ?

La question de l'irreversibilité est critique à tous égards. Sur ce point, autorités de régulation, ingénieurs et technologues sont très actifs [654] ; on trouve par ailleurs dans l'avis de 05/2014 du groupe de travail européen dit « GT article 29 » précité, un état de l'art d'alors des techniques d'anonymisation avec une analyse de forces, faiblesses, opportunités, menaces [655]. **Le contexte a changé,** avec l'essor des outils et l'accroissement exponentiel des capacités de calcul notamment – mais il n'est pas lieu ici de développements d'ordre technique [656].

Sur un plan juridique, peu de doctrines se sont intéressées à la distinction des obligations de moyen et de résultat dans la conformité sur ce point au RGDP, notant que les jurisprudences nationales et européenne auraient à tracer les contours des obligations [657]. Il n'en existe toujours pas d'exemple à la date de notre rédaction, mais nous avons vu la porte habilement laissée ouverte par le Conseil d'Etat, qui invite implicitement à la démonstration. Rappelons que depuis 2016, la CNIL « ***peut certifier ou homologuer*** *et publier des référentiels ou des*

---

justice dans des cas individuels, ***telles que l'anonymisation ou la pseudonymisation*** *de décisions judiciaires, de documents ou de données* ». Les enjeux ne sont pas les mêmes.

[653] Conseil d'État, 10ème / 9ème SSR, 26/05/2014, n° 354903, spéc. point n°9.

[654] Signalons notamment le Laboratoire d'innovation numérique de la CNIL.

[655] Avis 5/2014 sur les Techniques d'anonymisation 0829/14/FRWP216 préc., pages 12 et s.

[656] B. Nguyen, C. Castellucia, « Techniques d'anonymisation tabulaire : concepts et mise en œuvre », Bull. sté inform. Fr n°5, avril 2020, pp 23-41.

[657] Cabinet Randy Yaloz, « Conformité au RGPD : obligation de moyen ou de résultat », 19 sept. 2019, site https://elc-paris.com/conformite-au-rgpd-obligation-de-moyen-ou-de-resultat/

méthodologies générales aux fins de certification de la conformité à la présente loi ***de processus d'anonymisation*** *des données à caractère personnel* » (article 11, g.) [658].

Or, de cette activité de certification nationale, **le RGPD ne s'est pas fait le précurseur, ni l'écho** au plan européen. En principe, une activité de certification engage la responsabilité du certificateur. Mais quelle peut, aujourd'hui, être la durée de vie d'une certification utile, compte tenu des progrès technologiques exponentiels en calcul, en cryptologie, en agrégation de données, etc. ?

Ainsi, le Règlement 2022/868 sur la gouvernance des données a relevé qu'une donnée pouvait rester **hautement sensible, en dépit du processus d'anonymisation** censé la rendre « non personnelle » [659]. Le fait est d'ailleurs acté, par la proposition en 2022 de Règlement européen sur l'EEDS, que « ***même en cas*** *d'utilisation de techniques d'anonymisation de pointe, il* ***subsiste un risque résiduel que la capacité de réidentification soit ou devienne disponible****, au-delà des moyens raisonnablement susceptibles d'être utilisés* » [660]. De fait, le critère précité du « moyen raisonnable » a-t-il encore un sens, compte tenu des appétits des opérateurs doués des capitalisaitons et technologies nécessaires, pour des buts variés ?

En santé, l'exemple typique (non dominant) est celui des maladies rares dites « orphelines » [661]. Leur prévalence dans les pays membres, et même à l'échelle de l'Union [662], rend difficile que l'agrégation anonymisée des données avec une granulométrie utile pour l'exploitation, puisse préserver la vie privée des patients. En outre, dans ce cas, les techniques proposées pour réconcilier l'intérêt public et la protection de la vie privée, consistant en une dés-agrégation des données géographiques personnelles, apparaît d'intérêt limité [663].

---

[658] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
[659] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (Texte présentant de l'intérêt pour l'EEE) ; précédé de la Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données) COM/2020/767 final.
[660] Considérant n° 64 de la proposition de règlement.
[661] Orphanet (janvier 2021), Liste des maladies rares et de leurs synonymes classés par ordre alphabétique. Rapport disponible sur le site OrphaNet.
[662] COM(2008) 679 final « Les maladies rares: un défi pour l'Europe » (communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions). Ces maladies sont l'objet d'un règlement incitatif de la R&D de traitements à défaut délaissés par les industriels, règlement (CE) nº 141/2000 du Parlement européen et du Conseil, du 16 décembre 1999, concernant les médicaments orphelins.
[663] Boulos M., Kwan M.-P. El Emam K. Chung A., Richardson S. et D., « Reconciling public health common good and individual privacy : new methods and issues in geoprivacy », in Intern. Jl. Of Health Geographics vol. 21, Article number: 1 (2022), publié le 19 janvier 2022.

Enfin, dans le Règlement n° 2022/868 sur la gouvernance des données, ce risque résiduel général (bien au-delà des maladies orphelines, et pour des finalités très variées) est spécifiquement traité : son article 5§13 prévoit la possibilité d'actes législatifs spécifiques de l'Union, lorsque le « ***transfert vers des pays tiers peut*** *mettre en péril des objectifs de politique publique de l'Union, tels que la sécurité* ***et la santé publique, ou peut entraîner un risque de ré-identification de données anonymisées à caractère non personnel*** ». Il est frappant ici que le transfert puisse mettre en péril des objectifs « de santé publique », ce qui esquisse avec pudeur les **risques pour la souveraineté** d'une communauté politique.

Mais le critère d'application de l'article 5§13 est l'extranéité du traitement ; en outre, il postule qu'un traitement *intracommunautaire* se conformerait au droit applicable à tous Etats membres, à la fois au titre du droit commun gouvernant les données [664], et du droit dédié aux données de santé. Pour autant, il a été constaté en 2021 des écarts d'application du RGPD entre les Etats pourtant également obligés, rendant difficile une confiance en les utilisations secondaires [665] sans une évolution des textes et une mise en conformité.

3. La prévision dans le futur droit européen de situations tangentes

Dans la proposition européenne précitée, en mai 2022, de l'espace européen des données de santé, relevons l'article 44, qui a pour intitulé « *minimisation des données et limitation des finalités »*. Certes, les 44§1 et 44§2 exposent en matière d'utilisation secondaire légitime (cf. article 33 précité), l'obligation pour les organismes responsables de l'accès aux données, de restreindre cet accès « *uniquement aux données de santé électroniques pertinentes pour la finalité du traitement dont il est fait mention* », lesquelles **ne peuvent être que des données rendues anonymes, donc non personnelles**.

Mais dans le même, l'article 44§3 dispose que « ***Lorsque la finalité du traitement de l'utilisateur de données ne peut être atteinte à l'aide de données anonymisées*** *(…), les organismes responsables de l'accès aux données de santé donnent accès aux données de santé électroniques dans un format pseudonymisé* ». Or, ce §3 est frappant : il n'énonce pas

[664] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données

[665] Commission européenne, « Assessment of the EU Member States' rules on health data in the light of the GDPR », 2021.

une faculté (« peuvent »), mais dans le style européen, une obligation « *donnent accès* », ce qui met en exergue la question des finalités légitimes et de la proportionnalité des demandes.

En outre, le même 44§3 souligne in fine que, dans ce cas, « *Les utilisateurs de données* ***ne réidentifient pas les données de santé*** *électroniques qui leur sont fournies dans un format pseudonymisé* », ce qui serait une pratique sanctionnée.

Dans un champ d'application différent, celui du « *transfert de données électroniques à caractère non personnel dans un pays tiers* », l'article 61 dispose de façon emblématique au regard de notre démonstration précédente, que « *les* ***données électroniques à caractère non personnel*** *mises à disposition par les organismes responsables de l'accès aux données de santé, fondées sur les données électroniques* ***d'une personne physique*** *qui relèvent de l'une des catégories énumérées à l'article 33[, points a), e), f), i), j), k) et m),]* ***sont considérées comme hautement sensibles*** (…) », sous condition que l'on va voir.

Précisons d'abord que les catégories ici concernées de l'article 33 sont : le dossier médical électronique du patient (a) ; les « *données génétiques, génomiques et protéomiques humaines* » (e) ; « données de santé électroniques générées par la personne, dont *celles générées grâce aux dispositifs médicaux, aux applications de bien-être ou aux autres applications de santé numériques* » (f) ; « *données de santé électroniques contenues dans les registres médicaux concernant des maladies spécifiques* » (i) ; données de santé électroniques provenant d'essais cliniques (j) ; « *données de santé électroniques provenant de dispositifs médicaux et des registres des médicaments et des dispositifs médicaux* » (k) ; « *données de santé électroniques provenant de biobanques et de bases de données spécialisées* » (m).

Considérées comme **hautement sensibles, à quelle condition ? L'article 61 d'indiquer** « *à condition que leur transfert vers des pays tiers* ***présente un risque de réidentification par des moyens allant au- delà de ceux susceptibles d'être raisonnablement utilisés****, compte tenu du nombre limité de personnes physiques concernées par ces données, du fait qu'elles sont géographiquement dispersées ou* ***des évolutions technologiques attendues pour un avenir proche*** ». On notera dans le (f), la présence inattendue des « applications de bien-être ».

Ainsi ce projet d'article est éloquent, quant à la portée des protections par l'anonymisation. Il nous conduit à considérer **une autre catégorie de donnée, totalement absente** de la

proposition 2022 du règlement sur l'EEDS (n'aurait-elle pu / du y figurer ?) tout comme du droit français : la notion de « donnée synthétique ».

§2. L'AVENEMENT DE « DONNEES SYNTHETIQUES » DE SANTE ?

La notion de « donnée synthétique » prétend pour partie répondre à la question précédente. Cette notion est récente : par « donnée synthétique », on entend de prime abord une **donnée numérique de construction artificielle, par opposition à une donnée réelle** – mais nous allons voir que l'opposition n'est pas si claire. Son avènement serait porteur d'une « révolution » en santé, sur le plan conceptuel et applicatif, sachant qu'il existe depuis longtemps des données « synthétiques » pour des modélisations dans d'autres domaines [666].

La notion **n'a de véritable utilité que pour la simulation** [667]**, ou désormais pour l'entraînement (apprentissage / réapprentissage) d'algorithmes** d'intelligence artificielle dits d'apprentissage profond (*machine learning* ou *deep learning*) [668]. En France, ce dernier est entendu selon le vocabulaire officiel publié en 2018, d'un « *Processus par lequel un algorithme évalue et améliore ses performances sans l'intervention d'un programmeur, en répétant son exécution sur des jeux de données jusqu'à obtenir, de manière régulière, des résultats pertinents* » ; mais ce vocabulaire officiel de la République **ne définit pas (encore) la « donnée synthétique »** [669].

Or, ce processus d'apprentissage profond **requiert un volume considérable de données diversifiées, et en santé, un processus de supervision** par des professionnels de santé pour les qualifier (indiquer à la machine la signification des images par exemple) [670]. Cela soulève

---

[666] A. Demailly, « Health data: an introduction to the synthetic data revolution », (Exploratory research), Resolving Pharma, 19 juill. 2021.

[667] Par ex. en formation initiale ou continue des professionnels de santé, afin de diversifier les bases didactiques.

[668] V. le papier fondateur de Y. Le Cun, Y. Bengio, G. Hinton. « Deep learning » *Nature* 521 (2015), p. 436-444. Rapportons ici son résumé éclairant : « *Deep learning allows computational models that are composed of multiple processing layers to learn representations of data with multiple levels of abstraction. These methods have dramatically improved the state-of-the-art in speech recognition, visual object recognition, object detection and many other domains such as drug discovery and genomics. Deep learning discovers intricate structure in large data sets by using the backpropagation algorithm to indicate how a machine should change its internal parameters that are used to compute the representation in each layer from the representation in the previous layer. Deep convolutional nets have brought about breakthroughs in processing images, video, speech and audio, whereas recurrent nets have shone light on sequential data such as text and speech* ».

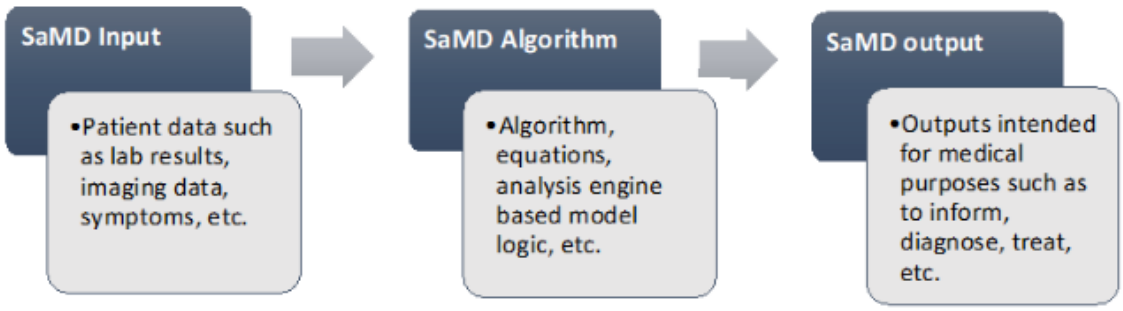
[669] Publié au JO sous couvert des « avis divers », sous l'égide de la Commission d'enrichissement de la langue française, sous le titre « Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptés) », JO 9 déc. 2018, NOR : CTNR1832601K.

[670] « *Apprentissage automatique dans lequel l'algorithme s'entraîne à une tâche déterminée* ***en utilisant un jeu de données assorties chacune d'une annotation indiquant le résultat attendu*** » (in Vocabulaire de l'intelligence artificielle, 2018 préc.)

la question de la confidentialité, représentativité, qualité, etc. de telles données nécessairement « réelles ». En 2021, l'usage en soins de l'IA par les professionnels de santé [671], a fait l'objet en France d'un régime d'autorisation (L. 4001-3 CSP) dont nous avons déjà discuté des termes, sous l'angle de l'accès du « *professionnel concerné* » aux données initiales du patient : cet accès semble viser la réassurance des opérateurs successifs (*infra*).

Il n'est pas lieu ici d'étudier en droit comparé l'environnement réglementaire du développement de « l'intelligence artificielle » en santé. Notons seulement que, si les synthèses comparatives mettent bien en exergue la question de l'accès aux données d'entraînement, elles sont encore peu dissertes, voire mutiques sur **les données « synthétiques » censées pouvoir y contribuer** [672]. Peut-être cela fait-il beaucoup de notions à convoquer, ce qui rend raisonnable de les aborder séparément [673] ? Mais on verra que même séparée, la question des « données synthétiques » y est encore peu traitée [674].

Figure 1. SaMD workflow



Source: Chhaya & Khambholja (adapted from original)

Or, la génération de telles données synthétiques en santé a suscité une attention considérable, car elle pourrait, **sans engager la confidentialité des données personnelles**, améliorer les IA existantes. C'est le cas rapporté dans des domaines déjà variés : imagerie [675], modélisation des

[671] Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique préc.
[672] Notamment aucune occurrence de la « donnée synthétique » dans l'étude internationale de V. Chhaya, K. Khambholja, « The SaMD regulatory landscape in the US and Europe, Regulatory Focus », RASP, 6 août 2021, https://www.raps.org/news-and-articles/news-articles/2021/8/the-samd-regulatory-landscape-in-the-us-and-eu-1
[673] Le sujet est en soi très complexe ; voir les prudences de la FDA, in « Proposed regulatory framework for modifications to artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD) », proposé à la discussion en avril 2019.
[674] Cela n'est pas une question de vocabulaire : nous y avons cherché tous les vocables équivalents (données synthétiques, données « virtuelles », données « artificielles », données « simulées », patient virtuel, et ces mêmes termes avec « échantillon » à la place de « données », etc.).
[675] A. Ghorbani, V. Natarajan, D. Coz & Y. Liu in *Proceedings of the Machine Learning for Health Neur IPS Workshop* (eds Dalca, A. V. et al.) 155–170 (PMLR, 2020) ; Y. Movshovitz-Attias, T. Kanade, Y. Sheikh, in *European Conference on Computer Vision* 202–217 (Springer, 2016) etc.

protéines[676], analyse comportementale [677] etc. alors que, de façon saisissante nous l'avons vu, une étude du cabinet Accenture aux Etats-Unis a rapporté en 2018 que 18% des employés sondés d'organisations de prestation ou de liquidation de paiement de soins, seraient **disposés à vendre des données de santé confidentielles à des parties non autorisées** [678].

Comme sa désignation le suggère, la donnée synthétique est au moins pour partie artificielle : c'est une construction numérique, qui peut combiner des éléments pertinents sans représenter une personne réellement existante : **toute tentative de re-identification est donc, *a priori,* vaine**. Ainsi, cette technique nouvelle est censée répondre à des problèmes de confidentialité et/ou à des besoins non couverts, en matière de traitement des données de santé (A).

Mais le caractère récent de la notion fait qu'elle n'est **pas en soi évoquée dans les *thésaurus* (supra), ni les textes et projets européens les plus récents, même dédiés à l'intelligence artificielle**. En l'état, elle ne dispose donc d'aucun statut, ni même de définition par des normes, ou (à la date de rédaction de notre thèse) par des doctrines administratives de régulateurs. Mais le CEPD vienne d'intégrer la notion dans son champ de veille (B).

A. LA GENESE CONCEPTUELLE DES « DONNEES SYNTHETIQUES » DE SANTE

En santé notamment, les données sont souvent considérées comme le « pétrole du XXIème siècle ». Mais nous avons vu que leur **utilisation secondaire était contraint par la nécessaire protection des personnes**, et leur disponibilité et granulométrie parfois non suffisantes, après anonymisation. Cela justifie aussi la massification des données, tout comme la surveillance des bases, et explique certains atouts du système français en la matière (*supra*).

En tous cas, l'utilisation secondaire conduit souvent à subdiviser la notion de donnée, **par déconstruction numérique selon le degré de protection souhaitable**, en lui retirant des éléments dont la combinaison seule serait identifiante. Or, la valeur des données en santé tient à leur finesse granulométrique et à leur réalité, ou réalisme.

---

[676] C. Wan, D.T. Jones, « Protein function prediction is improved by creating synthetic feature samples with generative adversarial networks. *Nat Mach Intell* **2**, 540–550 (2020) etc.
[677] L.A. Bolaños, D. Xiao, NL. Ford *et al.* « A three-dimensional virtual mouse generates synthetic training data for behavioral analysis », *Nat Methods* **18**, 378–381 (2021).
[678] Accenture, « Losing the Cyber Culture War in Healthcare: Accenture 2018 Healthcare Workforce Survey on Cybersecurity », https://www.slideshare.net/secret/2bnzxgIzzSTxD4 (contrôlé nov. 2022).

Dès lors, une protection forte par les procédés d'anonymisation classiques obère la valeur des données finalement utilisées. D'autre part, elle ne pallie pas leur manque de représentativité selon les patients dont elles émanent, quelles que soient les sources organiques (professionnels, établissements et technologies de santé, *supra*) qui les fournissent. Cela fait que la **(re)création numérique sans risque de données, avec une granulométrie pertinente, est un défi technologique, mais aussi donc juridique.** Il nous conduit à relever les motifs de génération de « données synthétiques » (1), avant leur génération même (2).

1. Les motifs de la génération de « données synthétiques »

Les données « synthétiques » sont des créations numériques artificielles par des algorithmes dits « génératifs », et utilisées hors santé depuis les années 1990 [679] notamment, pour disposer de populations synthétiques afin de tester des modèles pour l'aide à la décision publique [680].

A la différence d'un algorithme de calcul ou décisionnel, un algorithme « génératif » **a pour but la création plus ou moins *ex nihilo* d'entités** (sons, images, combinaisons de chiffres) **pouvant imiter de façon réaliste des attributs d'entités existantes,** attributs qu'elle peut éventuellement leur emprunter et mixer [681], et doit en santé être supervisé (*supra*). Nous esquissons ici le contexte de leur apparition (a) et le moteur de leur développement (b).

a. La justification des « données synthétiques » en santé

La performance des algorithmes dits « d'intelligence artificielle » ou « augmentée » dépend largement en santé, comme dans tout autre domaine, **des données qui auront permis leur apprentissage**, dont ils auront en quelque sorte été nourris. En l'état, leur développement repose donc sur la disponibilité massive et la conservation de données médicales, auxquelles peut (devrait) **être associée une garantie de pertinence** – c'est-à-dire une annotation par des opérateurs humains qualifiés et reconnus pour leur compétence permettant de les caractériser (on parle alors donc d'apprentissage « supervisé », à la différence de l'« automatique ») [682].

---

[679] La première application sociale civile connue est celle par les services du recensement fédéral aux Etats-Unis, pour des applications variées de modélisation, du fait de la faiblesse de certains échantillons de données « réelles », US Census Bureau, « What are synthetic data ? » (27 mai 2021), https://www.census.gov.

[680] J. Hradec, M. Craglia, M. Di Leo, S. De Nigris, N. Ostlaender, N. Nicholson « Multipurpose synthetic population for policy applications », EUR 31116 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-53478-5 (online), doi:10.2760/50072 (online), JRC128595, 2022 ; T. E. Raghunathan, Synthetic data, Annual Review of Statistics and Its Application, 8, 129-140, 2021.

[681] Il en résulte de forts enjeux de propriété intellectuelle, qui échappent à notre sujet.

[682] Pour une esquisse de l'opération de référencement des superviseurs et ses applications contractuelles, « Intelligence artificielle en santé et responsabilité civile : quelques interactions entre catégories », in *Cadre légal des projets d'e-santé*, Editions législatives, 2019, 140-145.

Or, les algorithmes sont ainsi entraînés par des données nécessairement limitées (leur massification pour exploitation transverse est un des enjeux nous l'avons vu, de la constitution de la plateforme des données de santé en France). Les données réelles annotées peuvent être affectées d'une **insuffisante diversité de cas, et d'un biais de sélection**. Il en résulte une **réduction de la performance de l'algorithme**, s'il est appliqué dans un contexte différent de celui des données d'entraînement quant aux populations traitées, à la stratification des risques, aux contextes de soins, aux résultats cliniques [683]. Cela exactement comme un praticien de santé, mais **avec pour particularité que l'algorithme ne doute pas**.

D'autres types de biais peuvent résulter de déséquilibres dans la représentation de certaines affections (nous avons vu le défi posé par les maladies rares sur l'anonymisation). Ils peuvent dégrader les performances d'algorithmes qui auront été entraînés à des fins de diagnostic et de pronostic. A cela peut être ajouté que de tels outils, s'ils sont entraînés par des données historiques (avant l'apparition de maladies présentant une symptomatologie inédite, etc.), ne seraient pas toujours à même de détecter de **nouveaux phénotypes**, définis comme la « *totalité des traits observables caractérisant un être vivant donné* » : ainsi chez des patients qui ont pu être victimes d'un AVC ou de cancers présentant des symptômes de la Covid19 [684].

En conséquence, l'entraînement d'algorithmes à finalité diagnostique / pronostique **nécessite de grands ensembles de données qui soient à la fois diversifiés quant aux phénotypes, mais aussi représentatifs de l'hétérogénéité** liée au sexe, la race, les conditions sociales, la géographie – tout comme de l'hétérogénéité quant aux parcours de soins, c'est à dire des flux de travail et des technologies qui ont pu être utilisées en biométrie, imagerie, biologie etc [685].

Ainsi, le but de la génération des données synthétiques est de **pallier la rareté / la faible représentativité des données médicales issues de pratique réelle et fournies annotées** [686], afin d'une richesse et performance supérieures des systèmes dans le but de la réduction des risques [687], de l'ouverture du champ de la recherche scientifique [688], et bien sûr et en premier

[683] Voir la synthèse de M. Pencina, B. Goldstein, R. D'Agostino : « Prediction Models - Development, Evaluation, and Clinical Application », New Engl. Jl of medecine, N Engl J Med 2020 (23 avril).
[684] T. Oxley, J. Mocco, S. Majidi et 13 autres co-auteurs, « Large-Vessel Stroke as a Presenting Feature of Covid-19 in the Young », N Engl J Med 2020; 382:e60 (28 avril 2020).
[685] A. Trister, « The Tipping Point for Deep Learning in Oncology » JAMA Oncol. 2019;5(10):1429-1430.
[686] A. Tucker, Z. Wang, Y. Rotalinti *et al.* Generating high-fidelity synthetic patient data for assessing machine learning healthcare software. *npj Digit. Med.* (2020) **3**, 147 (9 novembre 2020).
[687] En 2023, S. Davis, H. Ssemaganda, J. Koola *et al.* « Simulating complex patient populations with hierarchical learning effects to support methods development for post-market surveillance ». *BMC Med Res Methodol* (2023)

lieu de la robustesse des analyses automatisées, quelles qu'en soient les finalités. Elle vise aussi à faciliter l'interopérabilité dans le partage de données « de santé » précises, mais qui ne sont plus personnelles, donc cessent d'être confidentielles, et deviennent cessibles [689].

b. La génération de « données synthétiques » en santé

Nous serons bref : le but ici n'est que de donner quelques éclairages techniques pour comprendre la suite sur le terrain juridique, et la question dépasse de très loin notre compétence. Comme nous venons de le voir, les données synthétiques visent à imiter les données d'observations du monde réel. Elles sont **générées par un artifice maîtrisé de déconstruction / reconstruction**, ce dont le schéma didactique rend bien compte [690].

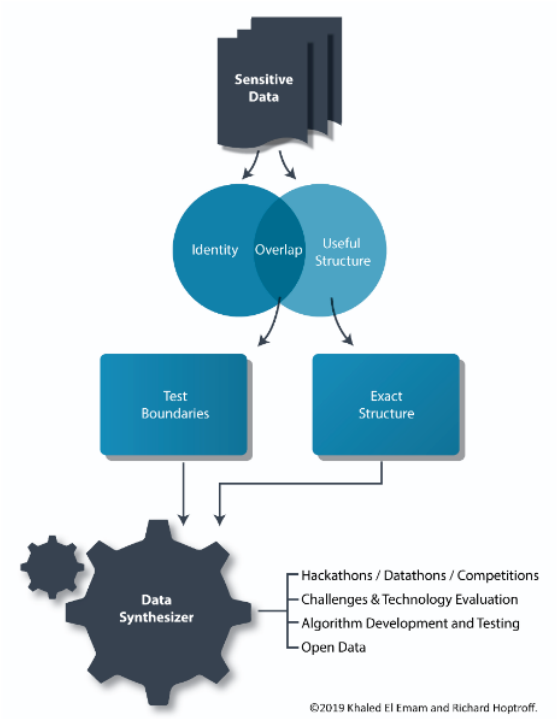


Figure 1 – The tradeoffs in the process of generating synthetic data.

23, 89 ; A. Chen, D. Chen, « Simulation of a machine learning enabled learning health system for risk prediction using synthetic patient data ». *Sci Rep* **12**, 17917 (2022) ;

[688] A. Smith, P. Lambert, MJ Rutherford, « Generating high-fidelity synthetic time-to-event datasets to improve data transparency and accessibility ». *BMC Med Res Methodol* **22**, 176 (2022).

[689] K. Elkam, R. Hoptroff « The Synthetic Data Paradigm for Using and Sharing Data » Executive Update (Cutter Consortium), Data Analytics & Digital Technologies Executive Update Vol. 19, n°6 2019, pp 1-10.

[690] K. Elkam, R. Hoptroff préc., page 4.

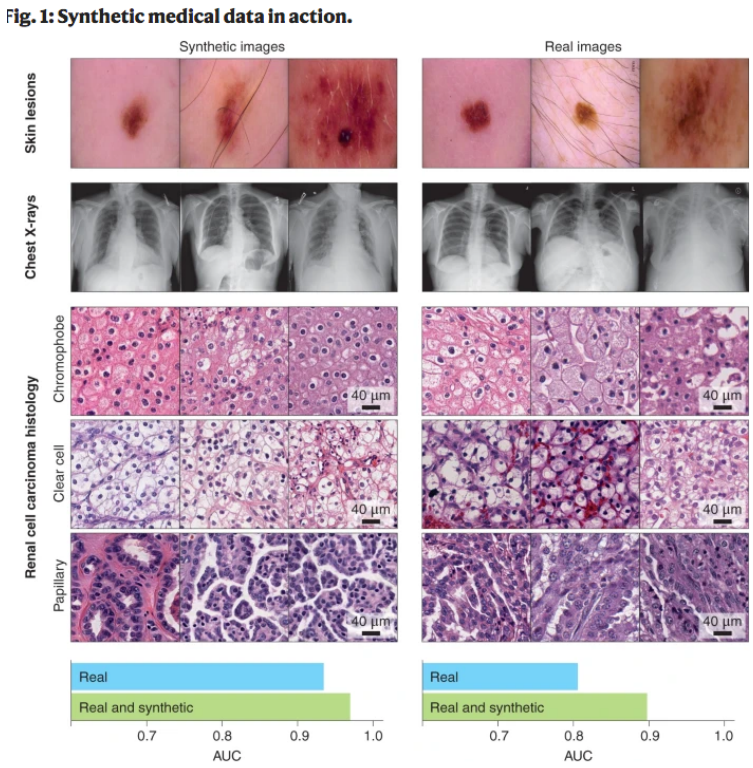
En effet, les systèmes informatiques dits d'« intelligence artificielle » par apprentissage profond ne se limitent pas au classement des images ou au traitement du langage. Certains algorithmes sont spécialisés et connus sous le nom de « *modèles génératifs profonds* » : ils **peuvent imiter la façon dont les données sont générées dans le monde réel**. Encore doit-on parmi les données synthétiques issues des modèles génératifs, distinguer les données synthétiques issues de simulation sur « modèles avancés », lesquels sont créés à partir de normes comme des références cliniques existantes ou des connaissances médicales validées.

Dans ce contexte, ces systèmes recourent à des réseaux antagonistes génératifs (Generative Adverserial Networks, GAN) qui sont *« un type de modèle génératif qui apprend les distributions de probabilité de la manière dont les données de grande dimension sont susceptibles d'être distribuées ».* Ces **réseaux antagonistes génératifs** sont composés de deux réseaux de neurones, l'un appelé « générateur », l'autre « discriminateur ». **Les deux réseaux s'affrontent, l'un tentant de leurrer l'autre**. L'exemple habituel de cet affrontement est donné pour la détection par le « discriminateur », de contrefaçons de peintures de Monet, qui entraîne le réseau « générateur » ainsi sanctionné [691].

Mais il s'agit là d'imitation en champ de créativité artistique, avec des conséquences pratiques limitées. En contraste, en santé, nous avons vu que les « modèles avancés » **devaient intégrer des références validées** *ex ante* (données annotées par un professionnel de santé, pour un

[691] Un GAN est formé pour produire des peintures dans le style de Monet, avec un réseau « générateur » qui vise à le contrefaire, et un réseau « discriminateur » qui tente de distinguer les contrefaçons. Au gré du jeu, le « générateur » apprend des mauvaises contrefaçons repérées par le « discriminateur » : cela lui permet de créer des contrefaçons toujours plus réalistes. R. Gonsalves, « GANscapes: Using AI to Create New Impressionist Paintings » Towards Data Science, avril 2021 ; D. Foster, « Generative deep learning: teaching machines to paint, write, compose, and play », O'Reilly Media, 2019.

apprentissage profond non moins « supervisé »). Il en résulte notamment dans le champ de l'imagerie, des **données synthétiques particulièrement réalistes**, y compris dans la représentation d'aberrations infimes (le but de l'entraînement du système étant aussi de distinguer les signaux faibles reflétant, ou annonçant des développements pathologiques) [692] :



Ainsi grâce au jeu émulation des GAN dans les modèles avancés, des « données synthétiques » imitant les phénotypes d'états physiopathologiques et de populations sous-représentés peuvent être créées à partir de « perturbations », à l'aide de modèles avancés précis [693], simulations physiques etc. Les hypothèses générées (dans le champ « *overlap* » du schéma précité) seront testées, avant d'être incorporées dans les bases de données servant à l'entraînement des algorithmes d'IA. Le but est de prendre de meilleurs décisions médicales, **au regard d'hypothèses diversifiées de façon artificielle mais fiable**, et dépersonnalisées.

En 2022, une étude suggère qu'en l'absence de données cliniques réelles (protégées par la loi), il est possible à l'aide d'un nouveau GAN de **produire massivement des collections de données synthétiques hautement réalistes** pour un but en l'occurrence spécifique : l'accès libre pour concevoir, évaluer et comparer des algorithmes d'apprentissage automatique. Les

[692] R.J. Chen, M.Y Lu, T.Y. Chen *et al.* « Synthetic data in machine learning for medicine and healthcare » préc.
[693] Modèles qui simulent des résultats en fonction d'entrées spécifiques.

auteurs estiment très bas le risque de dévoilement d'information confidentielle [694]. Mais il peut aussi en résulter la production massive de données non fiables pour l'usage visé.

2. Les défis lancés par les « données synthétiques » en santé

Le recours à ces données est notamment motivé par le fait qu'il pourrait évacuer les problèmes de confidentialité des données personnelles de santé, permettrait de développer les ensembles de données « fournies » à l'IA, et **favoriser leur partage entre opérateurs pour optimiser l'entraînement / recherche et réduire les coûts**, sachant ces données cessibles. Or, cela suppose que les ensembles de telles données capturent la distribution originale des données réelles avec précision, afin de pouvoir être utilisées utilement en substitut / complément [695] ; ce qui soulève les questions de leur qualité (a) et vulnérabilité (b).

a. Le défi de la qualité des données synthétiques

Parmi les logiciels relevant de la qualification de « dispositif médical » (*supra*), les systèmes auto-apprenants (*machine-learning*) lancent un défi particulier à la régulation, jusqu'alors dominée par la certification de modèles statiques [696]. Selon l'article 6§ 1 de la proposition de règlement de 2021 établissant des règles harmonisées concernant l'intelligence artificielle [697], les dispositifs médicaux embarquant un système d'IA sont considérés « à haut risque ». Si cette proposition européenne était adoptée sans modification, ces systèmes seraient soumis à une certification de conformité à inventer *ex nihilo* (la FDA américaine est en la matière très dynamique [698]), qui s'ajouterait aux règles *ad hoc* adoptées en 2021 dans le CSP [699].

Ce **cadre posé au plan national, et encore en gestation au plan européen, n'a pas retardé l'expression la réflexion** de la Haute Autorité de Santé (HAS) en France quant aux conditions éligibilité au remboursement ; cette réflexion découle d'un remarquable travail

---

[694] N. Kuo, M. Polizzotto, S. Finfer *et al.* « The Health Gym: synthetic health-related datasets for the development of reinforcement learning algorithms ». *Sci Data* **9**, 693 (2022). Les données proposés sont celles de patients présentant une hypotension aigue ; une septicémie dans des unités de réanimation ; ou HIV+ recevant un traitement antirétroviral.

[695] R.J. Chen, M.Y Lu, T.Y. Chen *et al.* « Synthetic data in machine learning for medicine and healthcare », *Nat Biomed Eng* **5**, 493–497 (2021).

[696] Univers de logiciels fermés, non évolutifs au sens d'évolutivité endogène, progressant par versions successives, bien identifiées et successivement certifiées.

[697] Comm. eur., 21 avr. 2021, COM(2021) 206 finals, qui renvoie à l'annexe II, laquelle vise en sa section A le règlement (UE) 2017/745 du 5 avril 2017 relatif aux dispositifs médicaux.

[698] Voir l'approche déjà de la FDA, « FDA Releases Artificial Intelligence/Machine Learning Action Plan » (12 janv. 2021), « Artificial Intelligence and Machine Learning in Software as a Medical Device » (22 sept. 2021), « Good Machine Learning Practice for Medical Device Development: Guiding Principles » (27 oct. 2021).

[699] C. Chrichton, « L'intelligence artificielle dans la révision de la loi bioéthique », Dalloz Actu.,16 sept. 2021.

initié en 2020 et publié en 2022 (CNEDIMTS) [700], qui permet d'illustrer déjà une partie du propos, en attendant une concrétisation européenne voire un complément national (*infra*).

En effet, à la différence des dispositifs médicaux classiques, les IA ont vocation à s'adapter aux flux de données dans le temps. A défaut de disposer d'une « masse » de données de santé réelles [701], leurs concepteurs peuvent être amenés on l'a vu à **utiliser des données synthétiques comme palliatif pour entraîner et affiner les algorithmes**. Cela peut poser problème lorsqu'il n'existe pas de mesures de qualité clinique et des paramètres d'évaluation.

Dans son annexe 6 de conseils pour la préparation de dossiers de candidature au remboursement de dispositifs d'IA (2022), la HAS présente en ce sens un sous-tableau très éclairant [702]. Titré « *Description des échantillons utilisés pour l'apprentissage initial ou le réapprentissage du modèle* », il précède un sous-tableau titré « *Description des données d'entrée impliquées dans la décision (une fois le dispositif médical déployé)* ». Si le second intègre des données du patient bénéficiaire du système, tel n'est pas le cas du premier, que nous reproduisons ici [703]. Nous y soulignons (en gras) dans la colonne de droite, les éléments **impliquant potentiellement des données synthétiques** :

Données		
Description des échantillons utilisés pour l'apprentissage initial ou le réapprentissage du modèle		
5	Préciser les caractéristiques de la population dont les données d'apprentissage initial ou de réapprentissage du modèle sont extraites	Celles-ci peuvent être : Démographiques (tranches d'âges, sexe...) Physiopathologiques (grossesse, personnes diabétiques ou asthmatiques, etc.) ou morphologiques (personnes amputées du membre inférieur, etc.)Cliniques ou biologiques (stade de la maladie, etc.). **Distinguer la population à partir de laquelle les données d'apprentissage initial sont produites** (entrainement, validation et test) de **celle utilisée lors de la phase de réapprentissage** (réentrainement, validation et test du système mis à jour), **le cas échéant**.
6	Préciser les caractéristiques de chaque échantillon utilisé pour l'apprentissage initial ou le réapprentissage du modèle	Sont attendues : leur fonction, leur taille et leur composition. Les variables incluses doivent être citées. **La manière dont sont pris en compte les événements rares doit être décrite.** Distinguer les bases de données des phases

[700] HAS, Annexe 6. Informations descriptives spécifiques à fournir pour les fonctionnalités du dispositif médical s'appuyant sur des procédés d'apprentissage automatique (technologies relevant du champ de l'intelligence artificielle), intégré au guide de dépôt en sept. 2020.
[701] Expression de données massives a été critique, voir B. Bévière-Boyer, « Numérique en santé : le projet de loi relatif à la bioéthique a accouché d'une souris », in N. Nevejans (dir.), Données et technologies juridiques, Mare & Martin, 2021, spéc. p. 245 et 246.
[702] *Comp*. FDA « Good Machine Learning Practice for Medical Device Development (…) » préc. oct. 2021.
[703] Grille descriptive, Annexe 6. Informations descriptives spécifiques à fournir pour les fonctionnalités du dispositif médical s'appuyant sur des procédés d'apprentissage automatique (technologies relevant du champ de l'intelligence artificielle), in LPPR : Dépôt d'un dossier auprès de la Commission nationale d'évaluation des dispositifs médicaux et des technologies de santé (janvier 2022).

		d'apprentissage initial (entrainement, validation et test) et en phase de réapprentissage (réentrainement, validation et test du système mis à jour), le cas échéant
7	Préciser la méthodologie de séparation ou de segmentation des échantillons	Par exemple, préciser les modalités de séparation (méthodes utilisées et proportions) et de segmentation (aléatoire, par date, par individu, etc.) des jeux de données d'entrainement, de validation et de test. Distinguer les bases de données en phases d'apprentissage et de réapprentissage, le cas échéant.
8	Préciser les caractéristiques des variables (type de variable, distribution...)	Distinguer les corpus d'entrainement, de validation et de test le cas échéant.
9	Indiquer le mode d'acquisition des variables et leur origine lors du processus d'apprentissage	Par exemple, une variable a-t-elle été saisie par un patient ? Provient-elle d'un capteur ? **A-t-elle été générée à partir de modèles de patients virtuels ? Préciser si les variables ont été extraites de corpus de données ouverts ou achetés et indiquer lesquels, le cas échéant, ainsi que leur caractère pérenne ou non**. Préciser les types de capteurs utilisés lors de l'acquisition des variables, le cas échéant
10	Décrire les prétraitements appliqués aux données	Par exemple, les actions de nettoyage des données, de transformation, de réduction, d'augmentation (**ajouts de bruits artificiels, de perturbations artificielles simulant des variations météorologiques ou des défauts capteurs, etc.) Préciser les données concernées et la proportion des données modifiées par ces prétraitements**
11	Indiquer la proportion des données manquantes au sein des données brutes et décrire leur gestion.	Préciser les types de données manquantes (aléatoires ou prévisibles)
12	Expliquer les procédures mises en place pour détecter et gérer les données aberrantes, le cas échéant	En particulier, préciser la manière dont sont distinguées les données aberrantes (ex : données physiologiquement impossibles) des valeurs atypiques (ex : événements rares)
13	Justifier de la représentativité des échantillons utilisés pour l'apprentissage initial (entrainement, validation et test) de l'algorithme par rapport aux données auxquelles cet algorithme sera exposé une fois déployé	Une justification des critères de représentativité est attendue. **Préciser notamment les outils et méthodes utilisés pour vérifier la représentativité des échantillons** et détecter les biais potentiels. En cas d'apprentissage incrémental ou continu, indiquer l'impact potentiel des mises à jour sur l'ensemble des données d'apprentissage.
Description des données d'entrée impliquées dans la décision (une fois le dispositif médical déployé)		
14	Etc	Etc

Dans un cadre réglementaire proposé en 2019 par la FDA pour les modifications logicielles dans les AI-SaMD basés sur l'apprentissage automatisé, il est préconisé de rendre obligatoires **les normes de référence et l'assurance qualité de toute nouvelle source de données** dans la mise à jour des algorithmes [704]. Dans son guide de bonnes pratiques en 2021, l'approche est en revanche lapidaire et ne cite pas spécifiquement les données synthétiques ; il y est mis en exergue le **besoin d'assurer « l'authenticité et l'intégrité des données** » [705]. Cette question

[704] FDA, préc. « Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback » (FDA, 2019).

[705] FDA préc., *Guiding Principles*, n°2 (version 2021).

est en cours de réflexion approfondie, notamment par des exercices comparatifs [706]. Mais comment une donnée « synthétique » peut-elle être « authentique » ?

Plaçons nous sur le terrain de l'application, non de la génération, pour ici entendre la notion « d'authenticité ». Il est en effet difficile de savoir si les données synthétiques imitent le bon phénotype. Les métriques quantitatives actuelles pour l'évaluation des modèles génératifs utilisent des scores de probabilité, de vraisemblance et de divergence. De tels scores ne sont **pas faciles à interpréter par les cliniciens,** ni ne reflètent les modes de défaillance spécifiques dans la génération de données synthétiques [707].

Enfin (notre survol ne prétend pas épuiser le sujet), les modèles génératifs restent limités par le volume et la qualité des données d'entraînement pour modéliser la distribution des données ; **ceux entraînés avec des ensembles biaisés seraient toujours eux mêmes biaisés** vers des états physio/pathologiques sur-représentés ; et pour les maladies / manifestations rares, il faut disposer d'échantillons suffisants **pour établir des normes de référence clinique**, ce qui est un problème aigu [708] ; il vaut par définition en matière de données réelles, avant de valoir en matière de données synthétiques qui en dériveraient (il faudrait alors s'assurer de la pertinence de la « perturbation » créée, sachant que l'IA ne doute pas).

b. Le défi de la vulnérabilité des données synthétiques

Il n'est pas lieu ici non plus, de prétendre épuiser le sujet. On relèvera plus brièvement qu'un des problèmes peut être la **fuite d'informations confidentielles lors de la conception** des modèles, puisque des données réelles sont requises. Cela justifie en France la première délibération de la CNIL en 2022 sur le sujet de la génération de « données synthétiques » à partir des bases de données du SNDS protégées par la LIL de 1978 (*infra*), **quand bien même il n'en existe aucune définition, même doctrinale,** à la date de notre rédaction. On a déjà

---

[706] M. Lenatti, A. Paglialonga, V. Orani et al. « Characterization of Synthetic Health Data Using Rule-Based Artificial Intelligence Models ». IEEE J Biomed Health Inform. 2023 Jan 13;PP. doi: 10.1109/JBHI.2023.3236722 ; A. Gonzales, G. Guruswamy, S.R. Smith, « Synthetic data in health care: A narrative review », A narrative review. PLOS Digit Health. 2023 Jan 6;2(1):e0000082. doi: 10.1371/journal.pdig.0000082 ; N. Kuo, M.N. Polizzotto, S. Finfer, *et al.* The Health Gym: synthetic health-related datasets for the development of reinforcement learning algorithms. *Sci Data* 9, 693 (2022) ; R.J. Chen, M.Y. Lu, T.Y. Chen *et al.* Synthetic data in machine learning for medicine and healthcare. *Nat Biomed Eng* 5, 493–497 (2021).

[707] Voir les très nombreuses contributions dans les actes de « Advances in Neural Information Processing Systems 29 » (30th Annual Conference on Neural Information Processing Systems 2016), https://www.proceedings.com/content/034/034099webtoc.pdf. (il s'agit de la table des matières exposant les contributions, non de l'ouvrage entier : plus de 5100 pages).

[708] Préc. « Synthetic data in machine learning for medicine and healthcare. *Nat Biomed Eng* **5**, 493–497 (2021).

signalé que les données de santé requises à cette fin entre autres, étaient susceptibles de vente illicite. L'étude de 2018 par Accenture du potentiel de compromission volontaire de données de santé par certains acteurs mêmes de systèmes de soins, étai à cet égard saisissante [709].

Sécurité, à quel point ? [710] A supposer les données synthétiques produites sans compromission des données réelles, la sécurité des données personnelles peut notamment être **engagée par les attaques par inférence d'appartenance** (*membership inference attack* [711]). Ce concept désigne des procédés d'acquisition illicite de connaissances sur les données réelles utilisées pour la production du modèle d'IA, qui consistent « *à déterminer si des données relatives à un individu ont été utilisées lors de la phase d'entraînement (…). Cette connaissance peut permettre à l'attaquant de* ***déduire des informations concernant une personne »*** [712], lorsque des échantillons de l'ensemble de données d'entraînement peuvent être reconstituées à partir de la distribution de probabilité. Or, ce risque en matière de données « anonymisées » [713] a aussi été identifié en 2022 dans le domaine des « données synthétiques » de santé [714].

D'autres applications de l'IA existent ; elles sont désignées sous le vocable de falsification sophistiquée (« *deep fake* »), laquelle consiste en **l'usage frauduleux du processus précité : la simulation vise alors un but illicite**. Si l'usurpation d'identité d'une personne peut notamment, ici, viser à compromettre des données personnelles (par exemple par par faux messages, par accès au dossier du patient, pour captation ou dénaturation de données) [715], d'autres usages peuvent selon les contextes, viser aussi à frauder à l'éligibilité au remboursement, surfacturer des soins factices, etc. Mais cela relève d'un autre sujet [716].

---

[709] Accenture, « Losing the Cyber Culture War in Healthcare: Accenture 2018 Healthcare Workforce Survey on Cybersecurity », https://www.slideshare.net/secret/2bnzxgIzzSTxD4 (contrôlé nov. 2022).
[710] T. Stadler, B. Oprisanu, C. Troncoso, Synthetic Data - A Privacy Mirage. arXiv preprint, 2020 - arXiv:2011.07018
[711] A.A. Poltavtsev, A.R. Khabarov, A.O. Selyankin, « Inference Attacks and Information Security in Databases », *Aut. Control Comp. Sci.* 54, 829–833 (2020). https://doi.org/10.3103/S0146411620080271
[712] CNIL, Attaque par inférence d'appartenance (membership inference attack) (définition sur le site CNIL).
[713] I.E. Olatunji, J. Rauch, M. Katzensteiner, M. Khosla « A Review of Anonymization for Healthcare Data ». Big Data. 2022 Mar 10. doi: 10.1089/big.2021.0169.
[714] Z. Zhang, C. Yan, B. Malin, « Membership inference attacks against synthetic health data » Jl Biomed. Inform. January 2022, 103977.
[715] Voir les études de compromission de dossiers de patients aux Etats-Unis in HIPAA Journal, Healthcare Data Breach Report, June 2021 (21 juillet 2021), et June 2022 (20 juillet 2022).
[716] S. Finlayson, J.D. Bowers, J. Ito, J. Zittrain et al, « Adversarial attacks on medical machine learning - Emerging vulnerabilities demand new conversations » Science, 22 mars 2019, vol. 363 issue 6433,1287-1289.

B. ABSENCE DE STATUT JURIDIQUE DE LA « DONNEE DE SANTE SYNTHETIQUE »

Pour quoi faire, un statut juridique, s'il ne s'agit pas d'une donnée « personnelle » ? Par sa nature, elle échappe aux dispositions de l'article L. 1111-8 CSP, selon lequel « VII.-*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 prévues à l'article 226-21 du code pénal* ». Or, elle devient ainsi **potentiellement un objet de commerce rémunérateur, et désinhibé.**

Pourraient-elles donc faire l'objet d'une production/ d'un commerce non régulé ? Nous ne sommes pas ici dans le champ de la création artistique ; les applications de données synthétiques pour de l'apprentissage d'IA ou de la simulation / imitation fine sont critiques.

Cette hypothèse n'est pas de science fiction : en 2022, des auteurs anticipent **la production et vente domestique et transfrontière de fausses données (constructions synthétiques fiables, ou viciées)** [717]. Cela permet d'inverser la formule « *fake it till you make it* », laquelle devient « *make it till you fake it* » [718], pour des applications très rémunératrices, voire très pertubatrices des systèmes selon la qualité et le dessein.

Or, il n'existe pas de méthode robuste permettant d'établir le caractère artificiel d'une « donnée synthétique » (à moins d'un marquage convenu, voire normalisé, que n'adopteront *a priori* pas les acteurs illicites, à moins de vendre de la donnée synthétique frelatée [719]) : elle aura précisément été produite en GAN par un réseau « générateur », puis été qualifiée **précisément en survivant à la détection par le réseau « discriminateur »**.

Dès lors, la protection des personnes **dépend du risque de ré-identification des données, mais aussi de pollution des systèmes décisionnels ou d'aide à la décision** ; la sécurité et la souveraineté dépendent de leur intégrité structurale, mais aussi fonctionnelle face à d'une part la prédiction, voire à l'induction d'états individuels et populationnels ; d'autre part la menace cyber visant la pollution, le rançonnement ou la destruction (*partie II*). Esquissons la place de

[717] A(nmol). Arora, A(nanya). Arora « Synthetic patient data in health care : a widening legal loophole », The Lancet, 2022 Apr 23;399(10335):1601-1602. Doi:10.1016/S0140-6736(22)00232-X
[718] K. Dankar, I. Mahmoud. « Fake it till you make it: guidelines for effective synthetic data generation », Applied Sciences 11.5 (2021): 2158, 2021.
[719] Tout dépend du développement du marché de la donnée de santé reconnue comme synthétique, *infra*.

la donnée synthétique en droit (1), puis dans la doctrine du contrôleur européen de la protection des données (2).

1. Quelle place pour la « donnée synthétique » en droit ?

A la date de la rédaction de notre thèse, la notion de « *donnée synthétique* » n'a pas de conceptualisation juridique générale [720] – *a fortiori* en santé. **Elle est trop liée à l'intelligence artificielle pour disposer encore d'un statut autonome**, c'est à dire avant que l'IA soit elle-même encadrée, ce qui est en cours [721]. Or la loi de 2021 qui soulève beaucoup de questions, ne porte pas sur la question des entraînements (apprentissage initial et réapprentissage) [722] ; elle subordonne toutefois l'usage de l'IA par les professionnels de santé, à un arrêté après les avis de la CNIL et de la HAS, avis dont on a relevé la complémentarité.

Aucun des éléments précités quant aux données synthétiques **n'est encore entré dans le débat normatif français, ni européen.** Si la faisabilité de la génération de données synthétiques en santé est étudiée en France depuis 2022 **(a), l**a question n'apparaît pas dans les propositions en 2021 et 2022 des règlements européens sur l'IA et l'EEDS **(b).**

a. Absence de conceptualisation juridique en droit français

Nous avons relevé la qualité de la réflexion de la Haute Autorité de Santé, publiée en 2022, quant aux grilles devant éclairer les candidats IA à l'entrée sur le marché remboursable [723]. Elle fait référence à la notion de « *modèles de patients virtuels* » ; **cela ne correspond à aucune catégorie du CSP** ; en outre, cela va au-delà des données synthétiques, puisqu'il s'agirait ici de mimer un organe, voire un patient complet [724]. Mais si la notion de données

[720] On a vu la notion absence du vocabulaire officiel de l'intelligence artificielle publié au J.O. en 2018.
[721] Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique..
[722] L'article L. 4001-3-I CSP dispose que l'apprentissage « a été réalisé », non « est réalisé », ce qui semble exclure l'entraînement continu.
[723] Voir l'annexe 6 préc., titrée « Informations descriptives spécifiques à fournir pour les fonctionnalités du dispositif médical s'appuyant sur des procédés d'apprentissage automatique (technologies relevant du champ de l'intelligence artificielle) ».
[724] D.A. Cook, M. Triola, « *Virtual patients: a critical literature review and proposed next steps* », *Medical Education*, vol. 43, nº 4, 2009, p. 303–311 ; récemment, A. Kononowicz, L.A. Woodham, S. Edelbring, Stathakarou N, Davies D, Saxena N, Tudor Car L, Carlstedt-Duke J, Car J, Zary N. Virtual Patient Simulations in Health Professions Education: Systematic Review and Meta-Analysis by the Digital Health Education Collaboration. J Med Internet Res. 2019 Jul 2;21(7):e14676.

synthétique n'est pas citée, elle y est présente en filigrane : l'IA n'est pas entraînée sur un patient virtuel (qui mimerait les réactions d'un « vrai » patient), mais par des sets de données.

Sur le site Légifrance, notre recherche ne fait apparaître à la date de notre rédaction qu'une occurrence pertinente (citation formelle), quant à la génération de « *données synthétiques* », et cela précisément en santé : il s'agit d'une décision rendue en 2022, par laquelle la CNIL autorise une entreprise à mettre en œuvre en France un traitement de données **à visée exploratoire, de la pertinence et faisabilité de la génération de données synthétiques** à partir des bases « pilier » du SNDS préc., ce qui justifie que la CNIL en soit saisie [725].

Le point ici est que ces données sont créées **« *à partir d'un jeu de* *données du Système national des données de santé (SNDS), nécessitant un accès aux données du SNIIRAM et du PMSI, pour les années 2009 à 2019* »**. Il ne s'agit pas de données créés *ex nihilo* : on a vu que cela n'était pas possible, dans la dialectique du GAN entre réseaux générateur/discriminateur : il faut pour l'action discriminatrice, des données de santé réelles et annotées par les professionnels (au minimum associées à un diagnostic précis et fiable, ce qui est un enjeu compétitif mondial entre les bases de données et les puissances en présence).

b. Absence de conceptualisation juridique en droit européen

Paradoxalement, il n'y existe qu'une occurrence du terme « *donnée synthétique* » : elle figure dans le considérant n° 7 du règlement de 2022 sur la gouvernance des données, au rang des méthodes qui permettent dans les bases, de **procéder à des analyses respectueuses de la vie privée** [726]. S'il encourage des Etats membres à « *aider les organismes du secteur public à exploiter au mieux ces techniques et à mettre ainsi à disposition un maximum de données à partager* » (considérant n°7), il n'en donne pour autant aucune définition dans son article 2.

Certes, il y cite les « *données à caractère personnel* » (article 2.3, qui renvoie à l'article 4.1 du RGPD), et les « *données à caractère non personnel* » (article 2.4, sans équivalent dans le

[725] Décision DR-2022-152 autorisant la société EURIS CLOUD SANTE à mettre en oeuvre un traitement de données ayant pour finalité une étude portant sur l'évaluation de la pertinence et de la faisabilité de la génération de données synthétiques à partir d'un jeu de données du Système national des données de santé (SNDS), nécessitant un accès aux données du SNIIRAM et du PMSI, pour les années 2009 à 2019, intitulée « SYNTHIA ». (Demande d'autorisation n° 922027).

[726] Le considérant 7 cite « *notamment l'anonymisation, la confidentialité différentielle, la généralisation, la suppression et la randomisation,* ***l'utilisation de données synthétiques*** *ou des méthodes similaires, et d'autres méthodes de préservation de la vie privée à la pointe de la technologie* ».

RGPD [727]) ; mais **aucune des méthodes qui permettent de passer d'un état à l'autre**. N'était-ce pourtant le lieu utile d'une telle définition ?

En revanche, nul ne sera étonné de ne pas trouver dans le RGPD, la notion de « *donnée synthétique* » : celle-ci en effet **échappe nativement à son champ d'application**, puisqu'elle vise, par conception, à ne pas être « personnelle » (les éléments recombinés peuvent l'être, ce qui justifie on l'a vu, l'implication de la CNIL dans l'usage à cette fin des « données réelles).

Dans la proposition de règlement de 2021 relatif à l'intelligence artificielle [728], la notion est évoquée dans l'article 54.1b), comme recours dans le cas où la « donnée synthétique » pourrait ne pas satisfaire au besoin du développement des « systèmes d'IA à haut risque » [729].

La proposition l'évoque au titre d'un « bac à sable réglementaire » (espace d'expérimentation de pratiques jouissant d'une autonomie temporaire surveillée [730]), comme justification du recours à des données personnelles : ainsi, si ces « *données traitées sont nécessaires pour satisfaire à une ou plusieurs des exigences visées au titre III, chapitre 2, lorsque ces exigences ne peuvent être satisfaites de manière efficace en* ***traitant des données anonymisées, synthétiques ou autres à caractère non personnel*** ». Mais nous avons aussi déjà relevé que la « donnée anonyme » ou « l'anonymisation » n'étaient elles-mêmes pas définies, malgré les conséquences en droit du changement de statut de la donnée **qui devrait être irréversible… et pourrait ne pas l'être**.

2. Futur normatif : quelle perception de la « donnée synthétique » en santé ?

L'adaptation du droit dépend de la perception politique du phénomène. La question de la « donnée synthétique » est sans doute trop fraîche et technique.

La notion est-elle un enjeu normatif ? Elle ouvre un horizon essentiel, du fait des enjeux en santé, mais aussi de **dimensions compétitives et géopolitiques de concentration de**

[727] Le règlement de 2022 définit les données à caractère personnel, comme « *les données autres que les données à caractère personnel* », article 2.4.
[728] COM(2021) 206 final 2021/0106 (COD) Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle.
[729] Ibid., cf. titre III, Chapitre 2 dédié « Exigences applicables aux systèmes d'IA à haut risque ».
[730] Sur la notion, M-D. et G. Campion, « Bacs à sable réglementaires en santé : des initiatives diversifiées à la recherche d'un cadre fédérateur au service du bien public », RGDM 2023, n°10, 233-248.

puissance [731], pas seulement des droits fondamentaux des personnes. Cela n'apparaît qu'en filigrane dans la perception du CEPD (a) ; la réflexion s'ouvre (b).

a. La perception par le contrôleur européen de la protection des données

Nous avons vu que le CEPD se voulait l'acteur des institutions européennes le plus avancés dans la veille quant aux nouveaux outils et sensibilités en matière de données [732]. Il a fait valoir des **observations sur la notion de « données synthétique » en soi** : sur son site, on trouve, élaboré par monsieur Riemann, un onglet dédié aux « données synthétiques », pas spécifiquement en santé [733]. Le CEPD en salue la contribution à la protection de la vie privée, à une meilleure représentativité dans les modèles statistiques. Mais il relève aussi lapidairement la complexité du contrôle de leur production, la difficulté de cartographier des valeurs aberrantes, et la dépendance aux sources de données.

Nous avons relevé le silence des normes et projets de normes français et européens (à la date de notre rédaction) quant aux « données synthétiques ». Le CEPD **aurait-il pu faire valoir des observations incidentes,** comme il l'a déjà fait nous l'avons vu au décours de l'analyse de projets normatifs ? **Il ne l'a en tous cas pas fait ici.**

Du fait de sa mission de protection des « *données personnelles* », le CEPD **concentre l'attention sur l'apport de l'IA sous cet angle, non sous l'angle de la protection plus globale des systèmes** contre la pollution des données ou l'intoxication des algorithmes [734]. En outre, la « santé » n'est qu'un champ d'application parmi d'autres. Cela peut expliquer que le CEPD se fasse peu l'écho circonstancié des constats et inquiétudes de la littérature précités (lesquels contiennent nombre de réflexions extrapolables à d'autres champs que la santé).

Ainsi dans ses avis, la notion de « donnée synthétique » est apparue en 2016, **sans y être conceptualisée** [735]. Le CEPD **associe alors les données anonymes et synthétiques** : il

[731] Par domination oligopolistique des systèmes, ou par domination des données : cela ne revient-il pas au même, lorsque les données sont le substrat nécessaire de l'apprentissage / du réapprentissage ?
[732] Voir la publication de l'EDPS TechSonar, notamment Rapport 2021-2022, page 10. Il reste lapidaire.
[733] Non daté, mais postérieur à 2021, en anglais : Synthetic Data, https://edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en
[734] EDPS, « Opinion on the European Commission's White Paper on Artificial Intelligence –A European approach to excellence and trust », Opinion 4/2020, 29 juin 2020.
[735] EDPS, Guidelines on the protection of personal data processed through web services provided by EU institutions, nov. 2016.

évoque l'opportunité de créer des « *synthetic, anonymised data using some production data as starting point* » (R 48), afin d'éviter l'usage de données personnelles pour des activités de test [736]. La même année, le CEPD évoque dans une perspective différente (le but n'est plus d'éviter le recours à des données personnelles pour des finalités de test) [737], que « *Where the simple production of random test data sets* ***is insufficient in a specific context****, more sophisticated techniques* ***for creating synthetic data need to be used*** » [738] .

Si en décembre 2019, la notion ne figure pas dans ses lignes directrices pour l'évaluation de proportionnalité de mesures qui limitent les droits fondamentaux à la protection de la vie privée et la protection des données personnelles [739], elle **figure en 2020, dans son avis sur la stratégie européenne pour les données** [740]. Il y encourage la Commission à investir dans des recherches sur les « données synthétiques » parmi d'autres solutions prometteuses, « *which may,* inter alia*,* ***facilitate access to training data*** *for machine learning (…. et …)* ***mitigate data protection risks*** » [741]. Ainsi la perspective est-elle ouverte et profondément élargie.

En revanche en 2020, **aucune occurrence de la notion de « donnée synthétique » n'apparaît dans son avis sur le projet relatif à l'Intelligence artificielle** [742].

* Cet avis présente des soucis apparentés : ainsi, quant au besoin que tout futur cadre légal considère des éléments relatifs à la qualité et la traçabilité [743] des données (point 20), des risques spécifiques résident dans un éventuel défaut en la matière (point 21), etc. ; surtout, le CEPD est en désaccord avec le projet **sur les biais pouvant naître lors de l'apprentissage**

[736] Recommandation 48, page 32.
[737] EDPS, Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions (également nov. 2016).
[738] Ibid., dans le point 4.2.3., §46.
[739] EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 nov. 2019.
[740] EDPS, Opinion 3/2020 on the European strategy for data, 16 juin 2020.
[741] *Ibid*., point 66 page 14.
[742] EDPS, Opinion 4/2020, EDPS Opinion on the European Commission's White Paper on Artificial Intelligence –A European approach to excellence and trust, juin 2020.
[743] Ainsi explicitée par le CEPD (Ibid., note de pas de page n°15, page 9) : « The data sets and the processes that yield the AI system's decision, including those of data gathering and data labelling as well as the algorithms used, should be documented to the best possible standard to allow for traceability and an increase in transparency. This also applies to the decisions made by the AI system. This enables identification of the reasons why an AI-decision was erroneous which, in turn, could help prevent future mistakes. Traceability facilitates auditability as well as explainability." HLEG Guidelines (page 18) »

par les données : **il considère ce problème comme de conception, non d'application** (point 22) [744]. Cela nous semble très ambitieux, peut-être à la limite du réalisme [745] ?

* Enfin, une autre ambition est énoncée par le CEPD, qui, en accord avec la Commission quant à l'opportunité de la mention de surveillance de conformité (*compliance monitoring*), considère qu'il devrait être ajouté que de tels contrôles **ne devraient pas se limiter au contrôle de la documentation et au test des applications** : il y ajoute le contrôle de transparence, au sens de l'explicabilité des décisions prises par l'IA [746] ; et des essais sur les données d'entraînement, pour s'assurer de leur adéquation (point 60).

Cette vision recoupe, en santé, **le besoin que des données synthétiques puissent être utilisées dans des « tests de résistance » réglementaires**, avant que les algorithmes d'IA soient utilisés par les médecins et patients. Or, l'explicabilité supposerait une généalogie du raisonnement, avec marquage de ses étapes. Peut-être cela sera-t-il un prérequis pour les IA « à haut risque » ? mais alors, les bases utilisées ne devraient-elles être en permanence re-convocables ? cela rend cette stratégie difficile, du fait de leur évolutivité et extranéité.

Même si tous ces éléments intéressent la notion de « donnée synthétique », le CEPD **ne cite pas une fois la notion,** hors de l'onglet sur son site et son rapport de veille lapidaire [747]. Pas plus, le projet de règlement sur l'intelligence artificielle en 2021 ; ni la proposition de règlement relatif à l'espace européen des données de santé en 2022, rendus après ses avis. Ainsi, **l'écart est grand entre l'approche institutionnelle de la notion, et les prévisions d'usage exponentiel** sur un horizon 2030 (pas spécifiquement en santé) [748].

---

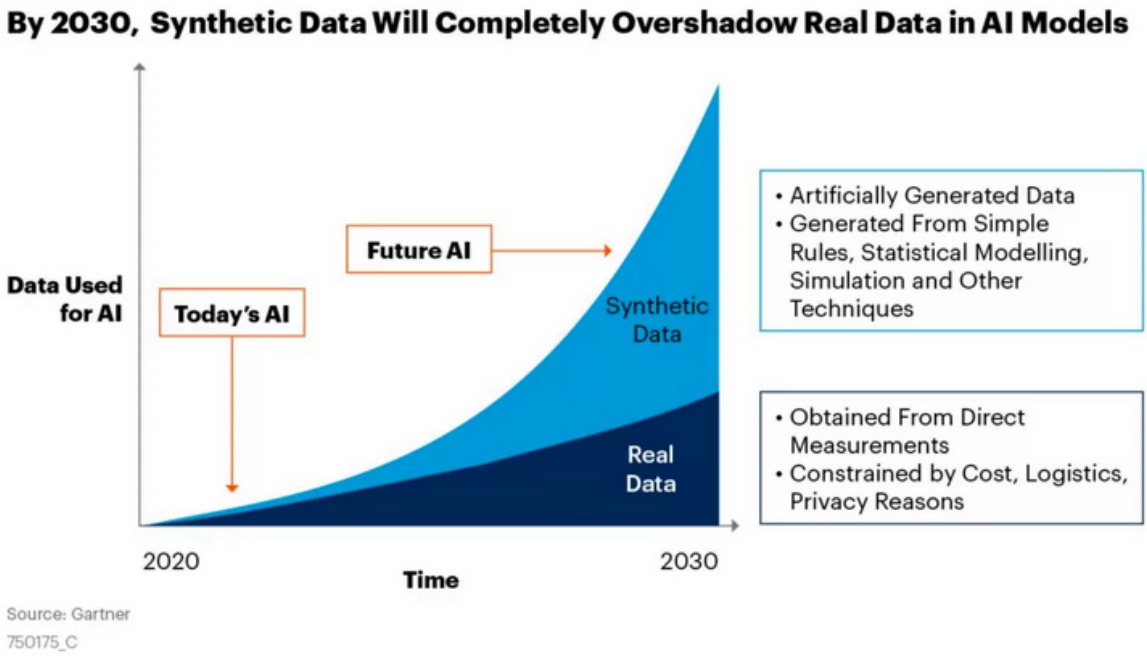
[744] « While the EDPS agrees that bias could also affect AI systems that learn during their operation, the White Paper goes further stating that when the AI system 'learns' while in operation '...the outcome *could not have been prevented or anticipated at the design phase*, the risks will not stem from a flaw in the original design of the system but rather from the practical impacts of the correlations or patterns that the system identifies in a large dataset.' (own emphasis). The EDPS disagrees with this assessment. **AI application design should take into account potential bias in the training data and, when applicable, in operational data.** Bias can and must be measured and corrected *during the operation* of AI applications as much as it can be measured and corrected during its development ».

[745] Il apparaît difficile d'intégrer des éléments d'inhibition de dynamiques d'apprentissages, qui ne pouvant de notre point de vue être facilement prévenues ex ante, ne semblent pouvoir être corrigées qu'ex post.

[746] « (including the capacity to explain how it reaches decisions) »

[747] CEPD (EDPS), Sonar Tech, 2021-2022 Report, voir pages 10-11.

[748] C. Dilmegani, « What is Synthetic Data? Use Cases & Benefits », publié en 2018, actualisé le 20 janv. 2023, sur https://research.aimultiple.com/synthetic-data/



Retenons toutefois pour nuancer ces prévisions que la production de « données synthétiques » qu'il n'est pas impossible que certains entendent en invoquant ce **marché des données synthétiques**, **stimuler son apparition.** Des doctrines s'en sont à juste titre, mais brièvement inquiétése [749]. Cela ne devrait il pas justifier l'appréhension de la notion par les normes ?

b. Quelle dynamique pour la « donnée synthétique », d'un point de vue normatif ?

Sans qu'aucune définition n'en soit donnée donc, la notion de « donnée synthétique » fait une **très courte apparition dans le règlement 2022/868** sur la gouvernance des données [750].

En effet dans son considérant n° 7, ce règlement procède à une liste des « *techniques permettant d'effectuer des analyses dans les bases de données contenant des données à caractère personnel, notamment l'anonymisation, la confidentialité différentielle, la généralisation, la suppression et la randomisation,* ***l'utilisation de données synthétiques*** *ou des méthodes similaires, et d'autres méthodes de préservation de la vie privée à la pointe de la technologie, qui pourraient contribuer à un traitement des données plus respectueux de la*

[749] A. et A. Arora, « Synthetic data in health care : a widening legal loophole », (correspondance) in The Lancet, 23 avril 2022 ; vol. 399, issue n° 10335, p 1601-1602.
[750] Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données). En contraste, il n'existe aucune occurrence dans le Règlement 2022(UE) du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).

vie privée ». **Mais l'emphase est encore ici sur la protection de la vie privée**, alors que cela n'est désormais plus qu'un aspect du défi, **face aux risques clinique, populationnel et souverain** [751].

Pour re-situer le raisonnement, nous complétons ici le tableau de la CNIL, qui explique les processus de pseudonymisation et d'anonymisation. Nous lui y **ajoutons une colonne pour les « données synthétiques »**, qui ne participent pas totalement des données anonymes :

Tableau CNIL original			**Ajout**
Processus	**Pseudonymisation**	**Anonymisation**	***Synthèse***
Statut des données	Personnelles (restent indirectement identifiantes et donc soumises au RGPD et à la loi Informatique et Libertés	Anonymes	*Synthétique*
Réutilisation des données	Sous conditions	Sans restriction	*Sans restriction ?*
Utilité des Données	Préservée car pas d'altération du niveau de détail des données	Plus ou moins altérée en fonction des objectifs poursuivis et des méthodes appliquées	*Pleine ? Mais pas seules !*
Méthodes à mettre en œuvre	Compteur, générateur de nombres aléatoires, fonction de hachage, chiffrement à clé secrète, etc.	Dépend des objectifs poursuivis : confidentialité différentielle, randomisation, k-anonymat, l-diversité, t-proximité, etc.	*Génération par GAN à partir d'une base réelle de données annotées*
Complexité de la mise en œuvre	Simple à moyenne	Dépend des objectifs poursuivis : simple dans certains cas comme l'agrégation ou le comptage et complexe dans d'autres	*Forte … pour être pertinente …*

N'étant pas des « données personnelles », les données synthétiques en tant que « produit » ne relèvent certes pas de l'autorité de la CNIL. En revanche, elle **est intéressée au processus de**

[751] Rappelons l'article 5§13 du Règlement (UE) 2022/868 préc. **En effet, il inverse l'emphase** : « *Des actes législatifs spécifiques de l'Union peuvent considérer que* ***certaines catégories de données à caractère non personnel*** *détenues par des organismes du secteur public sont hautement sensibles aux fins du présent article, lorsque leur transfert vers des pays tiers peut mettre en péril des objectifs de politique publique de l'Union****, tels que la sécurité et la santé publique****, **ou peut** entraîner un risque de réidentification de données anonymisées à caractère non personnel* ».

leur génération, dès lors que ce dernier mobilise en France des données personnelles pour leur construction [752]. Qu'en est-il au-delà ?

Mêmes s'ils ne définissent, ni *a fortiori* n'encadrent pas la « *donnée synthétique* » de santé, les textes européens et nationaux ne sont pas pour autant silencieux, on l'a vu. Nombre de leurs dispositions sont **extrapolables aux données synthétiques** : ainsi notamment l'exigence de caractère irréversiblement anonyme (face à des attaques « d'appartenance d'inférence »), de qualité et d'intégrité des données, etc. qui peut conduire à l'édiction de réglementations spéciales, quant à leur validation avant leur introduction pour apprentissage.

Dès lors, une nouvelle activité ne devrait-elle pas **être conceptualisée et encadrée, celle de producteur de données synthétiques de santé**, *a fortiori* dans les hypothèses d'IA « à haut risque » ? En santé, l'IA qui aide à la décision face à un patient déterminé sur la base de ses données personnelles (diagnostic, pronostic, thérapeutique, surveillance, adaptation de traitements etc.), est un dispositif médical. Les algorithmes qui constituent le logiciel ou le servent directement, reçoivent la qualification de « dispositifs médicaux », tout comme leurs accessoires. Les données synthétiques qui, par entraînement, accroissent leur capacité, **leur sont consubstantielles. Ne pourrait-on donc imaginer que, par leur destination,** elles suivent la même qualification ? que, en conséquence, leur génération (à visée d'apprentissage supervisé) soit soumise à une certification de conformité à des exigences à définir ?

Il ne s'agit pas ici d'ajouter une couche de régulation là ou elle ne serait pas utile. **La non-implication des « données de santé » personnelles n'est plus le seul sujet**. A cet égard, le travail d'éclairage des candidats IA publié en janvier 2022 par la Haute Autorité de Santé [753], nous semble répétons le une contribution majeure [754] : **ses exigences de qualité en vue de l'admission au remboursement d'une IA, ne recoupent-elle pas les exigences de sécurité en vue d'une commercialisation de « données synthétiques » sur le marché ?**

Les sujets étant nous l'avons vu liés, ce travail nous semble pouvoir servir de base raisonnable pour réfléchir à la génération des « données synthétiques » de santé : ceci sachant, en amont,

[752] On l'a vu *supra* avec son premier avis rendu en 2022, pour la génération de données synthétiques en santé.
[753] Dont HAS/CNEDIMTS Annexe (validée 6 janvier 2022) titrée « Informations descriptives spécifiques à fournir pour les fonctionnalités du dispositif médical s'appuyant sur des procédés d'apprentissage automatique (technologies relevant du champ de l'intelligence artificielle) », *supra*.
[754] On verra également avec intérêt, les principes très lapidaires principes élaborés par la FDA, l'agence canadienne, et le MHRA (agence britannique) en 2021 : « Good Machine Learning Practice for Medical Device Development : Guiding Principles - October 2021 ».

le **besoin notamment d'annotation des données** de santé « réelles » pour l'apprentissage des GAN (quels seront alors les centres de référence, dans quels pays, selon quelle école ?) ; en aval, le **besoin de cadrer des systèmes d'IA selon des référentiels cliniques** évolutifs au regard des connaissances – donc des données ! [755] - dynamiques de la science.

SYNTHESE P1T2C2

Ce second chapitre du **Titre II « définition de la donnée de santé, du contenu au contexte »** était le cadre de restitution de nos observations, toujours plus prospectives, de la dynamique de la notion de « donnée de santé » dans le cadre cette fois de la recherche : c'est à dire ici tant en matière de recherche biomédicale, que pour des exploitations « secondaires », étrangères au but pour lesquelles les données avaient été initialement produites et utilisées.

* Dans une première section, nous relevons la dynamique de la génération de données personnelles **dans le cadre de la recherche biomédicale**. Nous pointons les difficultés de catégorisation propres au droit français dit RIPH quant aux études participant de cette recherche, selon que la personne est réputée « impliquée », ou « non impliquée » dans celle-ci (quoiqu'elle « participe » à cette recherche). Nous relevons comment ces atermoiements sémantiques conduisent à des colmatages réglementaires et jurisprudentiels, et une faible intelligibilité de notre droit national. Puis nous relevons que cette catégorisation n'est pas pas un critère de qualification des méthodes de référence pour le recueil de données dans la recherche, que ce soit en droit commun, dont nous avons relevé les interférences entre champs interventionnel / observationnel ; ou en droit réformé en 2022 des accès précoce notamment, lequel du fait de son autonomie, échappe au droit de la RIPH.

* Dans une seconde section, nous relevons **l'avènement en droit, des « usages secondaires »** des données de santé. Cela met en jeu la subdivision de la notion et les paramétrages, soulevant les difficultés de conceptualisation et d'emploi de la donnée de santé « de vie

[755] M. Lenatti, A. Paglialonga, V. Orani et al. « Characterization of Synthetic Health Data Using Rule-Based Artificial Intelligence Models », IEEE J Biomed Health Inform 2023 Jan 13 ; doi: 10.1109/JBHI.2023.3236722 (Epub ahead of print. PMID: 37018683).

réelle ». Stratégiques pour la gouvernance publique et les compétiteurs, ces usages sont aussi de plus en plus promus dans le champ en France régalien des décisions d'acquisition et de négociation des technologies de santé remboursables. Alors que droit européen s'apprête à ouvrir massivement cet usage, la fiabilité des processus d'anonymisation et de pseudonymisation des données personnelles appelle une réflexion renouvelée par les technologies et le potentiel de réidentification. Nous relevons l'émergence de la notion de « donnée synthétique » de santé, laquelle prétend remédier au double défi de la protection des personnes, et du défaut de représentativité des données personnelles disponibles. Mais ses enjeux à l'ère de l'IA appellent une réflexion approfondie actuellement balbutiante ; peut-être aussi un statut en droit, du fait de sa vocation commerciale et internationale, et de ses conséquences dans les systèmes informatisés d'aide à la décision.

SYNTHESE P1T2

Si la donnée de santé ne dispose d'un contenu positif que depuis récemment, nous avons constaté dans ce titre II que sitôt défini, ce contenu tendait à aspirer du contexte informationnel qui de plus en plus participe également de la « donnée de santé ».

A côté des données de santé qui sont produites de façon organique par le système de santé où elles sont nativement générées et encloses, ou qui sont aspirées sur les bases de donnée légales (données « par qualification de la loi »), nous avons relevé le développement croissant de données de santé « par destination » : ceci non au seul sens retenu par la CNIL, de la vocation terminale éventuelle à l'utilisation médicale de données produites hors du système de santé, mais au sens de la vocation à être exploitées selon leur signification médicale, pour des applications potentiellement étrangères à la production des soins notamment, et comportant des risques pour la maîtrise de notre destin.

Après avoir relevé ces méthodes générales de classification, nous relevons que les catégorisations propres au droit français en matière de **recherche biomédicale** soulevaient de nombreuses difficultés et avait appelé des artifices juridiques de colmatage, mais sans mettre en cause la qualification des données qui en sont issues. En dépit de certaines prétentions, les procédures qui en conditionnent la production n'en assurent pas, et ne peuvent en assurer la qualité, ce qui conduira en partie II à s'interroger sur ce concept.

L**'avènement en droit des « usages secondaires »** des données de santé met en jeu la subdivision de la notion et les paramétrages induits. Le défi est patent pour l'emploi de la donnée « de vie réelle », dont la fiabilité de l'anonymisation devient improbable du fait des progrès technologiques, et dont la représentativité est limitée du fait des surfaces d'observations et conditions de recueil.

Il en résulte une poussée de la notion de « donnée synthétique », qui veut l'imiter. La maîtrise de sa production et l'acquisition d'un statut **deviennent en enjeu considérable** à l'ère de l'IA et de la capture oligopolistique, ou de la déstabilisation, de l'aide à la décision.

PARTIE II – SOUVERAINETE ET DYNAMIQUE DU REGIME DES DONNEES DE SANTE

Dans la première partie de notre recherche, nous avons cherché à appréhender la **transformation d'un champ complexe couvert par la notion floue** de « donnée de santé », et sa conséquence : **l'ajustement continu et à venir des catégories du droit, au plan national et européen.** Cela, du fait de phénomènes de nature et d'ampleur inédits, stimulés par les technologies de la production, de la collecte et du traitement transnational de l'information en santé (incluant les comportements et environnements non médicalisés) ; mais aussi de leur génération synthétique en développement, par l'IA et pour son apprentissage.

Dès lors, la sensibilité descriptive et prédictive de l'assemblage de ces données, voire son potentiel d'usage inductif, **ne sont plus seulement d'ordre individuel, mais populationnel, donc systémique et politique,** que les données « de santé » soient « personnelles », ou non : ceci donc au-delà des termes des normes et conventions qui historiquement focalisent sur les droits des individus, pour définir les devoirs des professionnels et des institutions.

En conséquence, nous nous proposons d'étudier **la dynamique des mécanismes de protection des « données de santé »**, laquelle a vu son fondement élargi, et a changé d'échelle : de l'individuel au populationnel, du national à l'inter-national. Il s'agit des mécanismes **d'usage partagé protégé**, non des mécanismes de mise à disposition internationale de statistique ouverte (sous couvert de l'OMS au plan mondial [756], de l'OCDE [757], d'Eurostat au plan européen [758] etc.), qui présentent une granulométrie et fiabilité variables.

Ils n'appellent pas moins de réflexion attentive : la première fois qu'un avis du CEPD a été sollicité sur une proposition de Règlement dans le domaine des statistiques communautaires, **était pour le règlement relatif aux statistiques communautaires de la santé publique** [759].

---

[756] OMS, Rapport 2023, « World Health Statistics 2023 : Monitoring Health for the SDGs, Sustainable Development Goals », ISBN 978-92-4-007432-3.

[757] OCDE, « Statistiques de l'OCDE sur la santé 2023 » (publication le 3 juillet 2023) : voir les bases de données en ligne (https://www.oecd.org/fr/sante/base-donnees-sante.htm).

[758] EUROSTAT, onglet « santé » statistiques par thèmes » (https://ec.europa.eu/eurostat/fr/web/health/overview).

[759] Avis du contrôleur européen de la protection des données sur la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, 2007/C 295/01, au JO du 7 déc. 2007 (signalé par le CEPD même, point 2).

Mais la dynamique des mécanismes de protection ne nous intéresse toutefois ici, **qu'en tant qu'elle suppose ou implique des aménagements de souveraineté** [760] **des Etats censés garantir la protection des « données de santé »** et des systèmes qui les traitent, au même rang que l'accès des personnes à la santé : nous ne traiterons donc pas ici du régime du secret, du droit national et comparé de protection des données personnelles, des accès individuel et des exceptions en la matière [761], ni des écarts nationaux observés dans leurs mises en œuvre [762].

Dans l'Union, cela révèle d'approches dont nous avons relevé la dynamique intégrative ; hors Europe, d'approches coopératives à base bi- ou multilatérale et à géométrie variable. Pour les raisons exposées en introduction de notre thèse, liées aux forts développements depuis le dépôt fin 2017 du champ de notre recherche, nous proposons ici seulement de traiter au sein de l'Union européenne, des causes et étapes (les effets du droit en vigueur n'étant pas encore toujours observables, et certains textes proposés en 2021, 2022 et 2023 pas encore adoptés), de l'avènement de **garanties réciproques pour un accès interne licite** aux données (Titre I).

Dans un second temps, nous traiterons de l'avènement, en accélération pressante du fait de la vulnérabilité révélée et accrue des systèmes et de l'Union, dont le destin commun est engagé, de **garanties réciproques contre l'accès externe illicite** d'acteurs privés et publics non UE ; ceci face à une ingérence parfois par voie de droit, parfois par voie de fait **au-delà de la cyber-criminalité de droit commun**, non sans difficultés de qualification dans une géopolitique sous tension (Titre II).

TITRE I. DYNAMIQUE DES GARANTIES UNIFIEES DE L'ACCES LICITE AUX DONNEES DANS LE CHAMP SANTE

Dans notre champ, nous constatons qu'ont été progressivement conceptualisées, puis institutionnalisées par actes contraignants, des garanties réciproques pour la **maîtrise unifiée**

---

[760] Sur cette question que nous n'approfondirons pas ici, spéc. Lemaire F, « Propos sur la notion de 'souveraineté partagée' ou sur l'apparence de remise en cause du paradigme de la souveraineté », Rev. fr. dr. constit. 2012/4 n°92, pp 821-850, qui invite audacieusement à ne pas confondre le partage de souveraineté et partage de ses attributs ; auparavant, Chaltiel F, *La Souveraineté de l'État et l'Union européenne, l'exemple français*, LGDJ, 2000 ; et Favret JM, « L'Intégration européenne et la France : quelques réflexions sur la divisibilité de la souveraineté », *RDP*, 1999, pp. 741-1764.

[761] Pour une présentation détaillée du droit français et de sa matrice RGPD en la matière, L. Maisnier-Boché, Fasc. 945 : Données de santé à caractère personnel – Régime général, Jurisclasseur Communication, Lexis 360 (2023) ; pour une analyse approfondie de la transformation de la notion, F. Megerlin, Fasc. 8-10, Traité droit pharmaceutique LITEC, Jurisclasseur de LexisNexis (2023).

[762] Objet en 2021, d'un rapport approfondi (anglais seulement) : EU DG Health and Food Safety, « Assessment of the EU Member States' rules on health data in the light of GDPR », Specific Contract No SC 2019 70 02.

et d'intérêt partagé, de l'accès aux données de santé. Outre ses moteurs philosophiques (vision) et politiques (stratégie) précités, cette dynamique possède deux causes mécaniques :

* La première est **institutionnelle et participe du droit originaire**. L'article 114 du TFUE promeut l'activité des institutions visant « *à améliorer le fonctionnement du marché intérieur et la libre circulation des marchandises, des personnes et des services* ». Dès lors qu'un tel enjeu intracommunautaire est caractérisé, le droit de l'Union « *doit se fonder sur* (cet article) ***même lorsque la protection de la santé publique est un facteur déterminant*** *dans les choix opérés* » [763] ; ceci sans préjudice d'un niveau élevé de protection de la santé (114§3 TFUE).

Or, tel est le cas ici ; à un double titre : la liberté de circulation de la personne **trouve pour corollaire** la liberté de circulation du patient, donc de ses données pour l'accès fluide aux produits et services de santé notamment. Mais la **liberté peut être aussi subordonnée** au partage de telles données : tel a été l'effet révélateur de la pandémie en 2020.

* La seconde **découle d'une crise systémique mondiale**. Certes, la pandémie de Covid19 n'est pas la première des crises sanitaires internationales modernes source de stress des populations et des institutions [764]. Mais elle a révélé l'impréparation et la faible performance collective au sein de l'Union, l'indisponibilité de ressource stratégique en technologies de santé, et **l'excitation par défaut, de stratégies compétitives de survie nationale** [765].

Or, cela explique **l'accélération consentie de l'information réciproque, et de mécanismes décisionnels centralisés.** L'ensemble vise à limiter les coûts de surprise future, après la fragmentation presque conflictuelle des initiatives dans l'Union.

Nous distinguerons donc deux temps, **sachant cette distinction non causée par la pandémie, mais stimulée par elle** : à une période d'approche coopérative horizontale, à base facultative et géométrie variable (chapitre I), succède de manière rapide depuis 2020, une approche intégrative verticale, à base normative et vocation unifiante (Chapitre II).

---

[763] Considérant 2, Dir. 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontalier.

[764] L'Organisation mondiale de la santé a néanmoins déclaré le 11 mars 2020 que la flambée de maladie à nouveau coronavirus (COVID-19) constituait une pandémie mondiale.

[765] Pour une approche des grands ensembles continentaux sur le terrain des données de santé, v. Martinez J, Tonon C, «La gouvernance des données de santé: leçons de la crise du Covid-19 en Europe, en Chine et aux États-Unis», Études de l'Ifri, Ifri, juillet 2021

CHAPITRE I - LA DYNAMIQUE NORMATIVE DE L'APPROCHE COOPERATIVE EN MATIERE DE DONNEES DE SANTE

L'Union a adopté plusieurs stratégies successives en matière de santé, sachant la compétence essentiellement nationale en la matière (article 168 TFUE) : l'Union ne vise qu'« *à compléter les politiques nationales et à soutenir la coopération dans le domaine de la santé publique* ». Le dernier texte programmatique est le Règlement 2021/522/UE, lequel établit un programme d'action pour la période 2021 / 2027 [766], abrogeant le précédant n° 282/2014 adopté pour 2014/2020 (les « données de santé » y sont alors encore peu présentes) [767].

Auparavant – cela est intéressant **quant au choix des véhicules juridiques**, ces programmes d'action dans le domaine de la santé **n'étaient le fait que de décisions** du Parlement européen et du Conseil : ainsi le premier (2003/2008) [768] et le deuxième programme d'action (2008/2013) [769], sur fond de communications de la Commission visant à baliser le débat et canaliser l'action normative, notamment en 2018 en matière de transformation numérique [770].

Nous voyons ici le primat de la base volontaire dans la dynamique européenne pré-pandémique (section I), avant de relever son accélération et le développement inédit de normes en la matière, sous l'effet de la pandémie de Covid19 (section II).

SECTION I. DYNAMIQUE EUROPEENNE PRE-CRISE COVID19 : LE PRIMAT DE LA BASE VOLONTAIRE

Les compétences de l'Union en matière de santé sont on l'a vu, limitées par le Traité (article 168 TFUE). Mais **le fait que la compétence soit essentiellement nationale, ne porte pas atteinte à la recherche**, en application de l'article 114 TFUE, de la libre circulation des personnes, des services et des marchandises.
Tel était l'objet en 2018 de la communication 233 de la Commission: éclairer l'intérêt de la transformation numérique des services de santé, dont nous verrons les applications.

---

[766] Règlement (UE) 2021/522 du Parlement européen et du Conseil 24 mars 2021 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.
[767] Règlement (UE) n ° 282/2014 du Parlement européen et du Conseil du 11 mars 2014 portant établissement d'un troisième programme d'action de l'Union dans le domaine de la santé (2014-2020).
[768] Décision n°1786/2002/CE du Parlement européen et du Conseil, modifiée par la décision n°786/2004/CE.
[769] Décision n°1350/2007/CE du Parlement européen et du Conseil du 23 octobre 2007 établissant un deuxième programme d'action communautaire dans le domaine de la santé (2008-2013).
[770] COM (2018) 233 final Permettre la transformation numérique des services de santé et de soins dans le marché unique numérique; donner aux citoyens les moyens d'agir et construire une société plus saine.

Relevons ici deux dynamiques au travers de leurs exemples emblématiques : la première est **une dynamique de fluidification, justifiée par la liberté** des individus et des activités (§1). La seconde est une **dynamique de coordination, fondée sur le besoin** d'un développement de protection collective par des outils nouveaux (§2).

§1. LA DYNAMIQUE NORMATIVE DE FLUIDIFICATION POUR LA LIBERTE DES PERSONNES

L'accès aux soins est un droit protégé depuis 2000 dans des termes communs à l'échelle européenne, par la Charte européenne des droits fondamentaux (article 35) ; le bénéfice de soins transfrontaliers est le corollaire nécessaire de la liberté de circulation des personnes. Mais ce principe de mobilité du patient et d'accessibilité de tous aux soins dans l'Union, devait y être concilié avec une recherche d'équilibre des systèmes, objet de la Directive 2011/24/UE [771] adoptée en 2011 mais proposée en 2008 [772].

Cette liberté a pour but de permettre aux patients **de se faire soigner en dehors de leur Etat membre d'affiliation** [773] ; mais elle ne doit pas avoir pour effet de l'encourager : il en résulterait un risque de désorganisation des systèmes nationaux et dès lors, un risque d'opposition légitime des Etats membres (sur le fondement des articles 52 et 62 du TFUE) [774].

Sur ce point, les régions frontalières sont depuis toujours considérées comme des laboratoires d'intégration [775], du fait des besoins spécifiques et complémentarités en santé notamment : la question de l'accès (régions démédicalisées, complémentarité transfrontière, politiques d'investissements, coopérations structurées) fait l'objet de débats récurrents [776].

---

[771] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers.

[772] Proposition de directive du Parlement européen et du Conseil relative à l'application des droits des patients en matière de soins de santé transfrontaliers. COM(2008) 414 Final, 2 juill. 2008.

[773] En ce sens, spéc. les consid. n° 4 et 21 de la directive 2011/24/UE.

[774] i.e. pour motifs de santé publique. En conséquence par exemple, une autorisation préalable peut ainsi être exigée à l'hôpital, ce que la CJUE juge nécessaire et raisonnable du fait de l'enjeu de la planification de l'offre et de la programmation des soins.

[775] Rapport de la Commission « Les régions frontalières de l'UE: des laboratoires vivants de l'intégration européenne », COM/2021/393 final.

[776] En mai 2022, étude publiée par la Commission européenne, « Study supporting the evaluation of the Directive 2011/24/EU to ensure patients' rights in the EU in cross-border healthcare ». Pour un exemple tout récent de questionnement en France, voir « Zone organisée d'accès aux soins transfrontaliers entre la France et le Luxembourg », Question orale n° 0238S de V. Guillotin, JO Sénat 27/10/2022, p 5235 ; Réponse du Secrétariat d'État, JO Sénat 15/02/2023, p 1033.

La **recherche de ce subtil équilibre** était rendue complexe, mais aussi est facilitée, du fait des outils technologiques émergeants, permettant la réalisation du but. Nous le voyons ici avec l'organisation graduelle des soins transfrontières dans l'Union européenne (A), dont l'expérience a fondé une pétition de partage élargi des « données de santé » à son échelle (B).

A. L'ORGANISATION GRADUELLE DES SOINS TRANSFRONTIERES DANS L'UNION EUROPEENNE

Dans tout système de santé, **la continuité des soins est un impératif majeur pour le patient**, qui au-delà de l'accès aux prestataires commande le *continuum* informationnel, par « échange » et « partage » des données de santé dans des conditions relevant de la compétence nationale. Nous les avons précédemment examinées *supra* en droit français.

Considérons deux exemples qui mettent en exergue le dialogue entre les systèmes, et non plus seulement leur fonctionnement interne (matière souveraine), portés par la directive 2011/24 : ces conditions de *continuum* devaient être déclinées pour un **objectif généraliste** sur les soins transfrontaliers (article 14) [777] ; un flux permanent doit être établi pour un **objectif plus spécifique** par la mise en place de réseaux européens de référence [778] mutualisation une expertise dispersée pour la prise en charge de « maladies rares » ou complexes [779] (article 12).

Nous relevons ici brièvement, sur les points qui nous intéressent quant aux « données de santé », la dynamique juridique du partage appelé par l'impératif du continuum informationnel (1), puis par l'établissement d'une mutualisation de l'expertise (2).

[777] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).
[778] Ibid.
[779] Dont la prévalence est de 0,05% (ne touchent que 5 personnes sur 10 000), mais qui présentent une grande variété de cas donc fortement dispersés dans l'Union. Définie par Décision no 1295/1999/CE du Parlement européen et du Conseil du 29 avril 1999 portant adoption d'un programme d'action communautaire relatif aux maladies rares, dans le cadre de l'action dans le domaine de la santé publique (1999-2003), abrogée par la décision no 1786/2002/CE.

1. Le partage appelé par l'impératif du *continuum* informationnel, sous la responsabilité des Etats membres (article 14)

Le développement pratique des soins transfrontaliers fait que la problématique des accès et *continuum* est très concrète sur le terrain, ce dont attestent en 2023 les plus récentes études [780]. Ce qui nous intéresse ici est que plusieurs dispositions de la directive de 2011 mettent en exergue ce *continuum* au titre des **responsabilités de l'Etat membre de traitement** (au sens de « *État membre sur le territoire duquel les soins de santé sont effectivement dispensés* » article 3.d), et que le **paramétrage du champ des données partageables** est en question.

La décision d'exécution en 2019, qui modifie la décision d'exécution antérieure [781], institue le réseau « santé en ligne », défini (article 2§1) comme le « *réseau constitué* ***sur la base du volontariat*** *reliant les autorités nationales chargées de la santé en ligne désignées par les États membres et poursuivant les objectifs énoncés à l'article 14 de la directive 2011/24/UE* », **pour de multiples activités à caractère facultatif** (article 4§1) : le but au-delà de la promotion du continuum pratique du soin, est de **fournir aux Etats membres des orientations à visée transformatrice** [782].

Dans le but exprès « d'assurer la continuité des soins », les patients concernés ont un droit à ce que le traitement reçu soit enregistré par écrit de façon électronique (Directive, article 4.f), doivent bénéficier de la protection de telles données au titre de leur droit fondamental à la vie privée (Directive, article 4.e), et de procédures transparentes en cas de demande de réparation fondée sur un préjudice subi dans le cadre des soins reçus (Directive, 4.c).

Pour ce qui est des **responsabilités de l'Etat membre d'affiliation** (affiliation nationale du patient, qui en est ressortissant ou non), des articles instituent des obligations de continuité fondées sur le partage d'information. Ainsi, l'égalité de suivi médical quel que soit le lieu où

---

780 La Commission a publié le 6 juin 2023, l'étude « Data on cross-border patient healthcare following Directive 2011/24/EU Reference year 2021 » ; auparavant le 13 mai 2022, l'étude « Data on patient mobility under Directive 2011/24/EU - Trend report reference years 2018-2020 » (disponibles sur le site de la Commission).

781 Décision d'exécution 2011/890/UE de la Commission du 22 décembre 2011 arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales responsables de la santé en ligne,

782 « *1. Dans la poursuite de l'objectif visé à l'article 14, paragraphe 2, point a), de la directive 2011/24/UE, le réseau «Santé en ligne» peut notamment: a) promouvoir une plus grande interopérabilité des systèmes nationaux de technologies de l'information et de la communication et la transférabilité transfrontalière des données électroniques de santé dans le cadre des soins de santé transfrontaliers; «* ensuite, les b), c), d), e), f) g) commencent par *« fournir des orientations ».*

les soins auront été reçus (Directive, 5.c), et surtout, le droit d'accès à distance à leur dossier médical, et de disposer d'une copie (Directive, 5.d).

Mais c'est dans l'article 14 dédié à la « santé en ligne » que sont **objectivés le mode d'échange d'informations et ses prérequis** techniques. Il n'est pas lieu ici d'entrer dans le détail applicatif, objet de travaux auquel le lecteur pourra se référer [783]. Ce qui nous intéresse est toujours notre fil rouge de la donnée de santé.

Or, tandis que l'article 3,m) définit le « dossier médical » comme « *l'ensemble des documents contenant les données, les évaluations et les informations de toute nature concernant l'état de santé d'un patient et son évolution clinique au cours du traitement* », l'article 14.2.b.i) dispose que le réseau doit notamment **élaborer des orientations** concernant une « ***une liste non exhaustive de données à faire figurer dans le dossier des patients et pouvant être partagées*** *par les professionnels de la santé pour permettre la continuité des soins et promouvoir la sécurité des patients par-delà les frontières* ».

Ainsi, on constate la combinaison de deux considérations : les données « à faire figurer dans le dossier » et « pouvant être partagées ». Cela peut introduit un questionnement : toutes les données devant figurer dans le dossier ont elles vocation à être partagées ? Les données à faire figurer dans le dossier sont-elles seulement celles ayant cette vocation ?

L'unité de raisonnement n'apparaît pas le dossier médical (entité historique) mais la donnée de santé pertinente. La question s'avérera ne pouvoir être tranchée, conduisant en 2022 nous l'avons vu à la proposition de « ***Catégories prioritaires de données de santé*** *électroniques à caractère personnel à des fins d'utilisation primaire »* [784].

En outre, le régime de responsabilité dans le traitement des données **ne sera précisé qu'en 2019** par acte d'exécution modificatif [785] : un article 7 titré « *Protection des données à caractère personnel traitées par l'intermédiaire de l'infrastructure de services numériques dans le domaine de la santé en ligne* » **met en exergue la responsabilité des Etats membres**

[783] Pour un approfondissement pratique de la mise en œuvre du cadre de 2011, voir Dubuis A., « L'article 14 de la directive 2011/24/UE sur le réseau « santé en ligne » : Quel contenu pour quelle application ? », in *La santé connectée et "son" droit : approches de droit européen et de droit français 2017 préc.*
[784] Article 5 de la proposition de règlement EESD mai 2022, préc.
[785] Décision d'exécution (UE) 2019/1765 de la Commission du 22 octobre 2019 arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales chargées de la santé en ligne, et abrogeant la décision d'exécution 2011/890/UE.

représentés par les autorités nationales compétentes ; c'est à eux de « (répartir) *de manière claire et transparente les responsabilités entre les responsables* (sic) *du traitement des données* » (7§1). La Commission est considérée comme un sous-traitant, qui n'a pas accès aux données personnelles des patients traitées par le réseau santé en ligne (7§2) ; en revanche, elle traite des données nécessaires aux accès aux services centraux, qui se limitent aux coordonnées des utilisateurs (7§3).

En 2020, le champ d'application du réseau santé en ligne sera élargi sous l'impact de la pandémie de Covid [786], mais sans modifier les points précités. On pourrait qualifier le dispositif de l'article 14 de « généraliste », au regard de l'article 12, dédié à la prise en charge spécifique par une infrastructure dédiée, **cette fois sous la responsabilité de la Commission**.

2. Le partage appelé par la mutualisation d'une expertise dispersée, sous la responsabilité de la Commission européenne (article 12)

Si l'article 14 vise à organiser un *continuum* informationnel par le réseau « santé en ligne » sous la responsabilité essentiellement des Etats membres, l'article 12 institue le concept de « *réseau européen de référence* » (RER) pour la prise en charge de maladies rares ou complexes. Le but est de mutualiser à l'échelle européenne une expertise souvent dispersée pour ces maladies de prévalence faible [787]. A cette fin, l'article 12 enjoint à la Commission d'aider les États membres à créer des réseaux européens de référence (RER) entre prestataires de soins de santé et centres d'expertise. Mais **cette fois, la responsabilité est essentiellement celle de la Commission européenne.**

Son article 12§4 prévoit qu'elle devra arrêter, par voie d'acte délégué, une liste de critères et de conditions spécifiques permettant d'instituer les RER, faciliter les échanges par ces « réseaux virtuels », et concentrer la connaissance pour une assistance optimale aux patients

[786] Complété notamment d'un h) ***fournir des orientations*** *aux États membres en ce qui concerne l'échange transfrontière de données à caractère personnel entre les applications mobiles nationales de suivi de contacts et d'alerte par l'intermédiaire de la plateforme de fédération* ». Décision d'exécution (UE) 2020/1023 de la Commission du 15 juillet 2020 modifiant la décision d'exécution (UE) 2019/1765 en ce qui concerne l'échange transfrontière de données entre les applications mobiles nationales de suivi de contacts et d'alerte dans le cadre de la lutte contre la pandémie de COVID-19.

[787] Sur les autres aspects, voir la Recommandation 2009/C 151/02 du Conseil du 8 juin 2009 relative à une action dans le domaine des maladies rares (dont la prévalence est inférieure à 1/2000, ce qui signifie que seul une personne sur 2000 est potentiellement concernée).).

dispersés dans l'Union. Le premier acte sera pris en 2014 [788] puis modifié en 2019 (pour une mise en œuvre effective avec les premiers résultats opérationnels en 2017 [789]).

Ce retard peut s'expliquer par l'absence d'infrastructure dédiée [790]. En 2019, la modification institue un « *système de gestion des données cliniques des patients* » (Clinical Patient Management System, CPMS) fourni par la Commission qui en est responsable, y compris de la gestion des droits d'accès aux membres du RER : cela **consacre une autonomie du système par rapport au réseau en ligne**.

Mais l'autonomie qui nous intéresse ici, est l'institution de dispositions spécifiques aux données pouvant être échangées par le **CPMS créé par la Commission**. L'acte de 2019 introduit plusieurs articles qui en établissent les bases. Or, alors qu'entre temps le RGPD qui définit la notion de « donnée de santé » a été adopté (2016) et est entré en vigueur (2018), les articles ajoutés, retiennent une **conception étonnante du périmètre des données** [791]**.**

* L'article 16bis institue le CPMS afin d'héberger et partager des informations en confiance de façon spécialement sécurisée, il comprend aussi un visionneur d'images médicales pour une « *communication en temps réel et opportun sur des cas de patients au sein des RER* ». Mais alors que cet article est très court, son §1 évoque la gestion des « *données cliniques des patients* » et dans la même phrase, des « *données à caractère personnel concernant les patients* » **(expression utilisée… pour expliciter la précédente !)** ; dans son §2, il définit le CPMS comme un outil sécurisé [792] pour le partage et hébergement de données « *sur les patients* », tandis que son §3 énonce dans son contenu des « *ensembles de données personnalisés* ». Il s'agit là de variantes dans les redondances.

* En outre, l'article 16ter est titré « *Données à caractère personnel traitées dans le CPMS* » dispose que (§1) « *les données à caractère personnel des patients, consistant en leur nom, leur sexe, leurs date et lieu de naissance* ***et en d'autres données à caractère personnel, qui sont nécessaires à des fins de diagnostic et de traitement,*** *sont échangées et traitées au sein des RER exclusivement par l'intermédiaire du CPMS*. ***Le traitement de ces données est limité***

[788] Décision d'exécution 2014/287/UE de la Commission du 10 mars 2014, établissant les critères de mise en place et d'évaluation des réseaux européens de référence et de leurs membres et de facilitation des échanges d'informations et de connaissances liées à la mise en place de ces réseaux et à leur évaluation.
[789] Third Conference on European Reference Networks, 9-10 mars 2017, Vilnius.
[790] Décision d'exécution (UE) 2019/1269 de la Commission du 26 juillet 2019
[791] Du fait de l'entrée en vigueur du RGPD qui définit les « données de santé », le CPMS n'est plus placé sous l'empire de la directive 95/46/CE qu'il a remplacé, et qui ne les définissait pas.
[792] La Commission s'institue en responsable des accès, réservés aux « prestataires de soins de santé membres d'un RER », les « partenaires affiliés » ou les « utilisateurs invités ».

aux finalités suivantes » qui sont la collaboration médicale, l'inscription sur les registres, et la prise de contact pour une éventuelle participation à des recherches.

Comment expliquer ces circonvolutions ?

On ne peut dire que ce « paramétrage » par les articles 16bis et 16ter soit une réponse aux observations du CEPD, lequel, à l'examen du projet de la directive de 2011, avait regretté que les références à la protection des données « *(soient) surtout de nature générale et ne reflètent pas adéquatement les besoins et les exigences spécifiques en matière de respect de la vie privée qui découlent des soins de santé transfrontières* » [793].
Pourrait on y voir **une tentative de caractériser le « *lien manifeste et étroit* *avec la santé* »**, qualification adoptée en 1997 par le Conseil de l'Europe [794], reprise en 2007 par le GT de l'article 29 dans l'Union [795], avant d'être abandonnée par l'adoption du RGPD, nous l'avons vu en introduction de notre thèse ?

En fait, l'enjeu apparaît dans les considérants de l'acte de 2019, qui d'abord énonce plusieurs truismes « *Le CPMS traite des données sensibles relatives aux patients atteints de maladies complexes rares ou à faible prévalence. Ces données sont traitées uniquement aux fins de faciliter le diagnostic et le traitement des patients ».* Puis il enchaîne avec l'introduction d'une dimension nouvelle : *« de les inscrire dans des registres pertinents ou d'autres bases de données dédiées aux maladies complexes rares ou à faible prévalence* (qui) *servent la recherche scientifique ou des objectifs cliniques ou de politique de santé, et* (à) *prendre contact avec des patients pour leur éventuelle participation à des initiatives de recherche scientifique* » (consid. n°11). **Or, cela préfigure l'usage secondaire, notant qu'«** *il convient que le consentement soit obtenu* ***séparément pour chacune de ces trois finalités*** » (*ibid*).

Ces circonvolutions des articles 16ter et 16quater contrastent avec l'approche unitaire de la notion de « donnée de santé » adoptée entre-temps par le RGPD. Elles peuvent s'expliquer par le fait que, à la différence du réseau de l'article 14, cette infrastructure dédiée **dépend de la Commission, non des Etats membres** (article 16ter §2). Cela conduit à un énoncé prudentiel du champ des données concernées pour un usage limitatif, d'autant que **pointe déjà la question d'utilisations des données qui ne seraient plus des utilisations primaires.**

---

[793] Consid n°8, Projet d'avis du contrôleur européen de la protection des données, préc. (2009/C 128/03).
[794] Recommandation n° R (97) 5 du Comité des ministres aux Etats membres relative à la protection des données médicales, adoptée le 13 février 1997.
[795] « Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques », février 2007, WP 131, point II.2.

B. LA PETITION D'UN PARTAGE ELARGI DES « DONNEES DE SANTE » A L'ECHELLE EUROPEENNE

De façon classique, cette pétition est fondée sur le constat que l'action seulement volontaire portée par la directive 2011/24 (UE) conduit à une « *fragmentation* » des mises en œuvre nationale. Ce terme est récurrent ; mais n'est-il pas discutable, puisqu'une fragmentation postule une unité qui aurait été perdue ? **L'absence d'unité préexistante** nous incline à constater plutôt une dispersion des pratiques nationales, que le droit européen entend pallier lorsqu'elles affectent les buts du Traité.
Esquissons les limites rencontrées quant aux « utilisations primaires » des données de santé dont on aura pu relever les limites (1), et quant aux utilisations secondaires dont la légitimité est alors à caractériser (2).

1. Cas des données pour utilisations primaires : limites rencontrées

Il n'est pas lieu de paraphraser ici les études d'impact très documentées (4 volets) réalisées sous l'égide de la Commission européenne [796], à l'appui de la formulation en 2022 de la proposition de règlement dédié à l'espace européen des données de santé, *infra*.

Sur le plan technique, la variété des infrastructures nationales, leur faible interopérabilité, la viscosité des échanges de données, la charge administrative et le gaspillage de ressources (redondance d'examens d'imagerie, de biologie etc. par défaut d'accès) sont un problème structurel. Ces problèmes **ne sont pas propres à l'échelle européenne, le défaut d'interopérabilité des systèmes étant en soi un enjeu national** [797]. Un obstacle particulier vient de ce que la directive de 2011 n'exige pas que le dossier médical soit fourni sous forme électronique (type dossier médical électronique, DME). Afin de renforcer l'interopérabilité, le réseau a ainsi recommandé que dans leurs marchés publics, **les États membres recourent aux spécifications du format européen** d'échange des DME, *infra*.

[796] Commission staff working document, « iImpact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council on the European Health Data Space » (COM(2022)197final), disponibles sur https://health.ec.europa.eu/publications/impact-assessment-european-health-data-space_en
[797] Voir les importants travaux réalisés en France sous l'égide de l'Agence du numérique en santé (ANS).

Sur le plan politique, la base volontaire d'implication des Etats membres dans le réseau « Santé en ligne », leur responsabilité juridique du déploiement et des traitements, *supra*, l'importance des investissements requis pour des usages variables selon le taux d'implication dans les soins transfrontières [798], peuvent aussi expliquer l'impact limité de la directive de 2011 sur le renforcement de l'accès et du contrôle et donc de la portabilité de leurs données de santé électroniques par les patients intéressés.

Ainsi, seuls 10 Etats ont mis en œuvre la plateforme MaSanté@UE (dont la France où le système est porté par l'ANS) [799], laquelle ne prend en charge en 2022 que deux services (prescription électronique et dossiers de patients). **Soulignons ici la forte impulsion donnée par la Délégation au Numérique en Santé** créée en 2019, qui a permis à la France, non seulement de rattraper son retard au regard de ses voisins, mais de reprendre de l'avance ! [800].

Mais à ces éléments, nous semblent s'ajouter ceux liés à la difficultés du paramétrage des données primaires partageables, dont nous avons vu les atermoiements tant sous l'article 12 que sous l'article 14 de la Directive. Le tout aboutit à la proposition, en 2022, de « ***Catégories prioritaires de données de santé*** *électroniques à caractère personnel à des fins d'utilisation primaire »* [801], que nous développerons *infra*.

Nous reproduisons ci-dessous une partie, **volontairement tronquée,** d'un des tableaux présentés dans l'analyse d'impact, titré « *Table 2. Overview for primary uses of health data (covering mainly SO1 and SO2) »* [802]. Il articule la réflexion autour de deux objectifs : Les SO1 et SO2 désignent les « objectifs spécifiques » 1 et 2.

- le SO1 vise l'autonomie des citoyens, grâce à un contrôle accru de leurs données de santé personnelles, et leur liberté de leur libre circulation assurée assurés que les données de santé les suivent.
- le SO2 vise à « *Libérer l'économie des données en favorisant un véritable marché unique des services et produits de santé numériques* » [803].

---

[798] Voir les études précitées, publiée en juin 2023 « Data on cross-border patient healthcare following Directive 2011/24/EU Reference year 2021 » ; auparavant en mai 2022, « Data on patient mobility under Directive 2011/24/EU - Trend report reference years 2018-2020 » (disponibles sur le site de la Commission).
[799] Porté par l'Agence du Numérique en Santé (ANS), le service Sesali.fr permet aux professionnels de santé d'accéder aux synthèses médicales de citoyens européens.
[800] Voir ANS, « La doctrine du numérique en santé » (2022, publiée en fév. 2023), p. 3s.
[801] Article 5 de la proposition de règlement EESD mai 2022, préc.
[802] Préc., volet 1, voir page 33.
[803] Ibid., page 30.

Sa colonne « *baseline* » rapporte les constats initiaux, lesquels valent tout à la fois bilan, et pétition, pour ce qui est des usages primaires, avant d'ouvrir 3 options politiques qu'il n'est pas lieu de développer ici :

Measure/ dimension	**Baseline: Voluntary cooperation**	**Policy Option 1: EU coordinatior regulatory meas**
Individuals' and health professionals' access and control over health data (SO1)	General provisions in the GDPR and Data Act, no specificities for health	Guidelines for co data
Scope of data domains (SO1, SO2)	Guidelines on interoperability of data domains in the European electronic health record exchange format (EEHRxF)[clvi]	Guidelines on EE data domains (e.g
Quality and interoperability requirements	-Requirements established nationally - Guidelines/recommedations focusing on interoperability of data domains for EEHRxF, and on identity management	-Same as in Base -Guidelines on in data domains for other digital heal identity managen -Voluntary qualit interoperability o digital health pro wellness applicat
Cross-border health data sharing (SO1, SO2)	Voluntary deployment of MyHealth@EU; Guidelines	Same as in Basel
Governance and EU cooperation (SO1, SO2)	Voluntary cooperation of national digital health authorities (eHealth Network)	Mandatory netwo digital health autl (strengthened eH

2. Cas des données pour utilisations secondaires : légitimité à caractériser

Les difficultés en matière d'utilisations secondaires sont également décrites dans les études d'impact. Le tableau de bilan titré « ***Table 3. Overview for secondary use of health data (covering mainly SO2 and SO3)*** » [804] est suffisamment éclairant. L'objectif spécifique 3 (OS3) vise à assurer un cadre cohérent et efficace pour la réutilisation des données de santé des individus pour la recherche, l'innovation, l'élaboration de politiques et les activités réglementaires [805]. Sa colonne *baseline* établit le bilan valant pétition.

[804] Ibid. préc. p 34.
[805] Ibid., page 30.

Measure/ dimension	**Baseline: No EU cooperation framework**	**Policy Option coordination measures**
Reusers' access to health data (researchers, innovators, policy-makers and regulators) (SO3)	Multitute of regimes: national legislation or consent; EDPB guidelines on research	Same as in Ba Guidelines on
Types of data in scope for reuse (SO3)	Defined in separate national legal bases; GDPR and Data Act	Same as in Ba Guidelines on and on volunta
Data altruism (SO3)	Data Governance Act (DGA) applies	Same as in Ba
Digital infrastructure for secondary uses (SO3)	- Possible disease-specific infrastructures; - No common EU infrastructure	Extend (MyHe uses of health Guidelines for infrastructure
Data quality (SO3)	No common data quality standards and labels	Voluntary lab Codes of conc
Support for AI development and verification (SO3)	Access to health data for development of AI technology based on separate national legal bases	Codes of conc 69 of AIA
Governance and EU cooperation (SO2, SO3)	-Separate governance frameworks focused on specific initiatives -Health Data Access Bodies in some Member States as national governance bodies for health data reuse	Voluntary coc national Healt (Health Data

En revanche, il nous semble intéressant de remonter le temps, pour voir la perception du phénomène lors du contrôle du projet de directive présenté en 2008 (qui deviendra la directive 2011/24). Le CEPD y exprime une préoccupation particulière quant à l'article 18, qui traite alors de la collecte à des fins statistiques et de suivi au profit de la Commission.

Dans le sillage de sa critique (*supra*) de la notion de « donnée de santé », le CEPD relève alors que l'article 18§1 **mentionne des « données statistiques *et autres données supplémentaires* »,** définies par la finalité du suivi qu'il met en exergue : le suivi porte sur un champ large quant à la prestation de soins de santé transfrontières ; il englobe le contenu des soins dispensés, les prestataires et les patients, les coûts et les résultats.

S'il n'est pas surprenant que la Commission européenne, gardienne exécutive du Traité, souhaite disposer de telles données, pour évaluer d'un point de vue quantitatif et qualitatif les modalités de prestation transfrontière (et d'éventuels dysfonctionnements du marché intérieur par pratiques discriminatoires proscrites par le Traité et la norme spécifique), le projet se contente d'invoquer la législation alors existante sur la protection des données (directive 95/46/CE) ; cela **sans ajouter d'exigence spécifique quant à une utilisation secondaire.**

Or, l'article 8§4 de la Directive pose le principe selon lequel **seul un motif d'intérêt public important pourrait conduire les Etats** à prévoir des dérogations autres que celles du §2 (intégrant le consentement et les applications médicales), par leur législation nationale ou sur décision de l'autorité de contrôle, et à la condition de garanties appropriées. **En l'espèce, de telles exigences spécifiques n'ont pas été explicitement énoncées**.

En outre, l'article 18§2 du projet prévoyait une obligation inconditionnelle de transférer un grand volume de données à la Commission au moins une fois par an.

Or, la condition de l'article 8§4 de la directive 95/46/CE **n'apparaît pas non plus ici satisfaite,** dans la mesure où « *aucune évaluation de la nécessité de ce transfert n'est mentionnée expressément, il semble que le législateur communautaire ait déjà établi lui-même cette nécessité* » [806] **sans la caractériser, ce qui ne permet pas d'établir de façon objective l'intérêt public important** auquel renvoie l'article 8§4 comme condition de traitement distinct du but primaire.

Dès lors, tout comme le CEPD invite à introduire une définition des « données relatives à la santé » selon une acception large (point 1), et à introduire un article spécifique sur la protection des données (point 2), il invite à clarifier la notion d'« autres données supplémentaires », et à spécifier les conditions d'utilisation ultérieure de telles données pour une fin non primaire (point 5). Enfin, il considère alors acceptable une obligation de transmettre ces données à la Commission, mais nécessaire, dans ce cas, que **l'obligation de transfert par les Etats soit assortie d'une obligation d'évaluation par la Commission, de la nécessité de ces transferts** pour des « *fins légitimes dûment précisées à l'avance* » [807].

[806] Avis CEPD préc., point 41.
[807] Ibid., 48.

Du fait des limites de la compétence de la Commission, il s'agit ici pour elle, par l'analyse statistique, de s'assurer du fonctionnement correct du marché intérieur. Cette application là est très limitée, **au regard de l'extension considérable des usages secondaires des données de santé** telle que prévue par les projets de textes ultérieurs, depuis notamment 2022, *infra*.

§2. LA DYNAMIQUE NORMATIVE DE COORDINATION DES ACTIONS DES ETATS MEMBRES DE L'UNION

Distinct du *continuum* informationnel pour des soins transfrontières à des patients individuellement considérés, la coordination en matière d'anticipation/réaction des Etats en matière de santé est un enjeu transfrontière mondial. Elle a été l'objet d'un règlement sanitaire international adopté sous l'égide de l'OMS, dont sont membres tous les Etats de l'Union [808].

Le droit européen devait ainsi **tenir compte de cette approche intégrée « tous risques » de l'OMS**, laquelle couvre toutes les catégories de menaces : naturelle ou humaine, accidentelle ou volontaire, dont terroriste (chimique, biologique, radiologique, cyber etc.), et les conséquences de conflits armés. Le but est de **renforcer la coordination de la préparation et de la réaction des Etats** aux urgences de santé publique de portée internationale.

En ce sens, depuis la directive 95/46/CE qui visait la protection des données personnelles, le dispositif européen monte en puissance, avec pour **premier souci de coordonner les comportements en situation de crises transfrontières**, lesquelles au regard du droit de traitement des données, constituent des « *motifs d'intérêt public caractérisé* » (A). Le corollaire est la centralisation de l'information pour une finalité de décision (B).

[808] Règlement sanitaire international (2005) (RSI), adopté le 23 mai 2005 par la cinquante-huitième Assemblée mondiale de la santé. Troisième édition en 2016.

A. COORDONNER LES COMPORTEMENTS EN SITUATION DE CRISE TRANSFRONTIERE

La surveillance épidémiologique et de contrôle des **maladies a été l'objet d'un réseau dédié mis en place à partir de 1998** par décision du Parlement européen et le Conseil [809], avant que son champ d'application soit en 2013 significativement étendu (l'extension sera encore plus significative en 2022 à la lumière de la crise, nous verrons cela *infra*).

En effet, le champ de cette décision organisant la surveillance, l'alerte précoce et la lutte, est alors restreint aux maladies transmissibles. **Il a du être élargi** à **« *d'autres agents biologiques ou chimiques, ou événements environnementaux* »** pouvant perturber des secteurs sociaux et économiques critiques, et obérer la capacité individuelle de réaction des États membres [810]. En outre, un **« comité de sécurité sanitaire »** (établi sur la base des conclusions de la présidence du Conseil du 15 novembre 2001 sur le bioterrorisme) **a été institutionnalisé.** Ce qui nous intéresse ici à nouveau, est la place des données à caractère personnel dans ce texte.

1. une soumission des données au droit commun

La décision de 2013 (article 16) prévoit que les données à caractère personnel sont traitées conformément à la directive 95/46/CE (source d'obligation pour les Etats membres), abrogée par le RGDP 2016 ; et au règlement (CE) n°45/2001 (source d'obligation pour les institutions de l'Union) [811], abrogé par le règlement (EU) 2018/725.

Il n'est pas lieu ici d'y revenir ; mais on relèvera dès ici que l'article 16§1 prévoit que « *En particulier, des mesures techniques et d'organisation appropriées sont prises pour protéger ces données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle* ***ou l'accès non autorisé, ainsi que contre toute autre forme de traitement illicite*** ». On verra le développement fort depuis, des approches européenne de cybersécurité, le champ des données de santé et les tableaux de bord des décideurs publics étant devenu un domaine d'ingérence critique à très fort impact, sanitaire mais également politique.

Cette adjonction à l'article 16§1 est frappante, puisque de telles mesures **doivent être prises indépendamment du contexte d'usage. Dès lors, leur invocation expresse ici vaut obligation renforcée.** Cela s'explique par l'échelle de traitement de la donnée au titre du

[809] Décision n°2119/98/CE du Parlement européen et du Conseil.
[810] Considn°3, Décision n°1082/2013/UE préc.
[811] Règlement (CE) n° 45/2001 préc.

système d'alerte précoce et de réaction, lequel ne relève plus d'un usage primaire des données de santé, **ni d'un usage purement national :** le risque de pollution informationnelle, voire de manipulation informationnelle à impact systémique, est collectif.

2. une communication des données à géométrie variable

La décision n° 2119/98/CE avait institué un système d'alerte précoce et de réaction (SAPR), absorbé depuis par le Centre européen de prévention et de contrôle des maladies (ECDC), *infra* [812]. Le SAPR **a été étendu à toutes les menaces transfrontières graves**. Cette plateforme d'information entre Etats membres (article 7) est un outil de notification d'alertes : il doit permettre la communication rapide de « *toute donnée pertinente disponible qui peut être utile pour la coordination de la réaction, telle que (...) i**) les données à caractère personnel requises** aux fins de la recherche des contacts conformément à l'article 16 ».*

* Ce qui nous intéresse ici, est que le SAPR est défini comme incluant une fonctionnalité de messagerie sélective. Celle-ci vise la communication de ces données aux (seules) autorités nationales concernées **par des mesures de recherche des contacts entre les personnes** pouvant être affectées par l'agent pathogène. Le critère de licéité de leur transmission est la « *nécessité* » au sens de l'article 9§3 précité. Or, cette nécessité est **strictement entendue** (nous le comparerons avec l'approche retenue depuis la pandémie de Covid19).

* En outre, l'article 16§6 dispose qu'une notification effectuée par une autorité compétente peut s'avérer contraire aux dispositions de la directive 95/46/CE « *du fait qu'(elle) n'était pas nécessaire à la mise en œuvre des mesures de recherche des contacts* » – ***a posteriori*** **donc, ce qui implique la responsabilité de l'autorité nationale** quant à l'obligation de notifier et rectifier les données par l'intermédiaire du SAPR (ibid., §7), **et de la Commission européenne** quant à leur stockage à ce titre (ibid., §8). Quelle peut être l'étendue d'une éventuelle communication intempestive sur les données ?

L'article 16§9 dispose que la Commission « *adopte (...) une recommandation contenant une **liste indicative des données à caractère personnel** qui peuvent être échangées aux fins de la coordination des mesures de recherche des contacts* ». Il en résulte qu'en principe, un nombre

[812] Adoptée avant le règlement (CE) n°851/2004 du Parlement européen et du Conseil du 21 avril 2004 instituant un Centre européen de prévention et de contrôle des maladies, *infra*.

certes très limité de données pré-identifiées pourrait être communiqué par le biais du SAPR, mais que la liste recommandée par la Commission ne possède qu'un caractère indicatif.

Dès lors, **il est loisible aux autorités nationales compétentes de notifier plus, ou moins,** de données à caractère personnel dans le but de recherche de contacts dans ces circonstances. **L'approche est donc à géométrie variable** (on comparera avec le droit adopté après la pandémie de Covid19), ce qu'explique l'anticipation d'une susceptibilité potentielle des personnes et des systèmes nationaux quant à ces partages inédits.

B. CENTRALISER LES INFORMATIONS POUR COORDONNER LES ACTIONS

Dans un second temps, le règlement (CE) n°851/2004 matérialise lui l'ambition de la Communauté européenne de protéger et améliorer la santé humaine en prévenant notamment les maladies transmissibles [813], lesquelles peuvent aussi résulter de la dissémination volontaire d'agents pathogènes donc de bioterrorisme.

Au-delà du SAPR, lequel fonctionne en mode réseau, il institue alors le Centre européen de prévention et de contrôle des maladies (pendant européen du CDC fédéral aux Etats-Unis). Mais ce centre **n'est pas censé traiter à titre ordinaire de données personnelles**.

1. la condition d'impact (avéré ou potentiel) communautaire

En cas spécialement d'épidémie / pandémie, qui par définition ignorent les frontières dans une économie globalisée, marquée par une grande fluidité des déplacements (*a fortiori* dans l'espace intracommunautaire, notamment de régime « Schengen »), une réaction efficace pour protéger les populations **postule une approche cohérente pour la préparation et le contrôle**.

Eu égard à la diversité des actions essentiellement publiques pouvant être requises à grande échelle, ce règlement met en exergue un impératif qui est en fait, à ce stade, une pétition : « *la communauté **devrait disposer d'un vaste champ d'action*** » (considérant n° 2) ; vaste champ d'action encore putatif : sa théorisation figure parmi les fondements invoqués du Règlement n°851/2004, **mais n'est pas un apport normatif de ce dernier**.

[813] Règlement (CE) n° 851/2004 du Parlement européen et du Conseil du 21 avril 2004 instituant un Centre européen de prévention et de contrôle des maladies.

Si les Etats devaient déjà communiquer les informations sur les maladies transmissibles par des structures *ad hoc*, appuyés sur une densification des réseaux de surveillance spécialisés des maladies transmissibles [814], le règlement **institue un interlocuteur institutionnel voué à la centralisation de l'information et au dialogue international** selon des procédures ad hoc, qui prend la forme d'une Agence émanation des institutions européennes : le Centre européen de prévention et de contrôle des maladies.
Ce dernier **endosse la responsabilité de la surveillance épidémiologique** des maladies transmissibles et de l'exploitation du système d'alerte précoce et de réaction (SAPR, précité).

Le Centre vise l'aide à la décision (avis, assistance, études et expertise indépendants), à la demande de la Commission, du Parlement européen ou d'un Etat membres, ou de sa propre initiative (article 7). Il dispose d'une autonomie budgétaire et d'une certaine marge de manœuvre (« *déceler et évaluer les menaces* ***susceptibles de se propager sur le territoire ou jusqu'au territoire de la Communauté »***). Il peut refuser ou proposer un demande d'avis, en cas de demande non claire ou non conforme au 7§2 : toute demande auprès de lui doit être accompagnée « *d'informations générales expliquant le problème scientifique à traiter* ***et l'intérêt communautaire*** », afin de ne pas risquer l'embolie sous l'effet de multiples demandes nationales d'intérêt territorial circonscrit.

Mais le Centre **ne possède aucun pouvoir réglementaire** : pour toutes conséquences de ses avis, il doit dialoguer avec l'autorité compétente décisionnaire (essentiellement nationale, accessoirement communautaire).
De même, il peut dialoguer avec des Etats non membres de l'Union, selon des accords qui supposent la réciprocité sur la base d'une transposition et d'une mise en œuvre des acquis communautaires dans le domaine concerné (article 30).

2. L'exception du traitement des données personnelles

Le Règlement ne prévoit **aucune transmission de données personnelles de santé**. Son article 4, qui traite des obligations des Etats membres, prévoit seulement que ces derniers « *fournissent en temps utile au Centre les* ***données scientifiques et techniques dont ils disposent et qui présentent un intérêt pour sa mission*** », en sus de l'obligation de

[814] Désignés selon l'article 4 de la décision n° 2119/98/CE du Parlement européen et du Conseil du 24 septembre 1998 instaurant un réseau de surveillance épidémiologique et de contrôle des maladies transmissibles dans la Communauté

communication de messages résultant du SAPR, et de l'identification de la ressource nationale (institutionnelle et personnelle) pouvant être mise à disposition du Centre.

Ainsi, l'article 11, qui traite de la Collecte et analyse des données, prévoit que le Centre « *coordonne la collecte, la validation, l'analyse et la diffusion des données au niveau communautaire* » ; la dimension statistique de la collecte **devant être développée en coopération avec les Etats membres** *(supra)*.

A cette fin, des « *procédures appropriées* » sont mises au point avec les organismes nationaux et la Commission, « ***pour faciliter la consultation, la transmission des données et l'accès à ces données*** » (article 11§2), sachant que les données mises à disposition doivent être objectives et viables, puisqu'elles peuvent être le fondement de décisions d'impact fort pour les populations au plan national (*infra*).

Certes, l'article 4 n'évoque pas de traitement ni de communication de données personnelles de santé.

Mais son article 20 n'en prévoit pas moins que cela puisse **par exception être** « ***absolument nécessaire à l'accomplissement de la mission du Centre*** » (article 20§4). Cela soumet à nouveau ces données aux règles de protection des données personnelles à l'égard des traitements par les institutions et organes de l'Union alors en vigueur [815]. De tels cas peuvent être justifiés par la connaissance nécessaire de circonstances d'exposition de personnes (dont des modes d'action bioterroristes, qui peuvent initialement s'appuyer sur des vecteurs humains sélectifs, à identifier et tracer) ; ou de réponses personnelles voire populationnelles différenciées aux « antigènes » (dont la personne agressée se défend par sa propre production immunologique, à défaut par l'administration / la stimulation externe d'« anticorps »).

La réserve de l'« absolue nécessité » a un caractère ici essentiellement politique dans le dialogue avec les Etats : en tant qu'organe communautaire, le Centre est en tout état de cause tenu à la protection des données personnelles par les textes dédiés ; le problème ne tient pas tant ici à la protection de la donnée (susceptibilité individuelle), **qu'aux conséquences d'une centralisation de telles données** dans un champ de subsidiarité (susceptibilités nationales).

[815] Règlement (CE) n°45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

En outre, la matière étant sensible – que le risque sanitaire soit d'origine naturelle, accidentelle ou intentionnelle de type terroriste, le règlement énonce une obligation de confidentialité quant aux informations dont « *un traitement confidentiel* ***a été demandé et justifié*** », « *sans préjudice de l'article 20* » (*ibid.*, article 21).

Le but, en phase d'analyse des données avant validation des informations et de proposition d'actions coordonnées, est naturellement **d'éviter par la médiatisation intempestive d'informations incertaines, la déstabilisation panique** de la confiance publique, du fonctionnement d'institutions, d'entreprises ou des marchés [816].
Ce point est nous l'avons vu fondamental pour la souveraineté politique.

SECTION 2. ACCELERATEUR DE LA COVID19 : LA MISE EN EXERGUE DE L'INTERDEPENDANCE SYSTEMIQUE

En 2020, la pandémie de Covid19 qui après la Chine, a frappé l'Europe puis le monde entier, a été un accélérateur fort d'adoption de mesures parfois drastiques, fondées sur un usage abondant des outils numériques générant et consommant des données personnelles de santé.

En 2021, un rapport au Sénat a inventorié les politiques des Etats quant à la place et au partage des données personnelles (de santé/non, individuelles/de masse) en Chine, Corée du Sud, Taïwan, Singapour, Hong-Kong, Japon ; puis dans d'autres pays touchés en seconde ligne, notamment dans l'Union européenne. Les premières réponses **y ont été fragmentées pour motifs parfois de souveraineté** en l'absence, en tous cas, d'un mécanisme collectif immédiatement opérationnel *et* pouvant convaincre des opinions et décideurs inquiets [817].

Rappelons ici que, au début de la crise, et même après sa qualification officielle par l'OMS de pandémie [818], les connaissances détenues quant aux causes d'apparition et mode de propagation du virus, sa virulence et son potentiel mutagène, sa létalité potentielle, **étaient très parcellaires et discutées**.

---

[816] En revanche, les « conclusions des avis scientifiques en rapport avec des effets prévisibles sur la santé ne peuvent (…) être tenues confidentielles » (article 20§3).
[817] V. Guillotin, C Lavarde, R-P. Savary, Rapport d'information fait au nom de la délégation sénatoriale à la prospective sur les crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés, Sénat, rapp. n° 673, enregistré à la présidence le 3 juin 2021.
[818] Le directeur de l'OMS a déclaré le 30 janvier 2020 une urgence de santé publique de portée internationale ; mais l'OMS n'a publié une évaluation qualifiant la COVID-19 de pandémie que le 11 mars 2020.

En 2023, les causes de son apparition, et la transparence quant aux conséquences initiales en Chine, restent discutées ; cela est d'ailleurs un point de crispation entre Etats, et **stimule d'autant l'adoption accélérée de mesures en leur sein et entre eux**, **selon leur degré d'interdépendance et de communauté politique** (puisque se repose la question des droits fondamentaux des personnes et des libertés publiques, en contexte de tension géopolitique).

Nous relevons donc ici – pour ce qui est de l'espace politique européen – la dynamique normative **de réaction** à la crise provoquée par la pandémie (§1), avant de relever la dynamique normative **d'anticipation** de crises futures (§2). Elle vise à tirer leçon de l'expérience 2020/2021, considérant un spectre d'actions publiques vastes qu'antérieurement, et **selon des modalités renouvelées quant à l'usage des données**, point qui nous intéresse.

§1. LA DYNAMIQUE NORMATIVE DE REACTION A LA CRISE SANITAIRE DANS L'UNION EUROPEENNE

L'ensemble du système européen préexistant, dont le SAPR et le CEPCM (*supra*), a été sollicité. **Cela n'était pas suffisant**.

Nous relevons ici l'activation du système de gestion des données cliniques, qui intéresse directement les données de santé (A) ; puis l'institution d'un certificat européen visant à restaurer la liberté de circulation intracommunautaire, lequel suppose le traitement de données personnelles **éclairant le statut vaccinal** notamment (B).

A. ADAPTATION DU SYSTEME DE GESTION DES DONNEES CLINIQUES TRANSFRONTIERES

En application de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011, relative à l'application des droits des patients en matière de soins de santé transfrontaliers, la décision d'exécution (UE) 2019/1269 de la Commission avait, dès avant la pandémie de Covid19, établi un système **de gestion des données cliniques transfrontières**, qui vise dans un champ étroit à mutualiser des données de santé (1).

Avant toujours la pandémie de Covid19, ce système est la même année complété d'un réseau élargi appelé « Santé en ligne » (*supra*) d**ont le but n'est pas la mutualisation des données, mais l'interopérabilité des systèmes** (2).

1. Mutualisation par un système de gestion transfrontière de données cliniques

La décision d'exécution (UE) n°2019/1269 établit un système de gestion des données cliniques transfrontières, et modifie à cette fin la décision d'exécution (UE) 2014/287 qui avait établit les critères de **mise en place et d'évaluation des réseaux européens de référence (RER)** ; nous n'avons pas précédemment cité ces critères, car ils échappent à notre sujet, centré sur le partage européen de données de santé jusqu'alors jalousement gardées.

Notons seulement que cette décision 2014/287 prévoyait que, afin de promouvoir le partage d'expériences et favoriser la cohérence avec d'autres échanges transfrontières de données médicales (ceux visés par la Directive 2011 préc.), un conseil *ad hoc* des Etats membres pût orchestrer une coopération étroite avec le réseau santé en ligne, **dans le but d'approches communes en ce qui concerne les structures de données notamment**. Tout cela repose au premier chef sur la confiance réciproque, nous ne reviendrons pas ici ce point crucial [819].

Ce qui nous intéresse ici est à cette fin, l'insertion en 2019, dans la décision d'exécution 2014/287, des nouveaux articles 16bis, 16 ter et 16 quater **entièrement dévolus aux données de santé, et complétant ce point absent du dispositif antérieur**, lequel pour la coopération s'appuyait sur la jonction des ressources étatiques. Le 16 quater posant un principe de responsabilité conjointe des traitements, seuls nous intéressent les 16 bis et 16 ter.

* L'article 16bis institue le système de gestion des données cliniques des patients (CPMS), voué à l'échange de données à caractère personnel et restreignant l'accès aux seuls prestataires autorisés à y accéder au sein des réseaux européens de référence. Le CPMS y est présenté comme un « *outil informatique sécurisé,* ***fourni par la Commission, pour le partage et l'hébergement de données sur les patients*** *et pour la communication en temps réel et opportun* ***sur des cas de patients au sein des RER*** » (article 16 bis §2).

* L'article 16ter prévoit que les données personnelles des patients concernés, en tant qu'elles sont nécessaires aux fins de diagnostic et de traitement, sont alors « échangées et traitées au sein des RER (réseaux européens de référence) **exclusivement par l'intermédiaire du CPMS** », pour des **finalités limitatives** : « *faciliter la collaboration sur l'évaluation médicale*

[819] Les considérants n° 3 et n°4 de la décision 2019/1269 sont parfaitement explicite, et restituent le partage d'expérience de la mise en œuvre des dispositifs initiaux.

du dossier d'un patient à des fins de diagnostic et de traitement, inscrire les données dans des registres et autres bases de données dédiés à des maladies complexes rares ou à faible prévalence (…) et prendre contact avec des patients pour leur éventuelle participation à des initiatives de recherche scientifique ».

Or, la Commission est alors **responsable du traitement**, et « ***n'accède pas aux données à caractère personnel des patients, sauf si elle a impérativement besoin d'un tel accès pour*** *remplir les obligations qui lui incombent en sa qualité de responsable conjoint du traitement »*, sachant l'accès strictement réservé aux seules personnes autorisées par les RER (ce qui module le besoin de connaître des données, *supra* Ière partie).

Son §5 dispose que « *le nom du patient ainsi que le lieu et la date exacte* (sic) *de sa naissance sont* ***cryptés et pseudonymisés*** *dans le CPMS. Les autres données à caractère personnel nécessaires à des fins de diagnostic et de traitement sont* ***pseudonymisées*** ». Nous avons précédemment souligné la difficulté particulière posée pour les maladies rares, du fait du potentiel de ré-identification.

Son §7 pose un principe d'effacement, de la base commune, des données qui ne sont plus nécessaires : « ***les données à caractère personnel des patients ne sont conservées qu'aussi longtemps que*** *cela est nécessaire pour assurer l'administration de soins aux patients, diagnostiquer les maladies ou assurer l'administration de soins aux membres de la famille des patients au sein d'un réseau européen de référence* » [820].
L'article 16ter §7 s'entend **sans préjudice du droit national** quant au délai de prescription médicale, mais ne porte par ailleurs **aucun élément sur le partage des responsabilités quant au diagnostic et traitement** [821] (question potentiellement complexe, en cas de co-élaboration de décisions dans le cadre des RER).

Ainsi, ce système focalisait sur la gestion transfrontière des données **cliniques pour des buts limités**. Il a été rapidement augmenté en contexte de la pandémie de Covid19, au-delà de ce que prévoyaient les textes, pourtant récents, qui visaient la préparation et réponse aux crises.

---

[820] Et de poursuivre que « *Tous les quinze ans au plus tard, chaque prestataire de soins de santé autorisé à accéder au CPMS réexamine la nécessité de conserver les données des patients dont il a la responsabilité du traitement ».*

[821] La nouvelle Annexe III, détaille de nombreux aspects, mais aucun ayant trait à cette responsabilité là.

2. Promotion de l'interopérabilité par le réseau à base volontaire « *Santé en ligne* »

Une autre avancée, qui a précédé et sera fortement accélérée par la crise Covid19 (*infra*), doit être signalée, quant au réseau précité « *Santé en ligne* ». Il est défini comme le « *réseau* ***constitué sur la base du volontariat reliant les autorités nationales*** *chargées de la santé en ligne désignées par les Etats membres* (…) » [822]. En application de l'article 14 de la directive 2011/24/UE précitée, une décision d'exécution de la Commission en décembre la même année, a prévu des règles de création, de gestion et fonctionnement du réseau [823].

* Mais dès octobre 2019 (avant donc, le début de la Crise Covid19), la Commission pointe le caractère incomplet et insatisfaisant de sa décision de 2011 en ce qui concerne notamment **les rôles respectifs du réseau et de la Commission.** A cela, s'ajoute le besoin de transparence quant aux adhésions / retraits des Etats membres du réseau, et sa conformité au regard des nouvelles règles portées par le RGPD – ces deux derniers point ne nous retenant pas ici [824].

Rappelons que le réseau « *Santé en ligne* » vise **à promouvoir, entre les seuls Etats volontaires, une plus grande interopérabilité des systèmes** nationaux de TIC (article 4§1a), en « *fournissant des orientations* » en ce sens (article 4§1 b à h). Il ne consiste donc pas en la mise à disposition d'une infrastructure informatique unifiée qui permettrait la mutualisation de données, et dont la Commission serait responsable. De cette promotion de l'interopérabilité, **résultera une géométrie très variable des engagements étatiques**, jusqu'à donc la pandémie de Covid19, laquelle va provoquer la décision de 2020 (*infra*).

En 2019, la Commission européenne rappelle ainsi que la communication électronique permet « *d'assurer des* ***échanges rapides et fiables de données entre les Etats membres participant*** *au réseau* » (consid. n°5), mais que d'importantes évolutions ont eu lieu en la matière ; des **Etats membres participant au réseau <u>et</u> qui ont décidé de renforcer leur coopération en son sein** (cela crée donc une double couche de géométrie variable) ont mis au point une

[822] Défini par article 2§1, a).
[823] Décision d'exécution 2011/890/UE de la Commission du 22 décembre 2011 arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales responsables de la santé en ligne (JO L 344 du 28.12.2011, p. 48).
[824] Décision d'exécution (UE) 2019/1765 de la Commission du 22 octobre 2019 arrêtant les règles relatives à la création, à la gestion et au fonctionnement du réseau d'autorités nationales chargées de la santé en ligne, et abrogeant la décision d'exécution 2011/890/UE.

infrastructure de services numériques avec un double volet : services transfrontaliers d'information, et outil informatique d'échanges de données sur la santé [825].

Or, cette dynamique aboutit au besoin « ***de préciser le rôle respectif des États membres participants et de la Commission*** *en ce qui concerne le fonctionnement de l'infrastructure de services numériques dans le domaine de la santé en ligne pour les services transfrontaliers d'information sur la santé en ligne* » [826], en faisant jouer un rôle de premier plan au réseau [827].

* Ce faisant, la Commission européenne **s'appuie sur le pilote résultant d'une coopération renforcée entre Etats au sein du réseau développé sur une base volontaire entre eux**, pour développer et généraliser cette approche à l'échelle européenne ; ceci notamment en ce que « *Le réseau aide les États membres à permettre* ***le partage et l'utilisation de données de santé et médicales à des fins de santé publique et de recherche*** » [828]. Ce sont bien les Etats membres, qui sont **seuls compétents** : le partage et l'utilisation n'ont encore pas d'autre moteur que leur volonté, laquelle n'est qu'« aidée » par le réseau.

Mais à cette fin, c'est la Commission européenne qui, en début 2019, adopte pour fluidifier les échanges une « *recommandation relative à un format européen d'échange des données de santé informatisés* » [829], qui vise à orienter, soutenir, encourager, et aider à l'échange des données. Ces **activités relèvent d'un règlement intérieur du réseau**, certes appelé par la Commission européenne, mais établi par les Etats qui en sont membres.

Ainsi sur plusieurs points, l'article 7 de la décision de 2019 contraste avec les dispositions antérieures :

- ce sont les Etats membres représentés dans le réseau, les responsables du traitement des données à caractère personnel, qui doivent entre eux se répartir « *de manière claire est transparente les responsabilités* » (article 7§1).

[825] Cet outil relève du mécanisme pour l'interconnexion en Europe, Règlement (UE) no 1316/2013 du Parlement européen et du Conseil du 11 décembre 2013 établissant le mécanisme pour l'interconnexion en Europe, modifiant le règlement (UE) no 913/2010 et abrogeant les règlements (CE) no 680/2007 et (CE) no 67/2010 (JO L 348 du 20.12.2013, p. 129).
[826] Considérant n° 5.
[827] *Ibid*., consid. n° 8.
[828] *Ibid*. consid. n°9, qui détaille les applications du réseau que nous ne paraphraserons pas ici ; v. également le Consid. n° 10, qui indique alors les pistes de travail en cours.
[829] Recommandation (UE) 2019/243 de la Commission du 6 février 2019 relative à un format européen d'échange des dossiers de santé informatisés (JO L 39 du 11.2.2019, p. 18).

- La Commission n'apparaît que sous-traitant ; en contraste de ce qui précédait, elle **n'a pas d'accès aux données à caractère personnel traitées dans le cadre de cette infrastructure** « Santé en ligne » qu'elle gère (*ibid.*, §2 ; *comp*. article 16 ter préc.).

La Commission n'est responsable du traitement des données à caractère personnel, que pour les aspects d'accord et de gestion des droits d'accès aux services centraux de l'infrastructure, **ce qui par définition ne recouvre pas les « données de santé »** [830] (ibid., §3).

B. INSTITUTION D'UN SYSTEME DE GESTION PARA-SANITAIRE DES DONNEES DE CONNEXION

Après avoir relevé la méthode d'établissement progressif, par la Commission européenne, d'un système de gestion transfrontière des données **appuyé sur une dynamique volontaire des Etats**, nous voyons ici comment le système a encore été adapté par décision dans la période de sortie de crise (1).
Ceci avant de relever **l'unification cette fois normative,** des outils permettant de restaurer la circulation des personnes dans l'Union, sur le fondement de la connaissance partagée de données personnelles minimales (2).

1. L'institution par décision d'une « Plateforme de fédération » volontaire pour l'interopérabilité

En contraste de ce qui précède, la question ici soulevée n'est pas celle des données de santé au sens clinique, mais des données de connexion entre personnes, qui renseigneront ultérieurement sur leur statut vaccinal.
Ce statut vaccinal est une **donnée de santé, même s'il ne préjuge pas** de l'acquisition, par le sujet vacciné, d'une immunité effective, *a fortiori* de la réalité de la vaccination (des cas de fraudes de certificats ont été signalés par Europol [831], puis observés dans nombre de pays [832]).

---

[830] L'article 7§3 précise ainsi qu'il s'agit des « *coordonnées des utilisateurs, y compris leurs prénom, nom, leur adresse électronique et leur appartenance* ».
[831] Dès le 1er février 2021, par diffusion d'une alerte précoce sur les ventes de certificats contrefaits de test négatifs COVID-19. I. Rachidi, « Europol met en garde contre la vente de faux certificats PCR négatifs », Euractiv, 2 févr. 2021.
[832] R. Dupré, « Les cas de fraude aux certificats de vaccination se multiplient », le Monde, 7 août 2021 ; M. Terrier, De faux *pass* sanitaires créés via une faille de sécurité en Europe, Huffpost, 29 oct. 2021.

En juillet 2020, la Commission a ainsi adapté le système dans l'urgence [833] : dans l'espace européen, très impacté par les restrictions sanitaires ordonnées par les Etats, le but est l'échange transfrontière de données sécurisées **entre les applications mobiles nationales** très tôt identifiées comme outil pertinent de gestion des interactions personnelles [834], après la levée en juin 2020 des restrictions.

La généalogie et le relevé de la dispersion des initiatives nationales, quant à la mise au point dans l'urgence d'applications permettant le partage de telles données, a été en France l'objet en 2021 du rapport critique précité, déposé au Sénat. Ce rapport n'a pas d'équivalent publié sous l'égide de la Commission européenne : à l'inverse des sénateurs auteurs du rapport français, cette dernière n'a (diplomatiquement ?) pas relevé la dispersion des choix nationaux en matière de technologies et de déploiements, plus ou moins efficients, des Etats membres.

En revanche, elle a relevé et valorisé la convergence des efforts de ceux qui, **participant en base volontaire au réseau préexistant, y ont établi des coopérations renforcées**.

* Dans ce contexte, la décision (UE) 2020/1023 modifie la décision (UE) 2019/1765, et introduit dans son article 2, la « plateforme de fédération ». Celle-ci est définie comme une « *passerelle de réseau gérée par la Commission par l'intermédiaire d'un outil informatique sécurisé qui reçoit, enregistre et met à disposition un ensemble minimal de données à caractère personnel entre les serveurs d'arrière-plan des États membres dans le but d'assurer l'interopérabilité des applications mobiles nationales de suivi de contacts et d'alerte* » (nouveau j) in article 2§2). De quelles données personnelles s'agit-il alors ?

Dans la décision de 2020, ces données **ne sont pas définies de façon autonome : elles s'infèrent de la définition,** par l'article 2§2 (augmenté d'un i), de l'« *application mobile nationale de suivi de contacts et d'alerte », conçue dans le but « d'assurer le suivi des contacts avec les personnes infectées par le SARS-CoV-2 et d'avertir les personnes susceptibles d'avoir été exposées à ce virus* ». On a donc là **typiquement deux types de données** : **les données relatives à un patient**, sachant que se pose la question de la

[833] Décision d'exécution (UE) 2020/1023 de la Commission du 15 juillet 2020 modifiant la décision d'exécution (UE) 2019/1765 en ce qui concerne l'échange transfrontière de données entre les applications mobiles nationales de suivi de contacts et d'alerte dans le cadre de la lutte contre la pandémie de COVID-19.

[834] Recommandation (UE) 2020/518 de la Commission du 8 avril 2020 concernant une boîte à outils commune au niveau de l'Union en vue de l'utilisation des technologies et des données pour lutter contre la crise de la COVID-19 et sortir de cette crise, notamment en ce qui concerne les applications mobiles et l'utilisation de données de mobilité anonymisées (JO L 114 du 14.4.2020, p. 7).

vérification de son infection qui peut être déclarée (par l'utilisateur), ou confirmée (par un laboratoire d'analyse, et/ou une autorité sanitaire nationale [835]) ; et **les données relatives à un sujet *a priori* bien portant : cela confère de fait au système une couverture universelle.**

En outre, la même décision introduit un article 7bis, dédié aux échanges transfrontières de données entre les applications mobiles. Il spécifie que leur traitement est limité (interopérabilité des applications nationales pour suivi de contact et alerte dans le cadre de la plateforme), que les **données doivent être transmises sous forme pseudonymisée** (7bis§2) et ne consister qu'en une liste restreinte *d'items* : ainsi les clés transmises par les applications nationales, les données de journal associés aux clefs, les pays concernés et pays d'origine des clés, la vérification de l'infection (7bis§3). **L'empreinte est ainsi très limitée**.

* Ce qui nous intéresse ici, est **l'ouverture du système au-delà du réseau Santé en ligne** : tout Etat membre qui souhaite participer (en cours de route, donc) peut rejoindre la plateforme par simple information de la Commission, et indication de son autorité ou organisme national responsable du traitement (les Etats membres étant responsables conjoints du traitement 7bis§4. La Commission n'est que sous-traitante, article 7bis§5).

En revanche, l'article 7bis§6 dispose que la Commission comme les autorités nationales autorisées par les Etats membres à avoir accès à cette plateforme, **testent, analysent et évaluent la sécurité des mesures visant à garantir la sécurité du traitement**.

Ce principe est inédit, notamment dans le volet des tests de sécurité / intégrité de système sur lequel nous reviendrons dans le titre II : la Commission possède ici le droit de tester dans sa globalité le dispositif dont les Etats sont co-responsables ; **mais ne faut-il en fait lire l'article à l'inverse ?** les autorités ou organismes nationaux autorisés par les Etats membres, **ont le droit de tester, analyser et évaluer l'efficacité des mesures prises par le sous-traitant**, ici la Commission européenne…

Les conditions vérifiables de la confiance étaient un préalable à l'approche normative en 2021, non plus seulement en base volontaire en 2020.

[835] En ce sens, la décision de 2020 définit (article 2§2 l) « vérification de l'infection", la méthode employée pour confirmer une infection par le SARS-CoV-2, selon que cette infection a été déclarée par l'utilisateur d'application concerné ou qu'elle a été confirmée par une autorité sanitaire nationale ou un test en laboratoire.

2. L'institution normative d'un cadre de délivrance, vérification et acceptation de certificats Covid19 interopérables

La décision d'exécution 2020/1023, qui complète le dispositif de la décision d'exécution 2019/1765, prépare en fait le Règlement 2021/953, lequel va doter l'union d'un cadre unifié et contraignant « *pour faciliter la libre circulation pendant la pandémie* ». Cela pourrait sembler un intitulé bien audacieux, si le but du règlement n'était pas la simple interopérabilité de mesures nationales [836] : **il n'y a là aucune action de l'Union qui empiète sur la souveraineté des Etats**, à rebours de ce que certains ont pu affirmer dans une période compliquée [837].

Au contraire, c'est le Conseil, non la Commission, qui a pris la main pour une approche coordonnées des stratégies des Etats membres : définition conjointe de critères et seuils communs de restrictions à la libre circulation ; cartographie des zones à risque par code couleur fondant les restrictions ; fonctions ou besoins essentiels pouvant justifier des déplacements malgré les restrictions [838].
Le Règlement contient 64 considérants souvent très approfondis, pour traiter d'une question pour bonne partie déjà éclairée par les décisions d'exécution précitées de la Commission ; mais **le politique national monte ainsi en première ligne**.

En tout état de cause, le Règlement 2021/953 **rappelle la compétence des Etats pour limiter le droit fondamental** à la libre circulation pour des motifs de santé publique, des motifs en l'occurrence caractérisés et partagés (consid. n° 6). Il constate le potentiel de perturbation unilatérale des droits protégés par le Traité, pour les ressortissants européens comme pour ceux de pays tiers (consid. n°9), objet d'un règlement distinct [839].
Il fallait donc **créer un certificat de vaccination commun** (cette création étant expressément subordonnée à « *des preuves scientifiques suffisantes que les personnes vaccinées ne*

[836] Règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19.
[837] Nous ne rapportons pas ici les revues de multiples médias qui ont pu ou ont voulu être égarés par la complexité et l'enchaînement rapide des mécanismes décrits ; il n'en existe toujours pas d'exposé chronologique à vocation didactique, ce dont cette thèse ne peut prétendre tenir lieu, du fait de son objet spécifique.
[838] Recommandation (UE) 2020/1475 du Conseil du 13 octobre 2020 relative à une approche coordonnée de la restriction de la libre circulation en réaction à la pandémie de COVID-19 (JO L 337 du 14.10.2020, p. 3).
[839] Dans le même JO 2021 L. 211/3, p 24, est publié le Règlement (UE) 2021/954 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) destinés aux ressortissants de pays tiers séjournant ou résidant légalement sur le territoire des États membres pendant la pandémie de COVID-19.

transmettent pas le SARS-CoV-2 », considérées constituées [840]), **et par la reconnaissance mutuelle des procédures nationales de vaccination** (consid. n°10).

Dès lors, la dynamique **n'est plus fondée sur un réseau en base volontaire, ou pouvant être sélectivement rejoint** par des Etats de l'Union non initialement membres du réseau, pour l'interopérabilité des applications mobiles : le cadre retenu est cette fois **contraignant et directement applicable dans tous les Etats membres**, sans préjudice de leur réserve de compétence nationale précitée pour motifs de santé publique.

Il n'est pas lieu ici de passer en revue le règlement, qui doit notamment traiter de la lutte contre la fraude aux certificats (fraude qui serait de nature à rompre la confiance mutuelle, sur laquelle tout l'édifice repose). Contentons nous d'y examiner **la place des données de santé.** Celles-ci y présentent de **nombreuses occurrences, plus d'une douzaine de considérants très politiques** [841]. Ce sont les articles 10 « *protection des données à caractère personnel* » et article 11, « *restrictions à la libre circulation et échange d'informations* », qui ici nous intéressent, car on peut en creux en inférer la philosophie du texte.

- L'article 10 pose un **principe d'exclusivité et de temporalité d'usage** des données contenues dans les certificats délivrés en application du Règlement 2021/953 : le but ne peut être que faciliter la liberté de circulation, et les données ne doivent plus être traitées lorsque **l'objet du règlement est juridiquement épuisé** (inapplicabilité par fin de la période d'application) ; dans cette période, les seules fins légitimes sont de « *vérifier et confirmer la vaccination du titulaire, les résultats de ses tests ou son rétablissement. À cette fin, les données à caractère personnel* ***sont limitées à ce qui est strictement nécessaire*** » (article 10§3). Cela met ici en exergue l'exécution d'un test ou le constat clinique d'un rétablissement, au-delà de la logique formelle de l'attestation de vaccination.

[840] Nous ne reviendrons pas sur ce point non plus, objet de discussions polémiques ; celles-ci sont implicitement évoquées par le considérant n° 13 selon lequel les restrictions au déplacement grâce à la certification commune « *pourraient être levées notamment pour les personnes vaccinées, conformément au principe de précaution, dans la mesure où des preuves scientifiques sur les effets de la vaccination contre la COVID-19* ***sont de plus en plus disponibles et plus systématiquement concluantes quant à la rupture de la chaîne de transmission*** »). Le règlement a le mérite de valider un mécanisme extrapolable à d'autres situations futures.
[841] Voir not. considérants n° 18, 19, 22, 38, 40, spéc. 48, 50 à 52, 58, 59.

En outre, cet article contient de nombreuses autres mises en garde quant aux données à caractère personnel considérées, pour *in fine* **interdire le transfert des vers un pays tiers** par l'effet de sous-traitance (ibid., 10§8). Nous verrons l'apparition systématique de ces réserves de localisation des données et de leur traitement, *infra*.

- L'article 11 pose le principe que les Etats s'abstiennent d'imposer des restrictions à la libre circulation des personnes au-delà de ce que prévoit le règlement de 2021, mais ce « sans préjudice de leur compétence » en matière de santé publique. C'est là relever que le Règlement fluidifie par la communauté d'outil et par l'harmonisation des critères, mais **n'exclut pas que des restrictions complémentaires** (tels des tests supplémentaire de dépistage d'infection, ou quarantaine d'auto-confinement) puissent être adoptées, **à la condition que ces mesures soient nécessaires et proportionnées**.

Dans cette hypothèse, l'Etat membre exigeant de telles mesures après l'entrée de ressortissants sur son territoire doit en informer la Commission et les autres Etats membres en indiquant leur raison, portée, date et durée ; cela si possible avec un préavis de 48h (article 11§2). Or, l'hypothèse ne saurait être exclue, en cas de détérioration rapide de situation épidémiologique du fait de l'apparition de variants etc. Ce dispositif **proscrit tout arbitraire et mesure arbitraire**.

Ainsi, l'équilibre obtenu **dans un délai limité et contexte de stress même résiduel** est à saluer, **au regard de pratiques observées dans nombre d'Etats tiers à l'Union européenne**, plus ou moins invasives [842]. Des mesures pouvaient certes y être fondées, mais n'y ont pas toujours été justifiées, ni même énoncées.
Or, elles y auront permis la privation temporaire de liberté et le recueil de données de santé (dont données génétiques) sur des ressortissants européens en dehors de la protection juridique par leur droit national et européen ; c'est à dire en dehors de la **nécessité et proportionnalité selon des critères explicites et vérifiables**.

Voyons après cette dynamique normative européenne de réaction à la crise Covid19, la dynamique d'anticipation de crises futures au travers de la place renouvelée qui y tenue, à la lumière de l'expérience européenne et internationale, par les données de santé.

[842] Rapport Sénat 2021 préc.

§2. LA DYNAMIQUE NORMATIVE D'ANTICIPATION DE CRISES SANITAIRES FUTURES DANS L'UNION

Cette dynamique d'anticipation par le droit européen recouvre plusieurs volets. On citera pour l'écarter aussitôt, le plus emblématique du fait de son originalité : l'institution en septembre 2021 de **l'Autorité de préparation et de réaction en cas d'urgence sanitaire (*Health Emergency Preparedness and Response*, HERA),** du fait du constat du besoin d'une action cordonnée « *au niveau de l'Union pour le suivi des besoins, le développement rapide, la fabrication, l'acquisition et la répartition équitable de contre-mesures médicales* » [843], que sont les vaccins, médicaments et dispositifs médicaux (dont les moyens diagnostic).

Cela résulte d'une communication de la Commission qui relevait à chaud le besoin de « *renforcer la résilience* » [844] (en fait, **constatait implicitement la dispersion de stratégies nationales, en compétition au sein même de l'Union**), comme la mise en place du plan de préparation en matière de biodéfense « *incubateur HERA* » [845].
Ce service de la Commission acte ainsi le **besoin d'une structure centrale spécifique**, en contraste de la fragmentation des cadres d'actions et financements de l'Union en matière de garantie d'approvisionnement et d'accès aux contre-mesures médicales (consid. n°6).

Dans ce texte, n'apparaît qu'une occurrence des « données de santé », lorsque sont définie les attributions de l'HERA (article 6) : il est seulement prévu que le Conseil d'HERA émette des avis notamment sur les propositions d'activités de l'HERA, et sur les nouvelles tâches qui pourraient lui être confiées au-delà des prévisions de 2021 ; or, cela intègre « *iv) la promotion de la recherche et du développement sur les contre-mesures médicales, de dispositions et de plateformes* ***pour le partage rapide des données*** ». La décision ne porte pas plus de précision, ce qui libère le potentiel de proposition ; à la différence des directives, décisions et règlements précités, **il n'est pas éclairé ni *a fortiori* restreint, par les considérants** (8) de la décision.

En pratique, **aucune donnée personnelle de santé n'est à ce jour partagée, ni ne semble avoir vocation à l'être** : les accords de travail en mars 2023 ne portent dans la relation

[843] Décision de la Commission du 16 septembre 2021 instituant l'Autorité de préparation et de réaction en cas d'urgence sanitaire, 2021/C 393 I/02 (entrée en vigueur le 16 sept. 2021).
[844] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Construire une Union européenne de la santé: renforcer la résilience de l'UE face aux menaces transfrontières pour la santé». COM (2020) 724 final.
[845] Communication de la commission au Parlement européen, au Conseil européen et au Conseil «Incubateur HERA: anticiper ensemble la menace des variants du virus de la COVID-19». COM (2021) 78 final.

HERA / l'ECDC que sur des données épidémiologiques ou biologiques[846] ; dans la relation HERA / EMA que sur les données « pertinentes » – ce qui, dans le contexte de l'accord de travail, n'inclut pas de données cliniques personnelles [847] ; mais nous avons vu que le règlement 2022/123 développait très substantiellement ce volet, *supra*.

En tous cas, il n'existe dans cette décision aucun article dédié à la protection de telles données ; cela suggère qu'**HERA n'a pas vocation à en traiter ni directement, ni indirectement.** Mais ce silence ne vaut pas indicateur précis du champ d'action juridiquement possible [848].

Pour ces raisons, et parce qu'il est inutile de spéculer plus allant sur ce point, nous écartons l'analyse du mécanisme HERA, et concentrons l'attention sur **deux règlements pivot adoptés en 2022, et convoquant des données personnelles de santé**. Le premier s'inscrit dans le sillage direct du mécanisme HERA : il institue un cadre inédit pour garantir la fourniture de contre-mesures médicales (A).
Le second abroge une décision de la Commission européenne : il **amplifie de façon contraignante le cadre de préparation aux menaces transfrontières** graves futures (B).

A. LA MOBILISATION DE DONNEES POUR LE « CONSEIL DE GESTION DES CRISES SANITAIRES »

Dans le sillage de la décision instituant l'HERA, le Conseil européen a en octobre 2022 adopté un règlement n° 2022/2372 qui vise à organiser la disponibilité des technologies de santé requises en cas d'urgence de santé publique d'ampleur européenne [849]. Il est fondé sur le constat que les mesures adoptées durant la crise étaient réactives par défaut d'anticipation ; que l'Union n'était pas suffisamment préparée, était vulnérable en ce qui concerne ses approvisionnements, etc.

---

[846] (publié en mars 2023, mais non daté) « Working arrangements between the Health Emergency Preparedness and Response Authority (HERA) and the European Centre For Disease Prevention and Control (ECDC) on health emergency preparedness and response in the area of medical countermeasures ».
[847] (publié en mars 2023, mais non daté) « Working arrangements between the European Health Emergency Preparedness and Response Authority (HERA) and the European Medicines Agency (EMA) on health emergency preparedness and response in the area of medical countermeasures ».
[848] De toute façon, tout traitement serait soumis au droit commun précité (quant aux données personnelles traitées par les institutions européennes), auquel une décision de la Commission ne saurait déroger.
[849] Règlement (UE) 2022/2372 du Conseil du 24 octobre 2022relatif à un cadre de mesures visant à garantir la fourniture des contre-mesures médicales nécessaires en cas de crise dans l'éventualité d'une urgence de santé publique au niveau de l'Union.

Or, il en résulte la volonté d'un cadre visant à garantir la fourniture de contre-mesures médicales d'ambition large, puisqu'il s'agit d'un « ***instrument de politique économique fondamental*** » (consid. n°2), **car il doit prévenir les conséquences systémiques socio-économiques etc. de la crise.** Nous n'entrerons pas ici dans l'analyse détaillée de ce règlement, porteur de nombreuses obligations nouvelles, et nous en tiendrons à la place qu'y tiennent les données de santé.

Auparavant, notons qu'en décembre 2022, un premier rapport prospectif sur le rôle de l'Union européenne dans le champ des contremesures médicales à l'antibiorésistance a été publié sous l'égide de la Commission européenne ; de façon très significative, **ce rapport est signé conjointement** par le *Directorate General for Health Emergency Preparedness and Response Authority* (HERA) et *l'European Health and Digital Executive Agency* (EHDEA) [850] ; il s'inscrit sur un fond de tensions qui en 2023, voit notoire la dépendance de l'Europe à l'égard de la République Populaire de Chine en matière d'antibiotiques, et en objective les conséquences géopolitiques [851].

1. La stimulation d'un potentiel de R&D accélérée pour la biodéfense de l'Europe

Outre la mise en place d'un conseil de gestion des crises sanitaires (article 1§2a), des procédures d'action sur les marchés de produits de santé et matières premières (ibid., b), de mesures relatives à l'inventaire, cartographie et stimulation de production européenne (ibid., e), et le financement d'urgence (ibid., d), le Règlement 2022/2372 institue un cadre visant à « *c) l'activation de plans de recherche et d'innovation d'urgence,* ***faisant également appel aux réseaux d'essais cliniques et aux plateformes de partage de données*** *à l'échelle de l'Union* ».

***** Il est spécifié que ce cadre d'urgence **ne peut être activé que lorsqu'il est approprié à la situation** (article 1§3) : c'est alors sur proposition de la Commission, que le conseil de gestion des crises sanitaires (CGCS), s'il reconnaît l'urgence de santé publique, et s'il estime les mesures appropriées à la situation économique, peut « *adopter un règlement portant activation du cadre d'urgence* » (article 3). Si l'article 5 relatif à sa propre compétence s'applique toujours, **il est loisible au CGCS d'activer, de façon sélective, les mesures**

[850] Commission européenne, « Study on bringing AMR Medical Countermeasures to the Market » – Final Report HADEA/2021/OP/0005. Sur l'usage des données, pages 31 et s.
[851] Martuscelli C, « How China could choke EU supply of medicines - Europe relies on China for the production of certain key drugs such as antibiotics », Politico, 24 mai 2023.

prévues par les articles 7 à 13 ; mais la désactivation ou l'expiration de ces mesures provoquent sa propre mise en veille (article 5§2). Seuls nous intéressent ici les articles 7 et 9.

- **l'article 7 relatif au « mécanisme pour le suivi des contre-mesures médicales nécessaires en cas de crise** » ne traite pas de données de santé en soi. En revanche, il renvoie au règlement (UE) 2022/123, où leur usage et protection sont abondamment développés. On les traitera sous l'article 9, dont l'objet est connexe.
- **L'article 9 relatif « à la recherche et à l'innovation d'urgence du plan de préparation et de réaction et utilisation de réseaux d'essais cliniques et de plateformes de partage de données »** traite par définition des données de santé. Son activation renvoie à la mise en œuvre du règlement 2022/2371 préc. (article 9§1). Dans le même article, il est entre autres spécifié que « *La Commission encourage l'accès aux données pertinentes issues des essais cliniques* ***mais aussi*** **(sic)** ***aux données réelles*** (…et…) *soutient les activités des organismes nationaux compétents qui promeuvent la disponibilité et* ***l'accessibilité des données, y compris les données relatives à la santé****, conformément à l'article 15 »* (article 9§2).

* Dans ce contexte, un renvoi explicatif au règlement (UE) 2022/123 est utile : son consid. 45 met en exergue **l'accès rapide aux données de santé et à leur échange «** ***y compris les données de terrain*** *(…) essentiels pour assurer une gestion efficace des urgences de santé publique et événements majeurs* ». Son considérant 48 le suit en conséquence, **et est l'expression la plus développée du statut de la donnée dans les textes en cours et post crise** : « ***Étant donné le caractère sensible des données de santé,*** *l'Agence (EMA) devrait garantir ses opérations de traitement et assurer qu'elles respectent les principes relatifs à la protection des données tels que la licéité, la loyauté et la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation, l'intégrité et la confidentialité* », puis renvoie à l'applicabilité du droit commun de protection.

Ce considérant justifie l'article 20 **« outils et données informatiques »** du règlement 2022/123, pertinent ici, **puisque le règlement 2022/2372 y renvoie**. On y relève que l'EMA « *développe et tient à jour des outils informatiques, notamment une plateforme informatique interopérable, pour la transmission des informations et des données,* ***y compris des données de santé électroniques générées en dehors d'études cliniques*** » (article 20, a) : il s'agit des données de santé de patients objet de soins, non de patients participant aux essais.

De même, selon ce règlement, l'EMA « *utilise, dans le cadre de ses tâches de réglementation* (entendre ici de police administrative sanitaire)*, des infrastructures numériques ou des outils informatiques afin de faciliter l'accès rapide aux* ***données de santé électroniques disponibles générées en dehors d'études cliniques ou l'analyse de ces données, ainsi que l'échange de ces données*** *entre les États membres, l'Agence et d'autres organismes de l'Union* » (ibid., c).

Le Règlement 2022/123 contient également un article dédié à la protection des données à caractère personnel (article 35), qui rappelle l'applicabilité du droit commun (RGPD), mais prévoit une exception pour « *certains transfert* ***de données à caractère personnel*** » vers des autorités de pays tiers « *lorsque ces transferts sont nécessaires pour des motifs importants d'intérêt public, tels que la protection de la santé publique* », sans plus préciser.

Revenons en donc ici au règlement 2022/2372, qui renvoyait lui-même au règlement 2022/123 dont nous venons, par incise, d'évoquer le contenu sur les points ici pertinents. **Sans le caractériser** (à la différence du règlement 2022/123, ce que nous venons de le voir), le règlement 2022/2372 **met en exergue la subordination à un critère d'absolue nécessité,** du traitement des données à caractère personnel.

2. Des dispositions spécifiques de protection des données à caractère personnel ?

Le Règlement 2022/2372 contient en effet un article 15 dédié à cette protection : il rappelle le droit commun opposable aux Etats et institutions européennes (15§1), **auquel il ne déroge donc pas** (i.e. : le droit de la protection des personnes n'est pas en soi compromis par les mesures d'urgences en cas de crise sanitaire, le modèle étant *privacy by design,* donc induisant une protection native). Mais cet article contient deux dispositions d'intérêt :

- l'article 15§2 **restreint explicitement le champ du traitement de telles données à caractère personnel à un besoin « absolument nécessaire »**. Nous avons vu *supra* que le règlement mettait en exergue la question de l'accès aux données de « vie réelle ». Ces données ne résultant pas d'études interventionnelles (essais cliniques) mais observationnelles (pratique de soins et leurs effets), leur rôle n'en est pas moins crucial et explicité dans le considérant n°17, *supra*. La mise en œuvre rapide de contre-mesures médicales, *a fortiori* si celles-ci sont rapidement conçues (vaccins, médicaments antiviraux, etc.) **suppose une capacité à confirmer par suivi voire**

définition de cohortes, pour la pharmacovigilance et l'analyse de performance. Remonter aux cas peut alors être « absolument nécessaire » pour expliquer des réponses différenciées selon des profils au sein de populations, éventuellement segmenter la recherche par sous-groupes de population.

- *A contrario* (lorsque le traitement de telles données n'est pas absolument nécessaire), l'article 15§3 dispose que les données à caractère personnel sont rendues anonymes. Or, **n'est-ce pas là une disposition redondante, puisqu'il s'agit du droit commun**, rappelé dans l'article 15§1 ? Dans ce contexte, la clef d'application du droit est le critère de la « nécessité absolue » (sachant nous l'avons vu que le traitement de données de santé nominatives dans ce contexte ne privait pas les personnes concernées, des garanties renforcées en matière de protection).

Or, le règlement ne formule pas d'hypothèses – **celle que nous proposons nous semble l'hypothèse principale**. Seul un de ses considérants l'évoque en filigrane, lorsqu'il souligne l'enjeu de « *garantir l'acceptabilité des essais cliniques* ***et des résultats qu'ils produisent*** *en vue de l'autorisation de médicaments nouveaux ou repositionnés* » (consid. n°17).

On notera la même considération présente dans le règlement 2022/123 précité, lequel renforce le rôle de l'Agence européenne du médicament en préparation et gestion de crise [852] : « *La création de l'ETF* (task-force pour les situations d'urgence, ETF) *devrait s'appuyer sur le soutien apporté par l'Agence durant la pandémie de COVID-19, notamment en ce qui concerne les avis scientifiques fournis sur la conception des essais cliniques et le développement des produits* ***ainsi qu'en ce qui concerne l'examen continu des données probantes émergentes afin de permettre une évaluation plus efficace des médicaments, y compris des vaccins****, lors des urgences de santé publique* (…) » (consid. n°28) [853].

Peut-être est-il politiquement plus sensible d'évoquer l'hypothèse justifiant la nécessité absolue d'accès aux données personnelles (l'incertitude quant aux effets d'une technologie développée très rapidement, et son besoin de confirmation de *ratio* efficacité/sécurité en vie réelle), **que de ne pas expliciter** les conditions de départage des régimes de traitement ?

[852] Règlement (UE) 2022/123 du Parlement Européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux.

[853] Son consid. 31 préconise dans le même sens que « *Les résultats des essais cliniques et les données cliniques produits après l'octroi d'une autorisation de mise sur le marché devraient être rendus publics en temps utile* ».

B. LA MOBILISATION DE DONNEES DE SANTE PAR LA « PLATEFORME NUMERIQUE DE SURVEILLANCE »

D'objet bien distinct de celui qui précède, le Règlement (UE) 2022/2371 du Parlement européen et du Conseil relative aux menaces transfrontières graves pour la santé abroge en novembre 2022 la décision n°1082/2013/UE préc. [854]. Il est ici notable qu'**un règlement, non une nouvelle décision, change le cadre juridique d'action**.

Ce règlement fait naître de nombreuses obligations pour les Etats membres et organes européens ; mais notre intérêt se limite ici à l'institution de la plateforme numérique de surveillance visant à la mobilisation de données (1), puis la discussion des règles d'accès, potentiellement ouvert par la Commission, à des Etats tiers (2).

1. L'institution de la plateforme numérique de surveillance

Dans le champ des données de santé, le Parlement et le Conseil notent le besoin de renforcer, par le jeu notamment de l'intelligence artificielle, les capacités de recherche des contacts ; et le besoin que la Commission s'assure que le SAPR réunisse et communique aux Etats membres les informations pertinentes issues des différents systèmes d'alerte précoce etc.

* Dans ce cadre, il met en exergue le fait (jusqu'alors implicite [855]), que cette « *coordination **pourrait nécessiter l'échange de données à caractère personnel, y compris des données sensibles relatives à la santé, et des informations concernant des cas humains** de la maladie ou de l'infection confirmés ou suspectés* », avec la prudence de limiter l'échange « *entre les États membres directement concernés par les mesures de recherche des contacts* » (consid. n° 37). Parmi ses nombreux apports, le Règlement met en place, outre une surveillance épidémiologique élargie (article 13), une « plateforme numérique de surveillance » en temps réel, **dont il attribue la charge du « développement constant » à l'ECDC**.

Pour cela, c'est l'ECDC qui doit avoir « *ainsi qu'il convient, effectué **des analyses d'impact de la protection des données et atténué les risques pour les droits et les libertés des personnes concernées** par le traitement des données* » (article 14§1). Le même prévoit

[854] Règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision no 1082/2013/UE (Texte présentant de l'intérêt pour l'EEE).
[855] Inféré des articles relatifs à la protection des données personnelles.

l'utilisation de « *données de santé à caractère non personnel pertinentes* ***issues d'une liste préalablement définie et autorisée émanant des dossiers médicaux électroniques*** *et des bases de données de santé* ». L'enjeu d'exactitude et de complétude est d'autant plus fort, que le traitement sera explicitement l'objet de l'intelligence artificielle (14§2,a), dont la mise en œuvre ne pourra explicitement être opérée que sous contrôle humain (14§1).

* Dans ce contexte, la protection des données fait l'objet d'un article dédié qui rappelle le droit commun applicable (article 27).

Mais elle est aussi l'objet d'un article distinct, dédié à leur protection en lien avec la fonctionnalité de messagerie sélective du SAPR (article 28), dont il est spécifié que cette fonction permet de « *communiquer des données à caractère personnel,* ***y compris les données sur les contacts et la santé, uniquement aux autorités nationales compétentes participant*** *aux mesures de recherche des contacts et aux procédures d'évacuation médicale* » (28§1).

Or, cette communication est sélective, elle ne peut être justifiée que par un **critère d'implication opérationnelle** dans la recherche de contacts et d'évacuation, ce qui fait que **seules les autorités qui les conduisent ont à en connaître**, ce qui, pour ce qui est de la fonction recherche de contacts, est un peu brumeux : comment savoir quelle autorité activer, dans ce contexte large ?

En outre, le règlement dispose que « *les autorités nationales compétentes ne conservent ni les données de contact,* ***ni les données de santé reçues au moyen de la fonctionnalité*** *de messagerie sélective pendant* (sic) *une durée supérieure à la durée de conservation applicable dans le cadre de leurs activités nationales de recherche des contacts* » (article 28§5). Ce passage soulève un point de rédaction non sans conséquences juridiques : nous considérons qu'il établit une **durée limite de conservation, laquelle n'est pas préfixe** : la durée de conservation ne peut excéder la durée d'activité nationale de recherche des contacts ; mais alors, la donnée disparaît une fois le contact identifié : cela permet-il une épidémiologie sur temps longs ?

Le choix est en tous cas fait, que ces données à soient à **usage exclusif et temporaire**.

2. L'accès d'Etats tiers au système, donc aux données : enjeux procéduraux ?

Dans le Règlement 2022/2371, c'est la Commission qui est compétente pour, par voie d'actes d'exécution, notamment déterminer « *les cas et les conditions dans lesquels* ***les pays tiers peuvent se voir accorder l'accès à l'interopérabilité de la recherche des contacts****, et les modalités pratiques de cet accès* », sans préjudice de la protection de droit commun précitée (article 28§6, b).

*** La matière étant très sensible,** notons que l'article 31 dédié à l'exercice de la Commission européenne, la délégation de pouvoir visée notamment « *à l'article 28, paragraphe 6,* ***peut être révoquée à tout moment par le Parlement européen ou le Conseil*** » (article 31§3) ; mais si cette révocation met fin à la délégation de pouvoir, cette révocation « *ne porte pas atteinte à la validité des actes délégués déjà en vigueur* » (ibid.), dont le Règlement ne prévoit pas l'hypothèse (toujours possible ?) du retrait par leur auteur délégué.

Or, on peut s'en étonner, si la révocation de la délégation (hypothèse certes maximaliste, mais envisagée dans le Règlement) était justifiée par un doute **quant à la légitimité des motifs réels d'accès** d'un Etat tiers au système, ou de **doutes sérieux quant à la protection ultérieure par lui de données** de ressortissants européens qu'il aurait obtenues sous le couvert de la recherche de contacts qu'organise le Règlement. Est-ce bien là le problème : la délégation… ou plutôt, les actes pris en application de la délégation ?

* Le fait que l'entrée en vigueur d'un tel acte adopté par la Commission sur le fondement de l'article 28§6, **soit subordonné à l'absence d'objections** dans un délai de deux mois (prolongeable) suivant sa notification au Parlement et au Conseil (article 31§6), ne lasse pas d'étonner : *a priori* rassurante, cette conditionnalité de l'entrée en vigueur est-elle compatible avec les besoins de réaction rapide en situation de crise sanitaire, objet du règlement ? Pourquoi, **en cas par exemple de doute sérieux quant à la légitimité d'accès ou d'usage par un Etat tiers**, l'acte incriminé antérieur à la révocation resterait-il valide ?

Paradoxalement, le règlement ne prévoit pas la possibilité d'un retrait de cet acte par la Commission même. On pourrait considérer ce pouvoir comme implicite ; mais ce point **n'aurait-il pu être précisé, du fait de son importance ?**

En outre, l'hypothèse de la révocation de la délégation de pouvoir (article 31§3) ne prive-t-elle pas *de jure*, la Commission du pouvoir de retrait ? Certes, le lecteur peut considérer cette hypothèse comme hautement improbable. Mais **cette hypothèse de réserve de souveraineté** est formulée par le Règlement même. Et si des circonstances par hypothèse géopolitiques peuvent être si graves, que l'accès n'apparaisse plus souhaitable, un scénario intermédiaire (action de la Commission à la demande du Conseil ou du Parlement) n'est il pas raisonnablement envisageable ?

A défaut, la logique commanderait que le Parlement ou le Conseil ordonnât à la Commission le retrait, **avant** de révoquer sa délégation, scénario maximal et peut-être inutile.

C'est certes **possible mais compliqué, en tous cas en dehors de tout délai utile**. De même en est-il de l'éventualité de la saisine de la CJUE, pour obtenir l'annulation d'un acte délégué dont les conditions d'adoption, ou surtout les conséquences (car elles sont dynamiques), seraient source de doutes graves – sur fond par hypothèse toujours, d'enjeux géopolitiques.

SYNTHESE P2T1C1

Ce premier chapitre de notre titre I sur la dynamique des garanties unifiées de l'accès licite aux données dans le champ de la santé restitue des observations plus descriptives que prospectives : il analyse la dynamique de l'approche coopérative consistant en la convergence en base volontaire pour les Etats membres de l'Union sur la base de son Traité, quant aux modalités de partage dans différentes circonstances. Dans ce contexte, nous ne considérons que notre fil rouge des données.

* Dans une première section, nous considérons la dynamique coopérative pré-covid19, qui augure la stratégie pour la transformation numérique de l'Union notamment en santé. Avant sa conceptualisation et mise en œuvre, nous relevons la dynamique de fluidification des données corollaire de la mobilité des personnes. Le développement des soins transfrontières est marqué par tant par la recherche d'un continuum informationnel que par la mutualisation en réseau d'une expertise dispersée. Il s'agit de des cadres encore réduits d'échange sélectif de données de santé, mais qui porte en germe la pétition d'un partage élargi pour leur usage

primaire et secondaire. Distinctement, nous relevons une dynamique de coordination des Etats membres, qui se dotent d'outils visant à la gestion des crises sanitaires transfrontières, et la coordination d'actions communes mais sans encore de transmission de données.

* Dans une seconde section, nous relevons la façon dont la pandémie de Covid19 a joué le rôle d'accélérateur à la faveur, à certains égards, d'une panique transformatrice. Toujours avec pour fil rouge la question de la donnée, nous esquissons la dynamique normative de la réaction à cette pandémie, fondée sur l'adaptation du système de gestion des données cliniques transfrontières. Il s'appuie sur la mutualisation d'un système de gestion transfrontières et la promotion de l'interopérabilité par le réseau « Santé en ligne ». De nouvelles données traitées au plan européen font aussi leur apparition, d'une sensibilité différente mais ombrageuse, avec l'institution d'un système de gestion para-sanitaire des données de connexion, par une plateforme de fédération volontaire et un cadre juridique de certificats Covid19 interopérables, dont nous avons relevé les points critiques de compétence et temporalité. Puis nous considérons la dynamique cette fois d'anticipation de crises sanitaires futures : elle nous conduit à relever la mobilisation inédite de données de santé pour le « Conseil de gestion des crises sanitaires », et la « Plateforme numérique de surveillance », qui appellent une approche de plus en plus intégrative, à laquelle les Etats consentent à l'épreuve des faits.
Cela soulève des questions nombreuses et inédites quant à l'articulation entre Commission d'une part, Conseil et Parlement d'autre part.

CHAPITRE II. UNE DYNAMIQUE NORMATIVE D'APPROCHE INTEGRATIVE EN MATIERE DE DONNEES DE SANTE ?

Dans la section précédente, nous avons relevé la façon dont le droit sanitaire a, selon une dynamique d'approche coopérative, **visé à caractériser et encadrer les usages partagés des données, essentiellement à titre primaire et de façon restrictive**. Le but est la possibilité d'accès aux soins et leur *continuum* transfrontières hors crise, puis la réaction et l'anticipation en cas de crise / de menace sanitaire grave transfrontière impactant l'Union, ce que nous avons vécu de l'intérieur, en lien alors avec le P. Megerlin lui-même en cellule de crise.

Or, il est d'autres usages et supports de données en plein développement.

Ce chapitre rapporte et analyse leur **accélération récente et forte, qui n'a pas encore donné lieu à l'épreuve pratique,** ni à une grande production doctrinale [856] : nous relevons ici la façon dont le droit européen vise la construction d'un **« espace européen » des données**, lequel ne traite la question sanitaire qu'à la marge (S1) ; puis un **« espace européen des données de santé »** qui leur est dédié, du fait de leur sensibilité et potentiel spécifiques (S2).

SECTION 1. LA DYNAMIQUE DE CONSTRUCTION DE « L'ESPACE EUROPEEN » DES DONNEES : DES BALISES NON SPECIFIQUES

Comme précédemment, cette dynamique est fondée sur l'article 114 TFUE. Elle résulte de la potentialisation réciproque de deux outils distincts. Nous les traiterons dans l'ordre chronologique de leur élaboration, **lequel n'est pas celui de leur entrée en vigueur**.

En effet, à la date de la rédaction de notre thèse, un de ces textes n'est encore connu que sous la forme d'une proposition de règlement, formalisée en février 2022 : le règlement européen sur les données dit « *Data Act »* [857]. L'autre est un règlement sur la gouvernance des données, dit « Data Governance Act », proposé en 2022 et adopté en juin 2023 [858]. Cela nous permet de traiter du droit qui détermine intrinsèquement l'objet (§1), avant d'évoquer un cadre spécifique (§2).

---

[856] Rappelons que nous procédons à une analyse de première main en situation opérationnelle.

[857] Proposition du 23 février 2022 de règlement européen du Parlement et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) COM(2022)68 Final.

[858] CE, communiqué 28 juin 2023, Règlement sur les données: La Commission se félicite de l'accord politique sur des règles pour une économie fondée sur les données équitable et innovante.

§1. DYNAMIQUE NORMATIVE DU DATA ACT : LA PROMOTION D'UN CADRE INTERSECTORIEL

Ce projet de norme européenne propose un outil d'harmonisation des règles pour l'équité de l'accès des personnes physiques et morales, publiques comme privées, aux données et à l'utilisation des données. Dans ses orientations 2019-2024, la présidente de la Commission madame Von der Leyen a en ce sens déclaré que l'Europe devait « ***équilibrer le flux et l'utilisation des données*** *tout en préservant un haut degré de protection de la vie privée, de sécurité, de sûreté et d'éthique* » [859].

En janvier 2020, avant donc la déclaration de la pandémie de Covid19, la stratégie européenne pour les données était inscrite au programme de travail de la Commission [860], afin, **par l'agilité intersectorielle du traitement des données,** de faire de l'Union un leader économique mondial.

La question n'est ici plus celle de la protection (traitée par le RGPD en 2016 portant droit commun, sur lequel il n'est pas revenu), mais de la **valorisation économique des données** entre, par et pour les entreprises et les administrations publiques, **dans un contexte de concentration des données aux effets anti-compétitifs donc inhibiteurs de l'activité** [861].

Le texte était assez avancé, pour que le CEPD donne un avis daté du 16 juin 2020 : **cela témoigne bien de sa maturité** [862]. On évoque rapidement ici son apport, limité en matière de santé, du fait de la gestation parallèle d'un texte dédié (A) ; ceci non sans un rapide focus sur des disposition de crise qui convoquent des leçons de la pandémie (B).

---

[859] U. von der Leyen, « Une Union plus ambitieuse —Mon programme pour l'Europe, Orientations politiques pour la prochaine Commission européenne 2019-2024 », 16 juillet 2019.
[860] Commission européenne, Annexes au programme de travail de la Commission pour 2020 —Une Union plus ambitieuse, COM (2020) 37, 29 janvier 2020.
[861] La question de la génération et ouverture des données par les administrations publiques relève d'un autre texte, *infra*
[862] CEPD, Avis 3/2020 sur la stratégie européenne pour les données, 16 juin 2020. https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_fr.pdf

A. APPORT NECESSAIREMENT LIMITE DU « DATA ACT » EN MATIERE DE DONNEES DE SANTE

Le but est de « *garantir l'équité dans la répartition de la valeur produite par les données entre les acteurs de l'économie fondée sur les données et de favoriser l'accès aux données et l'utilisation de ces dernières* » [863].

Il se décline en plusieurs objectifs pertinents en matière de données de santé, **sans pour autant les viser** (1). Nous voyons ensuite des dispositions d'impact sur les données de santé (2), qui seront précisées dans les textes ultérieurs.

1. Objectifs de la proposition de règlement sur les données « EEDS »

Si la proposition de règlement sur la gouvernance des données de 2022 définit la notion en soi de « donnée », elle n'entre pas dans les sous-catégories dont celle des données « de santé » [864], lesquelles avaient précédemment définies en 2016 par le RGPD, avant d'être précisées en 2022 (selon la typologie de leur usage) par la proposition de règlement dédié à l'EEDS, *infra*.

Les objectifs sont suffisamment énoncés dans les motifs de la proposition de règlement, fondés sur une analyse de situation dont nous avons extraits des tableaux éloquents, *supra*. Nous en citons ici quatre littéralement, du fait de leur intérêt pour la mise en perspective.

- Le premier est de « ***Faciliter l'accès aux données et (leur utilisation) par les consommateurs et les entreprises, tout en préservant les incitations à investir*** *dans les moyens de créer de la valeur à partir des données* ». Cet objectif fera l'objet de dispositions très spécifiques pour les données de santé. Toutes les données réclament une protection juridique renforcée, lorsqu'elle sont générées par des produits ou services ; mais nous avons vu la complexité de ce point lorsque des données peuvent être produites par des technologiques qui ne revendiquent pas d'applications en santé, mais n'en constituent pas moins des données de santé « par destination ».

[863] Exposé des motifs par la Commission, précédant la proposition de Règlement, spéc. p. 3.
[864] On verra toutefois infra des précisions dans les textes ultérieurs quant aux catégorisations dans l'ESSD.

- Le second est de prévoir des cadres d'accès exceptionnels et d'office par les autorités publiques, lorsque l'intérêt public l'exige ; nous le traiterons *infra*, puisqu'il se rattache aux seules situations de crise **justifiant un partage obligatoire**.

- Le troisième objectif est de « ***Faciliter le passage des services d'informatique en nuage aux services de traitement des données à la périphérie*** », qui présente une certaine connexion avec le quatrième objectif « ***Mettre en place des garanties contre le transfert illicite de données,*** *sans notification, par les fournisseurs de services informatiques en nuage* ». Nous en traiterons *infra* sous l'angle de l'analyse de l'avènement de garanties réciproques contre l'accès externe illicite (Titre II de la seconde partie de notre thèse).

- Le cinquième objectif aurait pu, techniquement et logiquement, précéder les autres ; mais il devait politiquement leur succéder : il s'agit de « ***Prévoir l'élaboration de normes d'interopérabilité pour les données destinées à être réutilisées*** *entre les secteurs* ». Cette question est majeure, mais hors du champ de notre recherche ; on verra toutefois la question spécifiquement abordée dans le règlement relatif à l'espace européen des données de santé.

2. Extrapolation de dispositions de droit commun aux données de santé

Le règlement sur les données de santé renforce la portabilité de certaines données générées par les utilisateurs. Ce droit prévu à l'article 20 du Règlement 2016/679 dit RGPD, est réexposé et développé dans l'article 5 relatif au **droit de partager des données avec des tiers**.

Ainsi, l'article 5§1 prévoit que lorsqu'un utilisateur ou son mandataire en fait le demande, « *le détenteur de données met à la disposition d'un tiers, dans les meilleurs délais, sans frais pour l'utilisateur et, le* ***cas échéant, en continu et en temps réel, les données générées par l'utilisation d'un produit ou d'un service lié****, à un niveau de qualité identique à celui dont lui-même bénéficie* ». Il n'est pas lieu ici d'entrer dans ce régime de la portabilité, détaillé dans les articles 4 et 5.

Notons seulement que ce régime **peut concerner des données qui ne sont pas nativement des données « de santé »**, c'est-à-dire une production organique du système de santé ou d'une technologie relevant de la qualification légale de technologie de santé, ce que donc nous avions appelé des données « par destination », *supra*. Sont spécialement concernées ici,

les données produites par des applications non santé mais « bien être » etc., lesquelles d'ailleurs seront pour partie incorporées au champ du règlement EEDS (*infra*).

Or, sur ce point, l'article 5 **vise à limiter la concentration des données** par les entreprises fournissant des « *services de plateforme essentiels* », qui ne sont pas considérées comme tiers.

Il en résulte que ces entreprises ne peuvent demander, à un utilisateur, l'accès à des données le concernant que celui-ci aura obtenues au titre de l'article 4§1 et 5§1. On peut aussi considérer que, si ces entreprises ne sont pas considérées comme « tiers » au sens de l'article 5, l'article 5§4 ne leur est pas moins applicable : elles **doivent alors s'interdire** le recours à des moyens coercitifs, ou d'exploiter des failles d'infrastructure technique du détenteur des données pour obtenir un accès, qui serait dès lors frauduleux, à celles-ci.

On note ici que le tiers recevant des donnés doit notamment s'abstenir « ***d'utiliser les données qu'il reçoit à des fins de profilage de personnes physiques*** *au sens de l'article4, point4, du règlement (UE) 2016/679, à moins que cela ne soit nécessaire pour fournir le service demandé par l'utilisateur* » (article 6§2, b). Cet élément est particulièrement pertinent ici, puisque nous avons vu comment le recoupement d'informations « non santé » permettait de supposer raisonnablement des facteurs de risques, de prédire des tendances voire des états sanitaires.

Si certaines dispositions sont ainsi pertinentes, le règlement sur les données **ne prévoit pas de règles applicables à l'ensemble des données de santé**, et les dispositions qu'il contient devront dans ce champ être pour partie précisées, *infra*.

B. APPORT ORIGINAL DU « DATA ACT » POUR LE TRAITEMENT DE SITUATION DE CRISE

La proposition de règlement sur les données intègre le retour d'expériences de la pandémie Covid19, lors de laquelle un désordre systémique a été induit, et a été observable dans l'Union européenne.
Il contient des dispositions d'intérêt pour faire face à des situations d'exception qui requièrent la mobilisation immédiate de données dans l'intérêt public (1). La disposition est extrapolable, pour partie, au champ de la santé publique (2).

1. La disponibilité d'office des données « pour le bien public »

Cette hypothèse n'est pas un apport original de la proposition de règlement de 2022 sur les données, puisque **cette philosophie était déjà annoncée** dans le RGPD de 2016 (considérant n°4). Mais la proposition **orchestre techniquement les modalités d'accès aux données**. Il n'en est pas moins salué par le CEPD dans son avis de 2020, puisqu'il acte la prise en compte du « *bien public* » et de l'« *intérêt public* », que le CEPD y note interchangeables [865].

Tel est l'objet du chapitre V qui justifie, par un « besoin exceptionnel », la mise à disposition de données au profit d'organismes du secteur public qu'il soient nationaux ou européen.

On peut s'étonner de ce que le « *besoin exceptionnel* » soit défini (article 15) seulement après l'énoncé des obligations des détenteurs des données (article 14). **Ce besoin est « réputé exister »** [866] **lorsque des conditions cumulatives sont satisfaites :** les données doivent être nécessaires pour réagir (a) ; le défaut de telles données empêcherait l'organisme public de s'acquitter d'une mission spécifique d'intérêt public prévue par la loi (b) ; cet organisme ne peut y accéder autrement que sous couvert de l'article 15 (les alternatives étant l'achat au prix marché, un cadre légal existant, cf. 15, c.1), et si la procédure de l'article 15 « (réduit) *substantiellement la charge administrative pesant sur les détenteurs des données* » (ibid., c.2).

Pour les détenteurs des données, **il s'agit d'une obligation de fourniture** (article 14), laquelle toutefois ne s'applique pas aux petites et micro-entreprises [867]. Serait-ce parce que l'on ne leur prête pas la détention de données significatives dans ces circonstances ? En situation critique, « *On a souvent besoin d'un plus petit que soi* » [868].
En fait, la demande peut être exprimée, mais hors du cadre du règlement qui prévoit que cette **fourniture est gratuite** pour réagir au titre de l'article 15 à une urgence publique (article 20§1). Les petites et micro-entreprises sont implicitement *a contrario*, rémunérées.

2. L'intérêt de la disponibilité immédiate pour la santé publique

Rappelons que les données « de santé » ne sont pas ici en soi citées : elles sont l'objet de textes distincts, que nous avons vu *supra* dans l'examen des mécanismes pré-crise, et verrons

[865] Avis 3/2020 préc., spéc. page 7, points 21 et suiv.
[866] Cela ne relève donc pas d'une qualification préalable par une juridiction ou une autre entité, mais relève des procédures de droit national.
[867] Définies à l'article 2 de l'annexe de la recommandation 2003/361/CE.
[868] J. de La Fontaine, « Le Lion et le Rat », onzième Fable du livre II.

infra avec l'examen du règlement dédié à l'EEDS de 2022. Mais par nature, nombre de « déterminants de la santé » sont appréciables au travers de données qui les expriment, soit de façon intrinsèque, soit par croisement (eau, alimentation, consommations, regroupements humains, salubrité, énergie, communication, etc). Le parallèle est donc intéressant.

Nous avons relevé que le CEPD s'était félicité de l'invocation de la notion « d'intérêt public », et de son interchangeabilité avec la notion antérieure de « bien public » [869]. Cela est une façon élégante, de la part du CEPD, **de ne pas demander, lors de l'examen du projet, d'aligner, d'un point de vue sémantique, les catégories d'exception** entre le RGPD de 2016 et la proposition qui a été déposée en 2022.

En effet, le RGPD excipe de « l'intérêt public » pour le traitement licite de certaines catégories de données (article 6§1 point e, si ce traitement est « *nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ») ; **dont les données de santé** (article 9§2, spécialement point i : si ce traitement est « *nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique* (…) » [870]).

Le relevé par le CEPD de l'identité conceptuelle, par-delà la variation sémantique, lui permet de souligner que les deux notions « *répondent aux mêmes objectifs importants, exprimés dans le RGPD (...) et devrai(en)t être soumis aux mêmes exigences* ».
En bref, **il ne saurait y avoir d'écart d'interprétation entre les conditions de mise en œuvre**, ce qui est une façon par voie doctrinale, d'éclairer un éventuelle contrôle juridictionnel. Il n'y a là **pas de différence de degré, *a fortiori* de nature, des qualifications**.

Cette exception donc stricte n'est acceptable, **que si elle n'emporte pas de réutilisation ultérieure de données** obtenues sur fondement de l'article 15, pour des finalités commerciales lucratives, comme notamment ici l'assurance et le marketing. Ainsi, le CEPD considère à l'avance (en 2020), qu'un « détournement d'usage » serait violer les principes du RGPD (art. 5) « *mais pourrait aussi miner la confiance des citoyens, qui est un élément*

[869] Avis 3/2020 préc., point 22 et s.
[870] Il les y définit de façon non exhaustive : « tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux » (article 9§2 point i).

fondamental de la stratégie » [871], ce dont l'article 19 de la proposition de 2022 prend acte : les autorités nationales ou européennes ayant activé l'article 14 ne **doivent utiliser les données que pour la finalité exclusive** de la demande sur fondement de l'article 14 (a), puis les détruire une fois ses motifs épuisés (c).

Qu'en est-il de l'article 19 (b) ? il énonce, au rang des obligations à charge des organismes nationaux et européen dans ce contexte de l'article 15, de mettre « *en œuvre, dans la mesure où le traitement des données à caractère personnel est nécessaire, des mesures techniques et organisationnelles garantissant les droits et libertés des personnes concernées* ». Cela pourrait sembler superfétatoire : cela n'est que l'expression du droit commun du RGPD. Mais **en filigrane, des données à caractère personnel peuvent être demandées, et la situation de crise (dont de santé publique) ne fait pas exception au RGPD.**

§2. DYNAMIQUE NORMATIVE DU REGLEMENT N°2022/868 SUR LA GOUVERNANCE DES DONNEES

Ce règlement (UE) 2022/868 « sur la gouvernance des données » (ou *Data Governance Act*) [872] est une déclinaison sectorielle de la « stratégie européenne pour les données », objet en 2020 d'une communication de la Commission qui met en exergue les enjeux multiples, politiques, économiques et stratégiques [873]. Il amplifie la **construction progressive de l'accès aux données produites et détenues par les Etats et organismes de droit public**.

Pour cela, il étend le champ du règlement 2018/1724 adopté en 2018, dont le but n'était que d'établir un portail numérique unique pour donner accès à des informations, à des procédures et des services d'assistance [874]. Or, l'établissement du marché intérieur et la prévention de pratiques anti-compétitives en matière de données, ont conduit le Parlement européen et le Conseil, sur proposition de la Commission, à préconiser la mise en place de règles et pratiques communes **supposant que soit promulgué un cadre commun de gouvernance**.

---

[871] *Ibid*. préc., point 25.
[872] Règlement (UE) 2022/868 du parlement européen et du conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724
[873] COM(2020) 66 final. Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions – « Une stratégie européenne pour les données ».
[874] Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) n° 1024/2012 (Texte présentant de l'intérêt pour l'EEE.)

Relevons d'abord qu'un des buts explicites, outre les considérations classiques de fonctionnement efficient du marché intérieur et de protection des droits fondamentaux des personnes, est de « *garantir le renforcement* ***de l'autonomie stratégique ouverte de l'Union*** » (considérant n°1), sans préjudice de la libre circulation internationale des données. Il n'est pas lieu de relever ici en profondeur en quoi le Règlement en est un des leviers ; mais on esquissera son apport à l'égard de notre champ de recherche sur les « données de santé » *(A), avant d'en relever les limites inhérentes à son objet général (B).*

A. APPORT DU REGLEMENT N°2022/868 SUR LA GOUVERNANCE DES DONNEES

Certes, le but de ce Règlement est notamment de contribuer à ce que la concurrence sur le marché intérieur **ne soit pas faussée par une asymétrie des règles nationales quant au cadre de gouvernance de ces données** (consid. n°1). Nous relevons ici son rattachement à la qualification « d'autonomie stratégique » européenne, qui n'est naturellement pas propre à la donnée de santé, mais permet une mise en perspective systémique du débat (1), puis esquissons le cas des données protégées détenues par les entités de droit public (2).

1. Un levier au service de « l'autonomie stratégique européenne »

Le concept d'« ***autonomie stratégique*** [875] ***de l'Union*** » est récent. Son ambition était initialement jaugée à l'aune de politiques d'intitulés explicites, comme la Politique étrangère et de sécurité commune (PESC), et la politique de sécurité et de défense commune (PESD). Mais, dans son programme stratégique 2019-2024, le Conseil européen a mis en exergue le besoin d'élargir cette conception originelle en diptyque.

Ainsi, *« La PESC et la PESD de l'UE doivent devenir plus actives et réactives, et* ***mieux s'articuler avec les autres volets des relations extérieures*** *(…) », dont 4 piliers identifiés* [876]*. Face à l'environnement en transformation rapide, et aux enjeux nouveaux, l'Union doit parmi les leviers identifiés, « s'atteler à l'ensemble des aspects de la* ***révolution numérique et de l'intelligence artificielle*** *: les infrastructures, la connectivité, les services, les données* » ; la santé n'a là qu'une place incidente, car il s'agit **d'une finalité parmi d'autres** (même si elle s'avérera primordiale parmi les applications citées), **non d'un moyen nouveau**.

---

875 Le concept « d'autonomie stratégique » est apparu en 1994 dans le Livre blanc sur la Défense, où il désigne une expression fonctionnelle de la souveraineté ; v. M. Long, E. Balladur, F. Léotard, *Livre Blanc sur la Défense 1994*, Documentation française.

876 Conseil européen, Communiqué de presse, 20 juin 2019. Les 4 priorités sont « *protéger les citoyens et les libertés; mettre en place une base économique solide et dynamique; construire une Europe neutre pour le climat, verte, équitable et sociale; promouvoir les intérêts et les valeurs de l'Europe sur la scène mondiale* ».

En 2021, le concept d' « autonomie stratégique » européenne a fait en France l'objet d'un rapport à la lumière de l'expérience de la pandémie de Covid19. Naturellement, celle-ci a mis en exergue la santé, les coopérations alors laborieuses en la matière, et la sécurité de nos approvisionnements stratégiques. Mais ce rapport de noter que l' « ***autonomie stratégique (est) une « percée conceptuelle aux contours imprécis*** » [877]. Cette percée présente des contours un peu plus nets depuis le Congrès de Versailles de mars 2022, qui a immédiatement suivi la tentative d'invasion de l'Ukraine par la Russie [878] ; ses leviers fonctionnels sont en tous cas bien identifiés, notamment dans le champ des technologies numériques.

Bien que l'environnement interne et géopolitique français et européen soient sous tension, ce règlement 2022/868 souligne bien **qu'il ne crée pas une base juridique nouvelle** pour le traitement des données personnelles, « *y compris lorsque les données à caractère personnel et non personnel d'un ensemble de données* ***sont inextricablement liées*** », consid. 4. Il met en exergue la prééminence du Règlement (UE) 2016/679 ou du droit national adopté en application de ce droit dérivé, **en cas de conflit avec ses propres dispositions** (article 1§3).

Dans ce contexte très maitrisé, dans le sillage de la Directive adoptée en 2019 et d'objet similaire [879], le nouveau règlement de 2022 établit des conditions générales applicables à l'utilisation secondaire des données **du secteur public**.

2. Le cas des « données protégées » détenues par des entités de droit public

Du fait de ses objectifs (réutilisation de données détenues par des organismes du secteur public, cadre de notification et surveillance pour l'activité de services d'intermédiation de données, enregistrement volontaire des plateformes à finalité altruiste, et institution d'un « *Comité européen de l'innovation dans le domaine des données* »), le règlement relève (consid. 63) que l'intervention au niveau de l'Union est nécessaire en application de l'article 5 TFUE, ces objectifs **ne pouvant être atteints de façon satisfaisante au niveau des Etats membres** du fait de leurs dimensions et effets.

---

[877] Mme M. Gatel, D. Quentin, *Rapport d'information (...) sur le sujet de l'autonomie stratégique de l'Union européenne,* n°4822 publié le 16 déc. 2021 ; auparavant, Mme H. Conway-Mouret, R. Le Gleut, *Rapport Défense européenne, le défi de l'autonomie stratégique* », Sénat, n° 626 (2018-2019) publié le 3 juillet 2019.
[878] Réunion informelle des chefs d'État ou de gouvernement « Déclaration de Versailles 10 et 11 mars 2022 », non autrement référencée. https://www.consilium.europa.eu/media/54777/20220311-versailles-declaration-fr.pdf
[879] Directive (UE) 2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

* L'article 3 du règlement (UE) 2022/868 énonce les données soumises au régime particulier du chapitre II du règlement. On y retrouve notamment le secret statistique précité (article 3§1b), et les données à caractère personnel, dans la mesure toutefois où elles ne relèvent pas de la directive 2019/1024 qui s'applique aux institutions européennes. **Cela recouvre les données de santé, dans les conditions** de disponibilité par ailleurs évoquées.

Pour autant, ce règlement ne s'applique pas aux « *données détenues par des organismes du secteur public qui sont protégées pour des raisons de sécurité publique, de défense ou de sécurité nationale* », dont nous avons vu que la qualification relevait d'une appréciation autonome, en fait souveraine car inconditionnelle, par les Etats (article 346 TFUE, ex article 296 TEC) [880]. **Or, cela peut inclure les données de santé** publique lorsque, selon les circonstances appréciées par eux, elles sont rattachables aux catégories précitées. Ces circonstances peuvent justifier des restrictions exceptionnelles aux principes de liberté de circulation, notamment de médicaments d'intérêt thérapeutique majeur [881].

*** La réutilisation des données (usage secondaire) relevant du Chapitre II est prévue par le règlement**. Elle ne peut donner lieu à accords « *qui octroient des droits d'exclusivité ou qui ont pour objet ou pour effet d'octroyer de tels droits d'exclusivité ou de restreindre la disponibilité des données à des fins de réutilisation par des entités autres que les parties à ces accords ou autres pratiques* » (article 4§1), sauf s'il s'agissait de la « *fourniture d'un service ou d'un produit* ***d'intérêt général qui sans cela, ne pourrait être obtenu*** » (ibid., §2).

Or, dès ici pointe la problématique de la capacité technologique de traitement des données (enjeu d'autonomie stratégique, donc de souveraineté), **qui peut conduire à un monopole ou oligopole d'opérateurs**. Or, cela recoupe ici, sous un angle public (car ces capacités ne sont pas détenues par tous les Etats), les questions formalisées sous un angle privé par le Règlement sur le marché numérique, dans le but de prévenir ou de sanctionner les positions dominantes par des plateformes de services essentiels.

---

880 Article 346§1-a) « *aucun État membre n'est tenu de fournir des renseignements dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité* ».

881 Ainsi, L. Collet, « Pénurie de médicaments et stocks de sécurité en France : fondement juridique », Bull ANM 2023, 207, pp 136-141, et la bibliographie citée par l'auteur.

Nous y reviendrons, car la non-maîtrise nationale de la technologie de traitement des données peut conduire à une exception temporaire au règlement 2022/22, et pose la question **du transfert transfrontières hors UE des données de santé** dans une telle hypothèse.

B. CONSIDERATIONS SUR LE REGLEMENT N°2022/868 SUR LA GOUVERNANCE DES DONNEES

Ces considérations se limiteront naturellement à l'objet de notre étude. L**e règlement étant de portée générale** pour les données détenues par les entités publiques, il est peu étonnant que les données de santé n'y soient pas spécialement développées dans le corps normatif. Pour autant, elles présentent de nombreuses occurrences dans les considérants (1).

Au regard du résultat de nos recherches jusqu'ici, l'analyse du règlement suscite quelques points d'étonnement, quant aux conditions juridiques d'utilisation secondaire (2).

1. Place des « données de santé » dans le Règlement 2022/868

En première partie de notre recherche, nous avons vu l'importance prise par les données de santé individuelles (personnelles, pseudonymisées, anonymes avec une granulométrie utile). Ces données sont partout dans le monde devenues la **source d'une florissante économie de la donnée**, sachant en France la prépondérance en la matière des données de santé « publiques » sur les données de santé « privées », du fait du statut des bases [882].

Dans ce contexte donc, le Règlement 2022/868 souligne que « *lorsqu'il existe des conditions de concurrence équitable dans l'économie des données, les entreprises se font concurrence* ***sur la qualité des services, et non sur la quantité des données*** *qu'elles contrôlent* » (ibid., consid. n°2). Ce règlement énonce alors, à défaut de priorités sectorielles dont la fixation n'est pas son objet politique, des champs d'intérêt spécifique de **production de tels effets qualitatifs** dont la mise à disposition de la donnée est un moyen.

Or, la santé est le premier exemple cité, dès le considérant n° 2 du Règlement 2022/868 ; la particularité du champ « santé » est aussi le caractère hautement consensuel du gain qualitatif.

[882] Cf. La distinction esquissée dans un document du Conseil d'Etat en 2018 ; nous avons souligné que cette distinction ne s'entendait que du support sur lesquelles les données devenaient disponibles, notamment le « Système national des données de santé », *supra*.

Ainsi, « *les données sont au cœur de cette transformation: l'innovation fondée sur les données apportera des avantages considérables aussi bien aux citoyens de l'Union qu'à l'économie,* ***par exemple en améliorant et en personnalisant la médecine*** *(...)* » [883]. Mais le but du règlement n'est, ici, que **d'améliorer les conditions** du partage des données dans le marché intérieur, sans préjudice des nombreux textes préexistants [884]. Il n'atteint pas les compétences nationales en matière d'activités relatives à la sécurité publique, à la défense et à la sécurité nationale, **dont la santé publique est parfois consubstantielle**.

Après de nombreux développements justifiant ses choix normatifs sur des points politiques et techniques, la santé **apparaît à nouveau comme le premier exemple,** dans la recherche de confiance dans les mécanismes de réutilisation, **notamment en cas de transfert vers des pays tiers**. Mais alors, il ne s'agit plus ici seulement de « données personnelles de santé », entendues comme identifiant la personne concernée. En effet, le règlement invoque « *par exemple,* ***dans le domaine de la santé****, certains ensembles de données détenus par des acteurs du système de santé publique, tels que les hôpitaux publics, (qui)* ***pourraient être reconnus comme des données relatives à la santé hautement sensibles*** » (consid. n°24).

Dès lors, il invite à leur définition pour une protection spécifique, laquelle définition sera, non l'apport du Règlement 2022/868, mais de la proposition de Règlement sur l'EEDS, *infra*.

En fin de compte, si à plusieurs reprises, les considérants du règlement (UE) 2022/868 évoquent les « données de santé » comme des données d'intérêt particulier, **le corps du règlement est peu disert** (un texte dédié allait s'en suivre). Son article 5§2 dispose seulement que « *Les conditions applicables à la réutilisation sont non discriminatoires, transparentes, proportionnées et objectivement justifiées en ce qui concerne les catégories de données et les finalités de la réutilisation,* ***ainsi que la nature des données pour lesquelles la réutilisation est autorisée*** (…) ».

---

[883] Question déjà couverte, on l'a vu, par la Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers.

[884] Des dix textes visés, seuls nous intéressent ici : Règlement (CE) n°223/2009 du 11 mars 2009 relatif aux statistiques européennes ; Règlement (UE) 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne ; Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») ; Directive 2007/2/CE du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE) ; Directive (UE) 2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.

2. Conditions quant aux conditions juridiques d'utilisation secondaire

La « *réutilisation* » est ici entendue (article 2, point 2) comme l'« *utilisation, par des personnes physiques ou morales, de données détenues par des organismes du secteur public, à des fins commerciales ou non commerciales* ***autre que l'objectif initial de la mission de service public pour laquelle*** *les données ont été produites* ». Nous verrons qu'elle donne lieu à une définition circonstanciée en 2022 dans le champ des données de santé, ainsi que le périmètre de données concernées au titre de l'énoncé de « catégories minimales » (*infra*).

En attendant, cet article 2.2 **assimile les faits de détention et de production**. Cela met aussi en perspective la distinction entre « données publiques » et « données privées », apparue de façon fugace en santé sous l'égide du Conseil d'Etat en 2018, sans fonder là une doctrine : en l'état, la question n'est, soulignons le à nouveau, que celle du statut des réservoirs des « données de santé », institués en France **pour une mission de service public.** Leur accès est subordonnée à une procédure spécifique qui n'est pas l'objet de notre thèse.

* Bien que le Règlement 2022/868 porte essentiellement sur des données détenues **par les organismes du secteur public** [885], il relève l'émergence d'un marché compétitif. Il en identifie et en régule soigneusement les acteurs, notamment les « *services d'intermédiaires de données* » privés ou publics [886] ; il comprend nombre de dispositions relatives aux activités impliquant des transferts de données vers des pays tiers. **L'échelle de raisonnement n'est pas purement intracommunautaire,** mais bien celle d'une économie globalisée compétitive.

En outre, ces transferts font l'objet d'un chapitre VII dédié « *accès international et transfert international* », constitué d'un unique article (article 31), lequel traite spécifiquement des données à **caractère non personnel**. Il comprend notamment une disposition subordonnant la force exécutoire de toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers, qui exigerait un accès à des données de la part des acteurs qui auraient pu y avoir accès au titre du règlement 2022/868, sans un accord international avec l'Union (article 31§2) ;

[885] Définis par l'article 2,§17 et § 18 de façon large : incluant institutions et autorités publiques de tous niveaux, leurs associations et combinaisons, entreprises publiques, organismes d'intérêt général sans caractère industriel et commercial.

[886] Objet d'une définition développée par l'article 2, § 11, scindé en quatre parties lesquelles portent exclusion de ce que n'est pas un service d'intermédiation des données. Cette activité fait l'objet d'un encadrement très précis par les articles 10 à article 14, l'article 15 n'ayant que pour but d'écarter de ce concept, les activités relevant du concept d'altruisme en matière de données (objet des articles 16 et s.).

mais cet article de ne citer que des accord internationaux « *tel qu'un traité d'entraide judiciaire en vigueur entre le pays demandeur et l'Union* », ou « *tout accord de ce type entre le pays tiers demandeur et un Etat membre* ». Or, cela peut poser question : **il n'est pas précisé que l'Etat membre dont il s'agit**, est ou non l'Etat dont émanent les données détenues par un autre acteur, et qui sont demandées par un Etat tiers.

* Dans ce contexte, l'article 5§13 contient une disposition emblématique **relative à la qualification des données,** en cas de transfert vers un pays tiers, qui, énoncée en amont de l'article 31, n'est pas reprise par ce dernier.

Ainsi selon l'article 5§13, des actes législatifs de l'Union « *peuvent considérer que certaines catégories de données à caractère personnel détenues par des organismes du secteur public* (nationaux ou européens) *sont* ***hautement sensibles*** *aux fins du présent article,* ***lorsque leur transfert vers des pays tiers peut mettre en péril des objectifs de politique publique de l'Union, tels que la sécurité et la santé publique****, ou peut entraîner un* ***risque de ré-identification de données anonymisées à caractère non personnel*** ».

Or, nous constatons ici que, conformément à son concept « d'autonomie stratégique », **c'est l'Union qui prend la main** (« *peut mettre en péril des objectifs (…) de l'Union »)*.

En outre, le règlement indique alors raisonner en termes de « *catégories de données* » pour « *ces conditions particulières* » (article 5§13, al. 2), sans jamais **invoquer explicitement un critère de contexte géopolitique,** lequel seul pourrait *a priori* justifier ces exceptions. En conséquence, le critère étant objectif (celui de des « *catégories de données* »), des actes législatifs d'une telle nature seraient **applicables à tous Etats tiers**.
Cependant, leur portée peut être graduée (de « conditions » à des « restrictions », en passant par des « limitations »). Par ailleurs, le texte n'évoque pas « *les* », mais « *des* » pays tiers (*ibid.*, al. 3) ; enfin il évoque des « *pays* », non des « *Etats* », avec l'effet d'émousser la question géopolitique ?

Sans donc le formuler explicitement, l'article 5§13 laisse la possibilité d'actes sélectifs traitant certes de catégories de données « *hautement sensibles* », **mais au regard évidemment de contextes** géopolitiques de destination (au double sens ici de lieu, et

d'usage). La désignation sélective d'une catégorie de données à fin de limitation/restriction de transfert vers un Etat particulier prendrait évidemment une forte signification politique [887].

SECTION II. VERS LA CONCRETISATION DE L'ESPACE EUROPEEN DES « DONNEES DE SANTE » (EEDS) ?

Nous venons de voir comment le règlement 2022/868 sur la « gouvernance des données » **réalisait une des facettes de la « *stratégie européenne pour les données* », consubstantielle à son concept d' « *autonomie stratégique européenne* »**. Mais si ce règlement évoque fréquemment les « données de santé » comme exemple emblématique, il n'en traite pas spécifiquement – comme d'aucune autre donnée d'ailleurs.

En effet, la « *stratégie européenne pour les données* » (communication de 2020) et d'autres doctrines formulées dans un faisceau convergeant [888], annonçaient un espace européen unique des données, lequel serait concrétisé de façon nécessairement sectorielle. Dans ce contexte, **le champ des données de santé est l'objet de la première proposition spécifique**.

Il s'agit d'une priorité [889], qui relève explicitement d'une « **commission géopolitique** » [890].

En mai 2022, la **proposition de règlement dédié aux données de santé**, « *relatif à l'espace européen des données de santé* » dit EEDS est ainsi publiée [891]. Loin de se réduire à un outil de gouvernance des données sur un marché dédié, cet espace est perçu comme **partie intégrante sinon comme socle**, **d'une « *union européenne de la santé* »** [892].
Outre ses copieux considérants, son article 1 énonce ainsi ses buts : renforcer des droits existants du patient (article 1-a), instituer un cadre unifié de dossiers personnels électroniques interopérables et l'utilisation secondaire des données de santé (*ibid*., -b, -c), et imposer des infrastructures obligatoires pour le partage des données de santé (-d, -e).

---

[887] Cela est à bien distinguer de la question des transferts de données objet des jurisprudences « *Privacy Shield* » et « *Safe Harbour* » de la CJUE, que nous étudierons dans le titre II de cette seconde partie de notre thèse.
[888] Not. Conseil de l'Union Européenne, « Conclusions du Conseil intitulées 'Façonner l'avenir numérique de l'Europe' » 9 juin 2020, n° 8711/20 ; Parlement européen, Rapport A9-0149/2021, « Rapport sur le thème « Façonner l'avenir numérique de l'Europe: supprimer les obstacles au bon fonctionnement du marché unique numérique et améliorer l'utilisation de l'IA pour les consommateurs européens », 2020/2216(INI).
[889] Lettre de mission de la présidente de la Commission U. von der Leyen, à S. Kyriakides, Commissaire pour la santé et l'alimentation, datée 1er déc. 2019 (en anglais), non autrement référencée.
[890] *Ibid*., lettre de madame U. von Der Leyen à S. Kyriakides, page 2.
[891] Présenté par la Commission le 3 mai 2022, « Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé », (COM 2022)197 final, 2022/0140 (COD).
[892] Proposition de Règlement 3 mai 2022, préc. in « Exposé des motifs », page 1.

A la différence des normes européennes précédentes, qui lui tiennent lieu d'étais [893], cette proposition est entièrement dédiée aux « données de santé ». Ce qui nous intéresse, n'est donc pas la place que la notion tient dans un texte dont elle est la raison d'être [894] ; encore sa **définition même y est-elle étendue au-delà** de la définition de la première définition en 2016 de la « donnée de santé » par le RGDP, nous l'avions vu dans notre première partie.

Ce qui nous intéresse ici, est **sa mise en perspective selon une dynamique et une échelle inédites**, nourries du fondement combiné des articles 16 et 114 du TFUE précités. En effet, l'invocation des droits des citoyens/patients européens en la matière, nous apparaît un **levier de transformation des infrastructures numériques** (§1) : le but est aussi de rendre obligatoire ce prérequis de l'autonomie stratégique européenne (§2).

§1. LES DROITS DES PATIENTS/CITOYENS, LEVIER D'UNE TRANSFORMATION D'ECOSYSTEME EUROPEEN

La proposition met en exergue **l'intérêt primordial du patient (données de santé) /citoyen (données de bien-être) : celui-ci doit pouvoir accéder à ses données en toute mobilité**, **jouir de leur portabilité,** en ouvrir / restreindre sélectivement l'accès etc. (article 3) selon les règles de droit national, dans le respect du règlement à venir.

Puis, dans la logique de production des soins et de continuité des parcours, la proposition organise l'accès des données aux professionnels de santé (article 4), sur la base d'un socle minimal de données de santé exigibles (article 5), avec un format d'échange électronique interopérable (article 6), des modalités unifiées d'enregistrement (article 7) etc.

Il n'est pas lieu de passer en revue ces **droits nouveaux intéressant la relation individualisée de soins**, externes à notre propos, **mais les obligations des Etats membres** et opérateurs qu'ils régissent. Ainsi, l'article 1.2 de la proposition souligne que le règlement « *d)*

[893] Outre les RGPD de 2016 et Règlement 2018/1725 sur le traitement des données personnelles, et la Directive sur les soins transfrontières de 2011 précédemment analysés, et la proposition de règlement sur les données (Data Act), il s'agit notamment des Règlement (UE) 2017/745 relatif aux dispositifs médicaux, Règlement (UE) 2017/746 relatif aux dispositifs médicaux, et de la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, COM(2021) 206 final. Nous ne développerons ci-après que cette dernière, car son objet est le **traitement des données de santé**. Il n'est en effet pas nécessaire dans les développements qui suivront, de revenir sur nos réflexions sur le droit des DM et des DMDIV en tant que technologies qui concourent à la **production de données de santé**.

[894] On rappellera ici un travail préalable précité, l'étude de la Commission européenne (2020) « Assessment of the EU Member States rules on health data in the light of GDPR ».

met en place une ***infrastructure transfrontière obligatoire permettant l'utilisation primaire des données de santé*** *électroniques dans l'ensemble de l'Union ; e) met en place une* ***infrastructure transfrontière obligatoire pour l'utilisation secondaire des données de santé*** *électroniques* ».

Nous proposons, selon toujours le fil rouge de notre raisonnement sur les données, d'examiner leur place dans l'obligation d'infrastructures inédites pour le partage des données de santé (A), avant d'examiner les conséquences en termes de catégorisation juridique de ces données, de l'avènement d'une obligation d'un cadre pour leur usage secondaire (B).

A. L'OBLIGATION D'INFRASTRUCTURES INEDITES POUR LE PARTAGE DES DONNEES DE SANTE

L'existence d'un dossier médical électronique (DME) interopérable, qui par la fluidité des données contribue à la mobilité des patients, est un enjeu mis en exergue par les limites constatées de la directive 2011/24, *supra*.

Après des recommandations du Conseil européen en 2017 [895], cet enjeu a en 2019 conduit à une recommandation de la Commission européenne [896], **dont le « mode incitatif » habille des prescriptions d'investissement, et d'utilisation d'un outil préexistant** : l'infrastructure de services numériques dans le domaine de la santé en ligne financée au titre du mécanisme pour l'interconnexion « *refined eHealth European Interoperability Framework* » [897].

En 2022, un cran supplémentaire est donc franchi.

Si la Commission ne retient pas la stratégie maximale qui consistait à confier, à un organe de l'Union, la définition d'exigences communes et l'accès transfrontières aux données électroniques, elle **s'écarte de la stratégie de simples coopérations renforcées à base volontaire.** Ce qui nous intéresse ici, est qu'il est ainsi prévu une obligation de création d'un DME unifié au plan européen pour le recueil de données (1), avec lequel des applications de bien-être peuvent être interopérables ; ce qui nous conduit à nous interroger sur la transformation juridique de leur statut (2).

[895] Conclusions du Conseil sur la santé dans la société numérique - réaliser des progrès en matière d'innovation fondée sur les données dans le domaine de la santé, 017/C 440/05 (JO 21 déc. 2017).
[896] Recommandation (UE) 2019/243 de la Commission du 6 février 2019 relative à un format européen d'échange des dossiers de santé informatisés
[897] Cadre d'interopérabilité européen affiné dans le domaine de la santé en ligne, adopté en 2015.

1. La création obligatoire d'un DME unifié, pour quelles données ?

Nous avons vu que la recommandation de 2019 préc. du Conseil avait mis en exergue les principes de l'accès aux dossiers de santé informatisés et de leur échange transfrontalier (points 8 à 10), du besoin d'un format européen d'échange (point 11), l'élaboration d'un tel format (points 12 à 17), en soulignant à chaque fois le rôle actif des Etats membres. **La proposition de règlement EEDS 2022 acte donc un renversement de perspective.**

En effet, l'infrastructure transfrontalière pour l'utilisation primaire des données de santé électronique » **devient obligatoire** (article 12), avec l'effet de généraliser MaSanté@UE (*MyHealth@EU*), plateforme à laquelle nous avons vu que la France était déjà connectée. Le but est donc de généraliser la possibilité d'échanges bidirectionnels avec les points de contacts nationaux (en France, l'ANS), auxquels doivent être connectés les prestataires de soins (article 12§5) et les pharmacies (article 12§6), sans préjudice d'une extension nationale de services complémentaires **sur une base facultative** (article 13) [898].

Dans ce contexte, le DME (dossier médical électronique) y est défini comme un « ***ensemble de données de santé électroniques*** *relatives à une personne physique* ***collectées dans le système de santé et traitées à des fins de soins de santé*** » (article 2.2, m). Un système de DME est défini comme « *tout appareil ou logiciel destiné par son fabricant à être utilisé pour le stockage, l'intermédiation, l'importation, l'exportation, la conversion, l'édition ou la consultation* ***des dossiers médicaux électroniques*** » (article 2.2, n).

En première partie de cette thèse, nous avons vu l'avance française matière de DME, consistant en l'ouverture opérationnelle en 2022 de l'espace numérique de santé (ENS) ; et l'attente de textes complémentaires pour l'admission de technologies qui pourraient l'abonder. Cela est une anticipation nationale du droit européen à venir.

La proposition (article 3.6) prévoit que les titulaires « *peuvent* ***ajouter des données de santé électroniques*** *dans leur propre DME ou dans celui des personnes physiques dont elles*

[898] Par l'intermédiaire de MaSanté@UE, les Etats membres peuvent fournir de tels services pour faciliter « *la télémédecine, la santé mobile, l'accès des personnes physiques à leurs données de santé traduites ou l'échange ou la vérification de certificats liés à la santé, y compris des services de carnets de vaccination (…) la surveillance de la santé publique ou les systèmes de santé numérique, ou des services et applications interopérables, en vue d'atteindre un niveau élevé de confiance et de sécurité, de renforcer la continuité des soins et de garantir l'accès à des soins de santé sûrs et de qualité* ».

peuvent consulter les informations de santé » et en consacre la portabilité [899]. **Dès lors, qu'entend-on ici par « données de santé électronique » personnelles ?**

***** L'article 2.2.a les définit comme les *«* données concernant la santé et les données génétiques **telles que définies dans le règlement (UE) 2016/679, *« ainsi que les données*** *se rapportant aux déterminants de la santé, ou les données traitées dans le cadre de la prestation de services de soins de santé, qui existent sous forme électronique* ». La définition par le RGPD **ne semble pas suffire** ; c'est logique pour les déterminants de santé, moins pour les données traitées dans le cadre de la prestation de services de soins de santé [900].

*** Or, n'y a-t-il pas un défaut de congruence** avec la définition de l'« *application de bien-être* » ? Celle-ci est en effet entendue comme (article 2.2.o) « *tout appareil ou logiciel destiné par son fabricant à être utilisé par une personne physique* ***pour le traitement de données de santé électroniques à d'autres fins que les soins de santé****, par exemple à des fins de bien-être ou de poursuite de modes de vie sains* ». Ainsi, cette définition semble intégrer dans le champ de la « donnée de santé électronique », des informations qui, selon la définition intrinsèque de celle-ci (article 2.2.a), n'y figurent pas : des objets et applications de bien-être ne se contentent pas de « traiter » des données, elles en produisent, *infra*.

Dès lors, quelles « données de santé » doivent, selon la proposition de règlement, être impérativement partageables ? Elles sont énoncées au titre des « *Catégories prioritaires de données de santé électroniques à caractère personnel à des fins d'utilisation primaire* » (article 5), dont la liste est modifiable par acte délégué de la Commission (article 5.2), *infra*.

Les catégories prioritaires que l'on peut ainsi dire natives (article 5.1) recouvrent les : « *a) dossier de patients; b) prescriptions électroniques; c) dispensations électroniques; d) images médicales et comptes rendus d'imagerie médicale ; e) résultats de laboratoire; f) lettres de sortie d'hospitalisation* », sachant que l'annexe I de la proposition rapporte les contenus concrets. Mais l'accès aux données de santé électroniques à des fins d'utilisation primaire et l'échange de ces données **peuvent en outre être autorisés pour d'autres catégories de**

---

[899] Elles ont « *le droit de donner l'accès à leurs données de santé électroniques à un destinataire de données de leur choix* ***du secteur de la santé ou de la sécurité sociale****, ou de demander à un détenteur de données de les transmettre à un destinataire de données de leur choix* (des mêmes secteurs) » de façon immédiate et gratuite, sans entraves du détenteur de données ou des fabricants des systèmes.

[900] Pour rappel, l'article 4.15 RGPD définit les données de santé comme « *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* ».

données de santé à caractère personnel disponibles dans le DME (article 5, dernier alinéa). Ce champ est donc large, et consacre une ouverture forte des données de santé concernées.

Pour autant, le RGPD **n'avait pas d'optique sanitaire, mais une optique de protection**. Nous avons relevé en introduction puis en première partie que sa définition tautologique **traçait en droit un cadre accueillant, dont nous constatons ici l'extension du contenu**. Quelle que soit la source des données, elles devraient être protégées à ce titre [901]. Mais elle ne l'est que dans l'enveloppe du DME ou du dossier patient, non à l'extérieur.

Enfin que, signalons pour la suite de nos développements quant aux accès illicites (*infra*, titre II) que, en tant que produits comportant des éléments numériques au sens de la proposition de règlement Cybersécurité en septembre 2022 [902], les DME devront en satisfaire les exigences essentielle **de façon cumulative** avec la proposition EESD. Ne seront toutefois pas concernés les DME fonctionnant en mode SaaS (*Software as a service*), ni les DME mis au point et utilisés en interne (ils ne relèvent pas du champ d'application du présent règlement, car ils ne sont pas mis sur le marché).

2. L'abondement du DME par des « applications de bien-être » enregistrées : quelles conséquences pour les « données de santé » ?

Le point qui nous intéresse est celui des technologies connectées non dispositifs médicaux. La proposition de règlement EEDS **donne la première définition juridique de l'« application de bien être »**, avec des conséquences systémiques : constitue une telle application « *tout appareil ou logiciel destiné par son fabricant à être utilisé par une personne physique* ***pour le traitement de données de santé électroniques à d'autres fins que les soins de santé****, par exemple à des fins de bien-être ou de poursuite de modes de vie sains* » (article 2.2, o).

*** Il ne s'agit donc pas d'une technologie médicale**, dont, selon la définition légale des dispositifs médicaux, on pourrait inférer de la destination aux soins par le fabricant, la production d'une donnée qui serait incontestablement « de santé » [903].

---

[901] Adopté au Sénat le 5 juillet 2023, le rapport d'information n° 848(2022-2023) de Mmes P Gruny et L Harribey sur la proposition de règlement ESSD, ne traite pas de ce point de qualifications ; mais il met en exergue les enjeux de sécurité soulignés dans sa proposition subséquente de résolution (6 juillet 2023).
[902] Proposition (COM(2022) 454 final) de Règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/102.
[903] *Infra*, Partie I

Néanmoins, il reste un critère de destination : il est « ***destiné par son fabricant*** *à être utilisé par une personne physique* ***pour le traitement de données de santé électroniques à d'autres fins que les soins de santé*** *».* Or, cela confère à l'application un statut intermédiaire, entre dispositif médical qu'il n'est pas, et produit/service courant **qu'il n'est pas non plus**. Cela explique l'intégration déjà réalisée, dans la définition du dispositif médical en droit français, de la surveillance de telles « *applications bien être* » par une autorité non sanitaire, *supra*.

Dès lors, en droit, ce n'est ici plus la technologie (DM ou pas) qui qualifie la donnée (de santé ou non) ; mais **la donnée (de santé ou non) qui, hors champ DM, qualifie la technologie (application « bien être », ou autre).**

Or, nous avons vu que des fabricants d'applications pouvaient souhaiter dénier la finalité de « *dispositif médical* » afin de se libérer des exigences correspondantes de certification de conformité, et éventuellement pour éviter la qualification « de santé » de la donnée produite. Mais la **dénégation de qualité de « dispositif médical » n'implique plus la dénégation du statut de « donnée de santé »**… **si le fabricant se plie aux règles proposées en 2022**.

* Dans une section 5 « *autres dispositions relatives à l'interopérabilité* », le texte prévoit le régime de ces applications. Il y est prévu l'étiquetage facultatif (article 31.1), lequel doit, le cas échéant, indiquer « *les* ***catégories de données de santé électroniques pour lesquelles la conformité*** *avec les exigences essentielles énoncées à l'annexe II a été confirmée* (sic) ». Mais l'annexe II **ne cite aucune catégorie de données de santé électroniques** : c'est donc au fabricant d'identifier celles pour lesquelles cette conformité aura été confirmée.

Dès lors, il sera intéressant de voir quelles « *catégories de données de santé électroniques* » seront éligibles sans remettre en cause la qualification « non DM ».

Ceci d'autant que le texte prévoit (article 5.1 dernier alinéa) que « *l'accès aux données de santé électroniques à des fins d'utilisation primaire et l'échange de ces données peuvent être autorisés* ***pour d'autres catégories de données de santé électroniques à caractère personnel disponibles dans le DME*** *de personnes physiques* », implicitement donc, celles précitées [904].

En outre, les « *données de santé électroniques générées par la personne, dont celles générées grâce aux dispositifs médicaux,* ***aux applications de bien-être ou aux autres*** *applications de*

[904] Elles ne figurent en effet pas dans l'article 5 qui énonce les « catégories prioritaires » et renvoi à l'Annexe I, non sans citer spécialement « a) dossier de patients; b) prescriptions électroniques; c) dispensations électroniques; d) images médicales et comptes rendus d'imagerie médicale; e) résultats de laboratoire; f) lettres de sortie d'hospitalisation ».

santé numériques » font partie de celles qui doivent être **obligatoirement communiquées** au titre des utilisations secondaires (article 33. 1,f), nous allons le voir *infra*.

Enfin, l'article 31.7 dispose que les « autorités de surveillance du marché » doivent vérifier la conformité des applications de bien-être avec ces exigences. Ici aussi, on trouve l'expression **d'une autonomie puisque le régime n'est pas celui de la certification des DM** [905]. Comme pour les DME, la proposition de règlement prévoit l'enregistrement des informations sur les applications de bien être **qui auront revendiqué et obtenu une telle étiquette**, dans une base de données accessible au public et tenue par la Commission (article 32).

En revanche, même si la proposition ne le souligne pas (en contraste des articles dédiés au DME), l'application ainsi qualifiée de « bien être » devra se conformer aux exigences de la proposition de 2022 en matière d'obligations horizontales de cybersécurité [906], tout comme les autres applications. Mais il est frappant que celles-ci semblent qualifiées « de santé ».

B. L'OBLIGATION DE L'OUVERTURE DES « DONNEES DE SANTE » NATIONALES AUX USAGES SECONDAIRES

Outre la satisfaction des besoins des patients et organisations de soins, l'EEDS vise à satisfaire les besoins des « *chercheurs, innovateurs, décideurs et organismes de régulation* » ; (pudiquement, il ne cite pas les entreprises), quoiqu'il vise aussi à « *contribuer à un véritable marché unique des produits et services de santé numérique, en harmonisant les règles de manière à renforcer l'efficience des systèmes de santé* » [907]. Le « marché » doit devenir un moyen de satisfaction des besoins de santé.

Certes, le terme n'est pas utilisé pour désigner l'EEDS quant aux données pour utilisation secondaire. **L'article 42 n'invoque pas des « prix », mais des « redevances », versées aux organismes publics ou privés cessionnaires de données** [908] (42§4) ; elles sont fixées par

[905] En outre, les exigences du projet de l'article 31 ne s'appliquent pas aux applications de bien être relevant de la qualification de « systèmes d'IA à haut risque » (article 31.10).
[906] Proposition préc. de Règlement concernant des exigences horizontales en matière de cybersécurité (COM(2022) 454 final).
[907] Proposition de règlement préc., exposé des motifs (motifs non numérotés), page 2.
[908] Elles doivent être « *transparentes, proportionnées au coût de la collecte des données de santé électroniques et de leur mise à disposition en vue de leur utilisation secondaire, objectivement justifiées et non porteuses de restrictions de la concurrence* ».

l'organisme responsable de l'accès aux données de santé en cas de désaccord (42§5), ou par un organisme *ad hoc*, en cas de désaccord persistant [909].

Ainsi, il s'agit bien d'un marché, mais quasi administré : la cession des données telles que définies est obligatoire et encadrée par le règlement, mais le prix n'est pas intégralement formé par la compétition [910]. Du fait de sa spécificité, la « *donnée de santé »* même *« d'usage secondaire* » **n'est définitivement pas un bien relevant du commerce de droit commun.**

Ce texte spécifique confirme néanmoins la dynamique observée (1). Sur cette base, nous considérerons la définition et la surveillance de ces « usages secondaires » **pour lesquels la cession des données ne peut être refusée (2).**

1. La proposition de 2022 porte une catégorisation inédite des utilisations des données

Dans la première partie de notre thèse, nous avons déjà vu que la distinction des usages possibles avait induit une sous-catégorisation des « données de santé ». Celle-ci est particulièrement explicite dans la proposition de règlement EEDS de 2022, lequel vise à remédier à la dispersion des droits nationaux et surtout à dessiner un véritable cadre d'échange.

Ainsi, il comprend notamment un Chapitre II tiré « *Utilisation primaire des données de santé électroniques* », composé de 14 articles (5 à 13) répartis en deux sections ; et un chapitre IV chapitre IV titré « Utilisation secondaire des données de santé électroniques », composé de 26 articles (33 à 58) répartis en 5 sections [911]. De façon évidente, la proposition de règlement EEDS de 2022 **met en exergue le droit des usages secondaires, du fait de son importance stratégique** précitée pour l'Union.

Ce qui nous intéresse ici, n'est pas le régime de chacune de ces catégories, mais les notions qui les sous-tendent. Ainsi, l'article 5 définit des « *Catégories prioritaires de données de santé électroniques à caractère personnel* ***à des fins d'utilisation primaire*** *»* ; l'article 33 énonce des « *Catégories minimales de données électroniques* ***destinées à une utilisation secondaire*** ».

---

[909] Accès aux organismes de règlement des litiges prévus à l'article 10 du règlement sur les données.

[910] Cette approche est intéressante et heureuse. Mais elle ne saurait égaliser les rapports de force subséquents : les services digitaux nourris de données cédées à prix quasi-administrés, seront facturés à des prix non administrés, *infra.*

[911] Section 1, « Conditions générales relatives l'utilisation secondaire des données de santé électroniques » ; section 2, « Gouvernance et mécanismes pour l'utilisation secondaire des données de santé électroniques » ; section 3, «autorisation de traitement de données pour l'utilisation secondaire des données de santé électroniques » ; section 4, « accès transfrontière aux données de santé électroniques à des fins d'utilisation secondaire » ; section 5, « qualité et utilité des données de santé à des fins d'utilisation secondaire ».

Or, **ces qualifications de « *catégories prioritaires* » et « *catégories minimales* » sont fondamentales** : elles dessinent le périmètre, et l'impérativité, d'un socle de raisonnement que l'on va voir à nouveau dynamique. Nous avons vu précédemment les « catégories prioritaires » énoncées dans l'article 5 assez court, *supra*. En contraste, l'article 33 est copieux, **bien que traitant de « *catégories minimales* »** de données, que l'on va de surcroît voir à fort potentiel d'extension. Ainsi, les détenteurs de données [912] **ont l'obligation légale** de mettre à disposition à fins d'utilisation secondaire, les :

*« a) DME; b) données **ayant une incidence sur la santé**, **dont les déterminants sociaux, environnementaux et comportementaux de la santé**; c) données génomiques sur les pathogènes pertinentes, ayant une incidence sur la santé humaine; d) données administratives relatives à la santé, dont les données relatives aux demandes et aux remboursements; e) données génétiques, génomiques et protéomiques humaines; f) données de santé électroniques générées par la personne, dont celles générées grâce aux dispositifs médicaux, **aux applications de bien-être ou aux autres applications de santé numériques**; g) données d'identification relatives aux professionnels de santé intervenant dans le traitement d'une personne physique h) registres de données de santé à l'échelle de la population (registres de santé publique); i) données de santé électroniques contenues dans les registres médicaux concernant des maladies spécifiques; j) données de santé électroniques provenant d'essais cliniques ;k) données de santé électroniques provenant de dispositifs médicaux et des registres des médicaments et des dispositifs médicaux; l) cohortes de recherche, questionnaires et enquêtes dans le domaine de la santé; m) données de santé électroniques provenant de biobanques et de bases de données spécialisées; n) **données électroniques relatives au statut en matière d'assurance, au statut professionnel, à l'éducation, au mode de vie, au bien-être et au comportement qui ont un rapport avec la santé** ; o) données de santé électroniques contenant diverses améliorations, telles que des corrections, des annotations ou des enrichissements, reçues par le détenteur de données à la suite d'un traitement sur la base d'une autorisation de traitement de données ».*

***** Ce qui nous intéresse est ici le **caractère obligatoire, et l'extension de l'obligation** à des données non nativement « données de santé », mais peuvent le devenir par destination :

[912] A l'exception des micro-entreprises (définies selon la Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, JO L 124 du 20.5.2003, p. 36).

Ainsi, les « *b) données ayant une incidence sur la santé, dont les déterminants sociaux, environnementaux et comportementaux de la santé; »* dont alors la liste devra être établie, ce qui peut conduire à une liste longue du fait de l'approche désormais holiste, de la « santé ». De même, relevons les données « f) (…) *générées grâce aux dispositifs médicaux, aux* ***applications de bien-être ou aux autres applications de santé numériques;*** *».*

Or, cela impose de **caractériser les applications** de bien-être, et plus encore les « autres applications de santé numériques », lesquelles par hypothèse ne relèveraient **ni de la catégorie des dispositifs médicaux (pourvue d'une autonomie juridique), ni de la catégorie des applications de bien-être (dépourvue d'autonomie juridique)** [913]. *Idem* pour les données (n) « *relatives au statut en matière d'assurance, au statut professionnel, à l'éducation, au mode de vie, au bien-être et au comportement* ***qui ont un rapport avec la santé*** *».*

En outre, l'article 5.3 dispose que les données de santé électroniques que l'on vient d'énumérer (article 5.1) « ***englobent les données traitées à des fins de fourniture de soins de santé ou de soins*** *(…) collectées par des entités et organismes du secteur de la santé ou des soins, dont des prestataires publics ou privés de santé ou de soins, des entités ou organismes effectuant des recherches dans ces secteurs (…)* ». Cette précision de l'article 5.3 est étonnante : la très grande majorité des *items* de la liste de l'article 5.1 sont, nous l'avons vu, des données issues de la production organique des systèmes « de santé » (incluant soins et assurance des soins).

L**'effet utile postule de ne pas considérer cet article 5.3 comme surabondant : force est donc de considérer** que l'article 5.1 vise en premier lieu toutes les sources de données qui ne sont pas des sources « organiques » du système de santé, mais procèdent de nouvelles technologies et organisations, et de nouveaux usages [914].

***** Enfin, ces deux sous-catégories « prioritaire » (article 5) et « minimale » (article 33) ont en commun **de ne pas être définitivement fixées.** Elles sont en effet ajustables par actes délégués de la Commission [915] : ces derniers peuvent modifier, non seulement le contenu de l'annexe I, **mais aussi le contenu même des articles** 5 (article 5.2) et 33 (article 33.7). Cela

[913] Sur les conséquences pour la qualification des données, de la qualification des technologies utilisées, voir supra notre démonstration in Partie I, titre II. Rappelons que l'article 1§3 de la proposition de règlement, qui définit les débiteurs des obligations, n'évoque pas les fabricants d'« autres applications numériques » …
[914] Sur le critère organique comme critère de qualification juridique des données, voir Partie I, titre II, chap I.
[915] En application de l'article 67 de la proposition.

est frappant dans un tel acte législatif de l'Union. Cela marque aussi une forte plasticité prospective, au service de l'extension potentielle de listes déjà très développées !

Si les cas de modifications ne sont pas cités (on peut imaginer la possibilité, improbable, du retrait d'un type particulier de donnée), **les cas d'ajouts** de données sont en revanche justifiés par les trois critères cumulatifs énoncés par l'article 5.2.

Ainsi, les « *catégories de données de santé électroniques ajoutées* » (doivent) être « ***pertinentes pour les services de santé fournis à des personnes physiques*** » (a) ; doivent être utilisées dans un nombre important de DME adoptés par les Etats membres (b), doivent être couvertes par des normes internationales, ces dernières devant être « *examinées en vue de leur application dans l'Union* ». **On pourrait se demander de quels ajouts il peut encore s'agir** : mais ne s'agit-il pas de l'incorporation au rang des « données de santé » organiques, des données de santé « par destination » ?

Quoiqu'il en soit, **nous relevons ici en quelque sorte un temps d'avance de l'article 33 (données minimales) sur l'article 5 (données prioritaires)** : l'article 33 intègre en effet d'emblée les données qui pourraient être pertinentes (article 33.1 *b), f), et n)* précités) ; tandis que l'article 5 pourrait les intégrer, mais ultérieurement, et sous réserve de la satisfaction des critères précités.
Or, cela marque à nouveau le **dynamisme considérable** de la « donnée de santé » **dans le champ des utilisations « secondaires »** .

2. La proposition de 2022 porte une ouverture obligatoire aux « usages secondaires »

Objet de l'obligation de communication [916] des données anonymisées, la notion « d'usage secondaire » est précisément définie par le règlement dans son article 34. Mais cet article ne trace pas seulement le champ d'une obligation de communication : ce faisant, **il énonce une obligation de ne pas communiquer**. Ainsi, les débiteurs de l'obligation « *ne donnent accès*

[916] Pour rappel, cette proposition de règlement a vocation à s'appliquer à (article 1§3) « a) *aux **fabricants et fournisseurs** de systèmes de DME et d'applications de bien-être mis sur le marché et mis en service dans l'Union, ainsi qu'aux utilisateurs de ces produits; b) aux **responsables du traitement et aux sous-traitants** établis dans l'Union (...) ; c) aux responsables du traitement et aux sous-traitants établis dans un pays tiers qui sont connectés à MaSanté@UE (MyHealth@EU) ou qui travaillent de manière interopérable avec cette infrastructure (...) ; d) aux **utilisateurs de données** auxquels les données de santé électroniques sont mises à disposition par les détenteurs de données dans l'Union ».*

aux données de santé électroniques énumérées à l'article 33[917] ***que si la finalité prévue*** *du traitement poursuivi par le demandeur est conforme* » (liste limitative en encadré) :

> *« a) aux activités pour des raisons d'intérêt public dans le domaine de la santé publique et de la santé au travail, telles que la protection contre les menaces transfrontières graves pour la santé, la surveillance de la santé publique ou la garantie d'un niveau élevé de qualité et de sécurité des soins de santé et des médicaments ou dispositifs médicaux;*
>
> *b) au fait d'aider les organismes du secteur public ou les institutions, organes et organismes de l'Union, dont les autorités réglementaires, dans le secteur de la santé ou des soins, à accomplir les tâches inscrites dans leur mandat;*
>
> *c) au fait de produire des statistiques officielles à l'échelon national, plurinational et de l'Union en rapport avec les secteurs de la santé ou des soins;*
>
> *d) aux activités d'éducation ou d'enseignement dans les secteurs de la santé ou des soins;*
>
> *e) à la recherche scientifique ayant trait aux secteurs de la santé ou des soins;*
>
> *f) aux activités de développement et d'innovation pour les produits ou services contribuant à la santé publique ou à la sécurité sociale, ou à la garantie d'un niveau élevé de qualité et de sécurité des soins de santé, des médicaments ou des dispositifs médicaux;*
>
> *g) à la formation, au test et à l'évaluation des algorithmes, entre autres dans les dispositifs médicaux, les systèmes d'IA et les applications de santé numériques, à la contribution à la santé publique ou à la sécurité sociale, ou à la garantie d'un niveau élevé de qualité et de sécurité des soins de santé, des médicaments ou des dispositifs médicaux;*
>
> *h) à la fourniture de soins de santé personnalisés consistant à évaluer, à maintenir ou à rétablir l'état de santé des personnes physiques, sur la base des données de santé d'autres personnes physiques. »*

Les finalités a), b) et c) ne peuvent toutefois être poursuivies que par**, et donc les données afférentes être accordées** seulement aux « *organismes du secteur public et aux institutions, organes et organismes de l'Union exécutant des tâches qui leur ont été attribuées par le droit de l'Union ou le droit national, y compris lorsque le traitement de données aux fins de l'accomplissement de ces tâches est effectué par un tiers pour le compte de cet organisme du secteur public ou de ces institutions, organes et organismes de l'Union* ». On pourrait considérer que ces tâches relèvent de **missions régaliennes, donc de souveraineté** (article 3§2), et sont exécutées sans préjudice des droits de propriété intellectuelle et du secret des affaires (article 3§4).

Mais ce qui nous intéresse ici est plus l'article 35 : celui-ci énonce, en sus de l'interdiction de communiquer (faite aux débiteurs de l'obligation portée par la proposition de règlement), **une**

[917] Il y a là une ambigüité : ne sont-ce que les données de santé électroniques qualifiées comme telles, ou cela inclut-il les données non qualifiées comme tel sinon par inférence (ainsi la fin de phrase du f), au l) et les données visées par le n) lesquelles « ont un rapport avec la santé ») ?

interdiction de demander (faite aux bénéficiaires potentiels de la proposition de règlement) pour certaines d'utilisations secondaires.

Au passage, on s'étonnera du fait que l'article 35, titré de façon large « *utilisation secondaire interdite des données de santé électroniques* », **ne porte qu'une interdiction de demander par des organismes qui n'en disposeraient pas**, **non une interdiction aux organismes qui en disposeraient nativement**[918]. Toujours est-il que le texte entend exclure les finalités suivantes (article 35, liste limitative dans l'encadré) :

> *« a) prise de décisions préjudiciables à une personne physique sur la base de ses données de santé électroniques; pour être considérées comme telles, les «décisions» doivent produire des effets juridiques ou avoir, de manière similaire, une incidence significative sur la personne physique;*
>
> *b) prise de décisions, à l'égard d'une personne physique ou d'un groupe de personnes physiques, les excluant du bénéfice d'un contrat d'assurance ou modifiant leurs cotisations et leurs primes d'assurance;*
>
> *c) publicité ou activités de marketing auprès des professionnels de la santé, des organisations de santé ou des personnes physiques;*
>
> *d) fourniture d'un accès aux données de santé électroniques, ou mise à disposition d'une autre manière des données de santé électroniques, à des tiers non mentionnés dans l'autorisation de traitement de données;*
>
> *e) mise au point de produits ou de services susceptibles de porter préjudice aux personnes et aux sociétés en général, comprenant, sans s'y limiter, les drogues illicites, les boissons alcoolisées, les produits du tabac ou les biens ou services qui sont conçus ou modifiés de sorte à porter atteinte à l'ordre public ou aux bonnes mœurs. »*

Ce sont là des pétitions de principe : c'est le demandeur, qui doit s'interdire de telles finalités [919].

Nous pensons que **ces dispositions seront rapidement l'objet de contentieux,** tant la présentation des finalités revendiquées pourrait susciter un art dialectique, pour contourner l'interdiction de demander. La réalité de la finalité pourrait certes être contestée par les autorités publiques compétentes responsables des accès (article 36) ; elle pourrait plus encore l'être par des opérateurs en compétition, notamment pour les éléments visés aux b), c) et d).

En effet, il existe en droit français un précédent de contentieux entre compétiteurs, en matière

---

[918] La seule explication qui nous semble valable, est que les organismes qui en disposent nativement (pour usage primaire) n'ont pas vocation à les utiliser directement pour un usage secondaire, encore cela peut-il se discuter.

[919] Selon l'article 46§1, l'organisme de contrôle qui autorise le traitement à usage secondaire, ne peut que contrôler les intentions sur base déclaratoire (ou de précédents) : « *Les organismes responsables de l'accès aux données de santé évaluent si la demande correspond à une des finalités énumérées à l'article 34, paragraphe 1, du présent règlement, si les données demandées sont nécessaires à la finalité indiquée dans la demande (...)* ».

d'usages secondaires ; sa spécificité ne tient qu'au moyen alors vainement invoqué (contestation de la réalité de la pseudonymisation des données, *infra*). **A moins que des partie prenantes conviennent d'une non-agression réciproque sur ces terrains ?** ce qui constituerait une forme d'entente, *infra*. Enfin, il n'est fait aucune référence à des demandes émanant **d'organismes œuvrant ou pouvant œuvrer pour des pays tiers à l'Union** [920].

L'article 35 est peut disert sur ce point : seul son e) évoque la « *mise au point de produits ou de services* ***susceptibles de porter préjudice aux personnes et aux sociétés en général*** » [921], parmi lesquels on pourrait compter les campagnes d'infox colelctive ou sélective [922]. De même, est silencieux l'article 37, lequel énonce les « *tâches des organismes responsables de l'accès aux données de santé* », désignés par chaque Etat membre.

Certes, son b) impose l'information des autorités de contrôle compétentes, lorsque le traitement discuté *« concerne une tentative de réidentification* ***d'une personne physique*** *ou un traitement illicite de données de santé électroniques à caractère personnel* » (encore faudrait-il le savoir). Mais ce faisant, il focalise sur la question de la protection **contre des risques individuels, non contre des risques populationnels**.

Voyons maintenant comment les (projets de) normes européennes anticipent les applications stratégiques de l'espace européen des données de santé.

[920] La section 4 « *Accès transfrontière aux données de santé électroniques à des fins d'utilisation secondaire* » ne traite que des frontières internes à l'Union !

[921] Le e) de préciser que cela « (comprend)*, sans s'y limiter, les drogues illicites, les boissons alcoolisées, les produits du tabac ou les biens ou services qui* ***sont conçus ou modifiés de sorte à porter atteinte à l'ordre public*** *ou aux bonnes mœurs* ».

[922] Sur les enjeux institutionnels aux Etats-Unis, D. Schillinger, R. J. Baron, « Health Communication Science in the Balance », JAMA 2023 (publié en ligne 31 juillet 2023, doi:10.1001/jama.2023.14763) ; sur le pratique observée, V. Suarez-Lledo, J. Alvarez-Galvez, « Prevalence of health misinformation on social media: systematic review ». *J Med Internet Res*. 2021;23(1):e17187.

§2. L'ANTICIPATION NORMATIVE DES APPLICATIONS STRATEGIQUES DE L'EEDS

L'institution d'un « *Espace européen des données de santé* » ne vise pas seulement à concrétiser la liberté de circulation des personnes au travers de l'interopérabilité des systèmes, la mutualisation d'infrastructures, l'unification de critères exigibles etc. pour remédier à la discontinuité découlant d'un cloisonnement des systèmes et de la rétention de données [923].

En effet, **si cette liberté est une promesse du Traité, elle n'est pas en soi un enjeu stratégique pour l'Union** (un faible % de citoyens européens est statistiquement concerné, hors situation pandémique [924]). En contraste, l'importance des dispositions relatives à l'usage secondaire des « données de santé » dans le règlement EEDS témoigne du fait que cet usage et que l'EEDS participent bien d'un **enjeu stratégique européen**. En témoigne aussi la place inédite des « données de santé » dans la plus récente production normative (textes adoptés et projets en cours), laquelle a anticipé l'avènement de l'EEDS dans deux champs stratégiques.

D'une part, celui bien établi de la régulation du marché des produits de santé : il devrait dans l'EEDS, trouver un éclairage inédit pour des applications communautaires dépassant les approches classiques de régulation (A).
D'autre part, le champ de l'intelligence artificielle, déjà évoquée *supra* lors de l'analyse des « données synthétiques » : l'EEDS apporte à son développement **un réservoir potentiel de données pouvant nourrir l'IA**, sous réserve de leur qualification spécifique, laquelle en 2022 marque la première qualification normative de la qualité des « données de santé » (B).

A. ANTICIPATION POUR LA REGULATION EUROPEENNE DES PRODUITS DE SANTE

La confiance des populations et pays membres en un marché intérieur des produits de santé passe notamment par l'édiction claire, l'application rigoureuse et l'évaluation régulière, d'une

---

[923] Y compris en période de crise sanitaire. Mais, si la crise sanitaire a eu un effet accélérateur de l'adoption des nouveaux textes relatifs à l'échange des données notamment, on peut raisonnablement considérer que le potentiel d'échange des données ne devrait pas enrayer le compartimentage des pays pour des applications de gouvernance de crise.

[924] Voir les études précitées, publiée en juin 2023 « Data on cross-border patient healthcare following Directive 2011/24/EU Reference year 2021 » ; auparavant en mai 2022, « Data on patient mobility under Directive 2011/24/EU - Trend report reference years 2018-2020 » (disponibles sur le site de la Commission). Il serait intéressant que les statistiques correspondantes hors Covid fassent l'objet d'un chapitre dédié (du type « être soigné à l'étranger ») dans les rapports *Européens en mouvement*, INSEE/EUROSTAT ; tel n'est pas encore le cas (voir édition 2019). Les données réunies dans l'étude *The future for Patients in Europe*, commandée par la Commission européenne, sont faibles et obsolètes (Contract nº: SP21-CT-2003-501586). Au début des années 2000, ils ne correspondaient qu'à 3 à 4% des citoyens de l'Union. Filhon, Guillaume, et al. « Mobilité des patients et coordination européenne », *Rev. fr. Aff. Soc.*, no. 1, 2012, pp. 103-107.

réglementation commune visant la qualité, la sécurité, l'efficacité des produits de santé commercialisés sur le marché de l'Union [925]. Cette réglementation doit **s'adapter à des technologies de santé innovantes, sur fond parfois d'urgence**, nous l'avons vu.

En outre, depuis peu, l'objectif primordial de sécurité est complété par un cadre impératif d'évaluation, **qui vise à éclairer les décisions nationales** dans les choix d'acquisition de technologies.

Or, dans les deux cas, **les « données de santé » telles que portées par l'EESD y tiennent une place importante, et croissante** : elles sont mises en exergue, tant dans la refonte en 2023 du régime de l'autorisation de leur commercialisation et surveillance européennes (1), que dans le régime d'évaluation commune pour l'aide à la décision nationale. Inédit dans son impérativité, il a été adopté en 2021, et sera applicable à compter de 2025 (2).

1. La refonte en cours des régimes d'autorisation de commercialisation et surveillance

Le régime d'autorisation et de surveillance des produits de santé en Europe est l'objet de nombreux textes de droit dérivés ; en matière de médicaments, ces textes ont été consolidés par la directive 2001/83 CE, laquelle les a codifiés (il n'existe encore rien de tel en matière de dispositifs médicaux).

Mais en 2023, ce régime global est en refonte, du fait notamment de l'ampleur de la transformation sous tension du marché (dont les problèmes de pénuries de médicaments, des besoins sanitaires prioritaires, des défauts de fluidité et d'efficience), des progrès technologiques (thérapeutique, numérique), et de l'impératif de promouvoir la compétitivité de l'Union et son potentiel innovant [926]. La refonte concerne tant la réglementation générale des médicaments [927], que les attributions de l'agence européenne [928].

---

[925] F. Sauer, « les grandes étapes de l'Europe du médicament », Rev. d'histoire de la pharmacie, LXII, n°381, 2014, 61-74.

[926] Cf. la communication de la Commission, « Pharmaceutical Strategy for Europe », COM/2020/761 final.

[927] (COM 2023) 192 final, 26 avril 2023 (en anglais seulement) : Proposal for a Directive of the European Parliament and of the Council on the Union code relating to medicinal products for huma nue, and repealing Directive 2011/83/EC and Directive 2009/35/EC.

[928] (COM 2023) 193 final, 26 avril 2023 (en anglais seulement) : Proposal for a Regulation of the European Parliament and of the Council laying down Union procedures for the autorisation and supervision of medicinal products for human usae and establishing rules governing the European medicine Agency, amending Regulation (EC) n° 1394/2007 and Regulation (EU) n°536/2014 and repealing Regulation (EC) n° 726/2004, Regulation (EC) n°141/2000 and regulation (EC) n° 1901/2006.

Or, ce dernier volet met **spécialement en exergue le recours aux données de santé au-delà des applications classiques** [929] ; notamment les données « *de vie réelle* », pour en faciliter l'accès et l'usage aux entreprises autant qu'aux régulateurs [930], dont les supports techniques ont anticipé la mise en place conceptuelle : tel est déjà un des objectifs du réseau DARWIN (« *Data Analysis and Real World Interrogation Network* ») initié en février 2022, visant à interconnecter l'Agence européenne et l'EEDS notamment.

* Nous voyons ici l'article 166 du projet de règlement présenté en 2023 quant aux attributions de l'Agence en la matière, justifié par trois considérants inédits et fondamentaux :

- Le considérant 60 met en exergue que la prise de décision en matière de police administrative (regulatory decision-making) peut être aidée par l'analyse de données de santé « ***including real world data, where appropriate,*** *i.e. health data generated outside of clinical studies* », d'où la mise en place du réseau DARWIN et l'intérêt de son lien avec l'EEDS. Ainsi « *through these capabilities the Agency may take advantage of* ***all the potential of supercomputing, artificial intelligence and big data science to fulfil its mandate, without compromising privacy rights*** *».* La mission demeure, mais les moyens sont démultipliés.

- le considérant 63 ne traite pas des données de vie réelle (issues de pratiques de soins hors des essais), mais des **données acquises durant les études interventionnelles mêmes**. Ainsi, l'accès aux données individuelles des patients impliqués dans les essais « *is valuable to assist regulators in understanding the submitted evidence (…) the introduction of such possibility in the legislation is important to foster data-driven benefit-risk assessments at all stages of the life cycle of a medicinal product* ». Le but est de mettre en perspective les données fournies par les industriels à l'issue des essais cliniques, ce qui permettrait l'analyse critique du ratio efficacité/sécurité (le texte évoque *benefit/risk*) dans un contexte élargi.

- les conséquences sont importantes (considérant n° 129) : la proposition de règlement autorise l'Agence « *to access and analyse data* ***submitted independently from the marketing authorisation applicant or marketing authorisation holder. On this basis, the Agency should take initiative*** *to update the summary of product characteristics in case new efficacy or safety data has an impact on the benefit-risk balance of a medicinal product* » Cela

[929] Instruction des dossiers d'autorisation de mise sur le marché selon les standarts CTD (common technical document), surveillance des marchés (pharmacovigilance) avec rapportage dans la base Eudravigilance, etc.
[930] En application de la communication précitée de la Commission européenne, « A European Health Data Space: harnessing the power of health data for people, patients and innovation », COM(2022) 196 final.

consacre un fort élargissement potentiel de l'assiette de l'évaluation au-delà des données fournies par les industriels qui développent les médicaments, **à l'initiative de l'Agence**.

* Cette nouvelle place des données de santé justifie que, dans la proposition de règlement relatif aux attributions de l'Agence donc [931], une place particulière leur soit consacrée en section 4 (dispositions générales).
Plusieurs **règles nouvelles relatives aux données de santé personnelles** (article 166) y sont évoquées après la transparence (article 165), avant la protection contre les cyber-attaques (article 167), la confidentialité (article 168), et le traitement des donnés personnelles (article 169). Ce dernier article n'apportant pas d'éléments originaux (rappel du droit commun applicable), **nous focalisons sur l'article 166.**

En effet, les considérants précités y sont concrétisés d'une façon inédite et puissante : selon l'article 166§1, « *the Agency **may process personal health data, from sources other than clinical trials,** for the purpose of improving the robustness of its scientific assessment or verifying claims of the applicant or marketing authorisation holder (...)* » ; et selon l'article 166§2, « *The Agency **may consider and decide upon additional evidence available, independently from the data submitted** by the marketing authorisation applicant or marketing authorisation holder* ».
Ce point est intéressant, car il introduit une forme de **stéréophonie entre la recherche interventionnelle et la recherche observationnelle**, dont nous avons relevé que depuis 2021, elle était en France le but des PUT-RD (protocoles d'utilisation thérapeutique – recueil de données).

Leur développement symétrique en France apparaît improbable, **car il n'aurait pas ou très peu d'application,** hormis les cas d'accès précoces et compassionnels [932]. En fait, il semble que la non-connexion des Etats membres à la plateforme DARWIN ne soit pas un sujet (ils pourront à tout moment s'y connecter, selon des textes en gestation) ; **l'évaluation des technologies ne leur échappera pas totalement**, même après le règlement adopté en 2021.

[931] Non dans la proposition de directive relatif au cadre général, mutique sur ce point.
[932] La compétence de l'Agence européenne est en effet obligatoire pour l'autorisation des médicaments biotechnologiques (y compris leurs biosimilaires) : les agences nationales n'en connaissent donc pas. Pour les produits qui échappent à cette compétence impérative, la saisine volontaire de l'Agence européenne évince les compétences nationales.

2. L'adoption d'un régime inédit d'évaluation commune des technologies de santé

Nous reprenons ici des éléments de notre étude intermédiaire publiée en mars 2023. Mais nous concentrons cette fois l'analyse sur les considérants du règlement n°2021/2282, qui seuls permettent la mise en perspective de dispositions techniques à défaut assez sèches [933].

C'est pour fluidifier l'accès aux technologies de santé dans l'Union, que ce règlement adopté en décembre 2021 prévoit la mutualisation à terme de leur évaluation, sans préjudice de la souveraineté nationale en matière de choix et de prix [934].

Dans ce contexte, **la génération et l'exploitation de données de vie réelle, en complément des données d'essais fournies par les développeurs, deviennent un enjeu critique**. Ces données peuvent être appelées par la nature même de technologies spécifiques, dont l'usage pressant ne peut attendre le recul ; par une actualisation programmée ou continue de l'« évaluation clinique commune » ; ou par un besoin de réassurance des payeurs nationaux, quant à la valeur thérapeutique qui aura été perçue au niveau européen.

Par « *évaluation clinique commune* », le règlement entend « *la compilation scientifique et la description d'une analyse comparative des données probantes cliniques disponibles concernant une technologie de la santé par comparaison avec une ou plusieurs autres technologies de la santé ou procédures existantes (...)* » (article 2). Cette évaluation est dite « clinique », mais ne suppose ni n'implique de contact au chevet des patients : **comme les procédures nationales d'évaluation des technologies de santé, elle vise l'expertise des dossiers et des données présentées à ce titre.**

Des échanges scientifiques entre développeurs et évaluateurs pourront aussi avoir lieu en amont dès les plans de développement, pour recommandations (article 16, 17). Ici, la qualification « clinique » ne sert donc qu'à distinguer des volets « non cliniques » [935] et **ne mobilise pas des données de santé personnelles en tant que tel,** sous réserve de l'usage de ses attributions par l'Agence européenne selon le projet de réforme en 2023, précité *supra*.

---

[933] F. Megerlin, E. Pinilla, Cl. Huriet, Règlement européen de 2021 sur l'évaluation des technologies de santé : place des données de « vie réelle » ?, Rev. gen. Dr. med. 2023, préc.

[934] Règlement (UE) 2021/2282 du Parlement européen et du Conseil du 15 décembre 2021 concernant l'évaluation des technologies de santé et modifiant la directive 2011/24/UE.

[935] Selon l'article 2, 7) du Règlement de 2021, on entend par « évaluation non clinique », la partie d'une ETS fondée sur les domaines non cliniques d'ETS que sont le coût et l'évaluation économique d'une technologie de santé, et les aspects éthiques, organisationnels, sociaux et juridiques liés à son utilisation ».

A ce stade donc, les « *données probantes cliniques disponibles* » au sens de l'article 2 du règlement 2021/2282 sont essentiellement les données fournies par les industriels. **Mais cela n'exclut pas la génération ultérieure ou concomitante de données dans d'autres circonstances** que les essais cliniques, et par d'autres acteurs : que ce soit en amont de l'évaluation commune, pour son actualisation européenne, ou en réassurance nationale de la valeur perçue dans le futur au plan européen. Dans les raisonnements étatiques, la place de telles données de « vie réelle », externes par définition aux essais protocolisés, est en pleine évolution [936]. La proposition de règlement présenté en mai 2022 pour un espace européen des données santé l'a, nous l'avons vu, mise en exergue [937].

Selon son agenda, le règlement 2021/2282 s'appliquera prioritairement à des médicaments relevant de la procédure d'AMM centralisée obligatoire [938]. Les données fournies pour leur « évaluation clinique commune » **ne devraient donc pas être différentes de celles fournies pour l'AMM**, **quoique potentiellement complétées** [939]**. L'enjeu est considérable**, d'où l'insistance du Règlement sur l'exactitude, la pertinence, la qualité etc. de ces données, comme sur les choix méthodologiques à venir, très sensibles car potentiellement décisifs.

En résulte aussi un principe de « *mise à jour de ces évaluations, en particulier lorsque des données supplémentaires,* ***devenues disponibles après l'évaluation initiale****, sont susceptibles d'accroître l'exactitude et la qualité de l'évaluation* » (Consid 19).

Or, distinctement de la pertinence, qualité etc. exigibles des données, le Règlement **prend acte de limites parfois particulières, quant à leur disponibilité et donc complétude initiale** [940] : ainsi faudra-t-il spécialement intégrer « *les spécificités des nouvelles technologies de santé* ***pour lesquelles certaines données peuvent ne pas être facilement disponibles****. Cela peut concerner, entre autres, les médicaments orphelins, les vaccins et les médicaments de thérapie innovante* ». La liste n'est donc pas exhaustive. Dans ce cas, « *il convient d'adapter*

[936] En France, voir Rapport B. Bégaud, D. Polton, F. von Lennep, « Les données de vie réelle, un enjeu majeur pour la qualité des soins et la régulation du système de santé – exemple du médicament », juin 2017 ; HAS, Études en vie réelle pour l'évaluation des médicaments et dispositifs médicaux, Guide méthodologique (guide études post-inscription » retitré, validé par la HAS le 10/06/2021) ; European Comm, Study on the use of real-world data (RWD) for research, clinical care, regulatory decision-making, health technology assessment, and policy-making, juillet 2021.

[937] Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final2022/0140 (COD).

[938] Nouvelles substances en cancérologie et thérapies innovantes (à compter de 2025), médicaments orphelins (2028), etc.

[939] On a vu des cas de « repérimétrage » opportuniste ou maladroit, à usage national, de données des EPAR.

[940] Les données initialement disponibles comportent toutes des limites : mais elles peuvent être considérée nécessaire et suffisantes pour établir le ratio efficacité/sécurité justifiant l'AMM, sans préjudice des plans de gestion de risque et procédures de pharmacovigilance de droit commun etc.

les méthodes utilisées pour la réalisation des évaluations cliniques commune et des consultations scientifiques communes » (Consid 24). De même, en matière de dispositifs médicaux (dont les DMDIV), le règlement souligne que les données probantes peuvent n'être disponibles qu'ultérieurement, du fait de la forte décentralisation de leur accès au marché. Ceci implique une évaluation nécessairement *ex post* (consid 37).

En tout état de cause, le considérant 24 postule qu'un complément de données post AMM peut être rendu nécessaire par étude observationnelle, quant à la signification clinique (à l'échelle individuelle ou populationnelle), en vie réelle et à terme, de ces technologies spécifiques dont l'évaluation suppose un certain recul [941]. De même, il n'est pas rare qu'hors de ce champ, des médicaments soient autorisés sur la base de marqueurs de substitution (*surrogate markers*), par défaut d'un horizon temporel permettant la pleine appréciation de leur bénéfice clinique (*clinical endpoint*) lors des essais.

Le développement des connaissances *ex post* permet/justifie alors une évaluation dynamique, sans donc retarder l'accès du patient à une technologie porteuse d'espoir, et parfois sans alternative thérapeutique. Enfin, la transposabilité en « vie réelle » des résultats établis à l'issue d'essais protocolisés appelle parfois de nouvelles approches dans la relation entre acheteur et vendeur des technologies, pour le management contractuel de l'incertitude : ces approches peuvent inclure la génération et exploitation de données d'usage en pratique de soins, au delà des données d'essais généralement fournies par les industriels, *supra*.

3. Vers un recours systématique aux données de santé « de vie réelle » ?

Dès lors, on ne peut que se réjouir de l'anticipation, par le Règlement européen de 2021, du **besoin d'établir un lien entre la plateforme informatique européenne qu'il met en place (article 30), « *et les autres infrastructures de données pertinentes (…) comme les registres et bases de données liées à des données de terrain* »** (Consid 52). Celles-ci sont essentiellement une émanation d'institutions nationales (ETS, tarification), d'organisations de soins (hospitalières, parfois ambulatoires), voire de payeurs de soins (PMSI, SNIIRAM) [942], voire de systèmes ou registres *ad hoc* prévus par certains contrats d'achat des technologies.

[941] La Commission de la Transparence publiera en fin 2022 ou 2023, une doctrine actualisée d'évaluation prenant en compte ce défi, notamment pour les technologies visant à la correction d'anomalies biologiques.
[942] Distinctement de l'analyse de données médicales, l'analyse de données de remboursement fournit parfois de précieuses pistes d'investigation par l'analyse de la trajectoire, dans le système de soins, de patients traités.

L'ensemble a vocation à être réuni sur la plateforme nationale française des données [943]. Il a aussi vocation, à terme, à une interconnexion européenne, envisagée en 2022 par le projet de règlement sur un espace des données de santé (EEDS, préc.) [944].

*** Mais les obligations des États ne les privent pas du droit de** « *tenir compte d'informations, données, analyses et autres données probantes* qui ne faisaient pas partie de l'évaluation clinique commune *au niveau de l'Union* », sachant que, dans ce cas, « *l'ETS menée au niveau national ou régional sur une technologie de la santé qui a fait l'objet d'une évaluation au niveau de l'Union* ***devrait être mise à la disposition*** *du groupe de coordination* » (Consid 30). Non seulement une étude observationnelle nationale n'est pas exclue, mais « devrait » le cas échéant être fournie au groupe en charge de l'évaluation commune, à toutes fins utiles.

Un partage d'expériences nationales, donc ; à quel point ? Nous avons vu que la notion de « vie réelle » ne relèvait pas d'une définition, d'un périmétrage ni de méthodes de recueil univoques [945], ce qui rend important l'énoncé des concepts et contours, l'appropriation des systèmes et pratiques, et le référencement des bases et études [946].
Cela pose aussi la question des données acquises par les études observationnelles ; la statistique multivariée et les registres intéressent aussi les contrats de prix des technologies – sachant que la question du prix (par extension, des contrats qui entendraient moduler ces prix selon ces données) est écartée du champ du règlement.

En outre, le primat dans le règlement de 2021, des « *études cliniques de comparaison directe, contrôlées, randomisées, en aveugle et dont la méthode est conforme aux standards internationaux de la médecine factuelle* » ne saurait exclure [947] « *les études observationnelles, y compris celles fondées sur des données de terrain, lorsque ces études sont disponibles* » (Consid 35). **Nous ne voyons pas ici que la prise en compte d'études observationnelles doive se limiter au cas où ces études seraient « disponibles »** (c'est-à-dire *préexistantes*).

---

[943] Arrêté interministériel du 29 novembre 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 » dite Health Data Hub (termes anglais bannis à compter de 2023, TA Paris 20 oct. 2022).
[944] Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final2022/0140 (COD).
[945] Par ex., Makady A, de Boer A, Hillege H, Klungel O, Goettsch. « What Is Real-World Data? A Review of Definitions Based on Literature and Stakeholder Interviews », Value Health. Jul-Aug 2017;20(7):858-865.
[946] Ainsi par la Haute Autorité de Santé depuis 2022, supra.
[947] Le Règlement de 2021 est ici elliptique : « *ne devrait toutefois pas exclure en soi (…)* ». Mais on voit mal qu'un État membre infère de cette ellipse, une autolimitation de sa compétence nationale.

Il est légitime que les États puissent diligenter de telles études à l'échelle nationale, éventuellement multilatérale : n'est-ce pas ce qui est prévu par le consid. n° 30 précité ?

* Le consid. 28 **a déjà attiré l'attention sur la dépendance des conclusions nationales à l'égard du « *contexte spécifique des soins de santé* »** ; ce n'est qu'à titre d'exemple, qu'il cite le seul cas des choix de comparateurs. Le contexte spécifique peut en effet être beaucoup plus vaste : populations traitées, standards pratiqués, systèmes d'information, personnels, etc. Cela peut justifier des demandes additionnelles par voie d'études observationnelles, sans nécessairement que ces demandes diffèrent la mise à disposition de l'« évaluation commune ». La question de l'objet et de la qualité scientifique des études est alors en question au premier chef, sans préjudice de la protection bien établie des données personnelles [948].

Nous de détaillerons pas ici la question très spécifique des prise en compte de données de vie réelle *hors cas d'une AMM*, que ce soit au titre des autorisations d'accès précoce, ou d'accès compassionnel : en effet, ces questions **relèvent par essence de la compétence nationale**.

En tout état de cause, l'articulation de ces textes met en exergue les attentes conçues à l'égard de la centralisation européenne des données de santé sur l'EEDS. Mais **ses applications stratégiques vont encore au-delà**, puisque l'EEDS doit aussi servir de réservoir de données pour le développement de l'intelligence artificielle en santé.

B. ANTICIPATION NORMATIVE POUR L'EMERGENCE EUROPEENNE DE L'« INTELLIGENCE ARTIFICIELLE »

Enjeu stratégique majeur pour la France et l'Union (la transformation numérique est nous l'avons vu, une priorité de l'UE), l'« IA » a fait en 2021 **l'objet d'une première proposition de cadre juridique européen [949], dans le cadre d'un plan coordonné avec les Etats membres** [950]. A la date de notre rédaction, le projet de texte et le mandat de négociation ont été largement adoptés par l'assemblée plénière du Parlement [951], l'ensemble pourrait être finalisé en 2024.

---

[948] Protection dont en France, les modalités de mise en œuvre relèvent dans les études, de différentes « méthodologies de référence » élaborées sous l'égide de la CNIL (Ière Partie, Titre II).

[949] COM (2021) 206 final - Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union. https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1682

[950] COM (2021) 205 final - ANNEXES de la communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions - Favoriser une approche européenne en matière d'intelligence artificielle.

[951] En juin 2023, 499 votes en faveur, 28 contre, 93 abstentions.

Pour rappel, on y entend par système d'IA, « *un logiciel qui est développé au moyen d'une ou plusieurs des techniques et approches énumérées à l'annexe I et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit* » (article 3.1).

Le but est tant de contribuer à l'établissement d'un **« écosystème de confiance »,** que de dynamiser le potentiel européen. Le projet vise à introduire un cadre applicable **à l'ensemble des parties prenantes de l'industrie de l'IA ayant un lien avec le marché européen** (fournisseurs, importateurs, distributeurs, utilisateurs, etc. qui y sont tous définis), sans donc être spécifique au secteur de la santé, malgré nombre d'occurrences du terme [952].

Après avoir relevé la matrice des qualification, portée par le texte du règlement, des risques associés aux systèmes d'IA dans le champ de la santé (1), nous relèverons la qualification de la « donnée de santé » requise par et pour l'IA notamment (2).

1. Qualification juridique de la criticité des risques de l'IA en santé

Le projet de règlement prévoit que les obligations des parties prenantes varient selon que le niveau de risque présenté par le système d'IA, est considéré « faible », « haut », voire inacceptable – ce qui alors justifie son interdiction.

Aucune disposition ne qualifie spécialement un risque en santé. La matrice des qualifications figure dans le titre III « *systèmes d'IA à hauts risques* », lesquels sont définis en deux grandes catégories : ceux (article 6§1) destinés à un usage « *en tant que composants de sécurité de produits* » ou en tant que produits visés par des actes législatifs rapportés en annexe II du texte ; ceux « *autonomes* » énumérés à l'annexe III, qui mettent principalement en cause le respect des droits fondamentaux (article 6§2). On peut ainsi distinguer les systèmes selon qu'ils relèvent des critères de qualification selon l'annexe II, ou de la liste positive de l'annexe III. **Qu'en est-il ?**

*** La qualification du « haut risque » en santé relève en premier lieu de la matrice de l'article 6§1,** qui renvoi à l'annexe II. En substance, il faut que le système d'IA considéré, de façon autonome ou en tant que composante d'un système, soit « *soumis à une évaluation de la*

[952] Tous ses considérants mettent en exergue son caractère primordial, *avant* les risques pour la sécurité et les droits fondamentaux (article 7, 67,) ; seule une occurrence le fait apparaître après eux (article 54).

conformité par un tiers en vue de la mise sur le marché ou de la mise en service » du produit qu'il constitue intrinsèquement ou par combinaison. Dans ce contexte, force est d'analyser l'annexe II pour relever les textes pertinents en santé : on y trouve les règlements n°2017/745 en matière de dispositifs médicaux [953] et n°2017/746 en matière de dispositifs médicaux de diagnostic *in vitro* [954]. Les dispositions alors applicables au titre de ces règlements selon la criticité du DM, le sont **sans préjudice des dispositions applicables en application du règlement sur l'IA si la qualification de système d'IA « à haut risque » est établie**.

Dès lors, le droit européen s'applique en tout ce qui concerne le système de gestion des risques (article 9), les données et la gouvernance des données (art. 10) sur laquelle on va revenir *infra*, la documentation technique (art. 11), l'enregistrement (art. 12), la transparence et fourniture d'informations aux utilisateurs (art. 13), et le contrôle humain (art. 14), l'exactitude, robustesse et cybersécurité (art. 15).

Le « *contrôle humain* » dont il s'agit (article 14) dans le texte de 2023 correspond de loin à celui prévu en France par la loi n° 2021-1017 sur la bioéthique [955]. Nous avons *supra* souligné que, dans la 4ème partie CSP (Professions de Santé), cette loi avait créé un article L. 4001-3, lequel traite des conditions d'emploi, par un professionnel de santé, d'un dispositif médical « *comportant un traitement de données algorithmique dont l'apprentissage a été réalisé à partir de données massives* » (L. 4001-3-I). Il y est notamment spécifié que les « *professionnels de santé concernés sont informés du recours à ce traitement de données. **Les données du patient utilisées dans ce traitement et les résultats qui en sont issus leur sont accessibles*** ».
Or, cela introduit un potentiel contrôle par un acteur subséquent pour comparer les données traitées et les propositions, non sans soulever nombre de questions nous l'avons vu. Dans la proposition de texte relative à l'ESSD, une telle éventuelle appréciation *ex post* des sets de donnée de santé de santé **n'est pas mentionnée : cela relève du droit national.**

*** L'annexe III dédiée aux systèmes autonomes (article 6§2) ne fait pas apparaître le domaine sanitaire**. N'y sont mentionnés que les domaines de l'identification biométrique et

[953] Règlement (UE) 2017/745 du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) nº 178/2002 et le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.
[954] Règlement (UE) 2017/746 du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission.
[955] Loi n°2021-1017 du 2 août 2021 relative à la bioéthique.

catégorisation des personnes physiques (1) ; la gestion et exploitation des infrastructures critiques (2) – mais l'annexe ne cite alors que « *la gestion et l'exploitation du trafic routier et dans la fourniture d'eau, de gaz, de chauffage et d'électricité* », non la santé ou la production des soins [956] ; l'éducation et la formation professionnelle (3) ; l'emploi, la gestion de la main-d'œuvre et accès à l'emploi indépendant (4) ; l'accès et droit aux services privés essentiels, aux services publics et aux prestations sociales (5) – mais **ni le mot « santé », ni le mot « soin », n'y sont évoqués,** seulement les prestations et services d'« aide sociale » ; les autorités répressives (6) ; l'administration de la justice et le processus démocratique (8).

C'est dans son seul (7) « ***gestion de la migration, de l'asile et des contrôles aux frontières*** **», que la santé est mentionnée,** lorsqu'il s'agit des systèmes d'IA « *destinés à être utilisés par les autorités publiques compétentes pour évaluer des risques, y compris des risques pour la sécurité, des risques d'immigration irrégulière* ***ou des risques pour la santé, posés par une personne physique qui a l'intention d'entrer ou qui est entrée*** *sur le territoire d'un État membre* ».
Nous avons vu *supra* ce qu'il en était de l'interopérabilité des systèmes pour la mobilité transfrontière, nous n'y reviendrons pas ici. Les « risques pour la santé » sont par ailleurs mis en exergue parmi les critères de mise à jour, par la Commission européenne, de la liste par l'annexe III des systèmes d'IA à « haut risque » [957].

La méthode de qualification des systèmes d'IA étant ainsi établie dans le projet de texte de 2023, voyons la qualification des données, question consubstantielle au développement (performance/sécurité) de ces systèmes, lorsqu'elles les nourrissent et les entraînent.

2. Première qualification juridique d'une « qualité » des données en santé ?

***** Pour bonne partie anticipée par le texte sur l'EESD de 2022, notamment quant à la qualité exigible des « *données de santé* », la question des données a été mise en exergue par le texte sur l'IA de 2023. Si ce texte possède une vocation générale, **il évoque à plusieurs reprises la question de la santé, qui peut appeler le traitement par exception de données personnelles**, en cas de limites des alternatives.

---

[956] L'objet de ce règlement n'est pas le traitement de la cybersécurité en la matière, cf. *infra*.
[957] Selon l'article 7, la liste des systèmes d'IA concernés de l'annexe III est susceptible d'être mise à jour par actes délégués de la Commission en application de l'article 73, notamment si les systèmes considérés présentent « *un risque de préjudice pour la santé et la sécurité, ou un risque d'incidence négative sur les droits fondamentaux, qui, eu égard à sa gravité et à sa probabilité d'occurrence, est équivalent ou supérieur au risque de préjudice ou d'incidence négative que présentent les systèmes d'IA à haut risque déjà visés à l'annexe III* ».

Mais si parmi ces alternatives, figure la « *donnée synthétique* », cette notion **n'y est pas définie et encore moins encadrée** ; cela nous semble un manque dans le dispositif, *supra*.

* Le projet de texte 2023 du règlement IA **est le premier qui traite spécifiquement de la gouvernance des données en la matière** [958], au travers de plusieurs occurrences, dont l'article 10 (données et leur gouvernance) ; l'article 54 (« *traitement ultérieur de données à caractère personnel en vue du développement de certains systèmes d'IA dans l'intérêt public dans le cadre du bac à sable réglementaire de l'IA* »), article 64 (Accès aux données et à la documentation). Ce qui nous intéresse ici, est le lien qui va apparaître avec la proposition de règlement EESD qui a stratégiquement anticipé.

En effet, l'article 10 met en exergue le besoin de **régulation des données et des jeux de données voués à l'entraînement des systèmes d'IA à haut risque**. Les « pratiques appropriées » (article 10§2) concernent « *en particulier* » (la liste n'est donc pas exhaustive) les « *choix de conception pertinents* » (a), la collecte des données (b), leur préparation ainsi l'annotation, l'étiquetage, le nettoyage, l'enrichissement et l'agrégation (c), la « *formulation d'hypothèses pertinentes* » quant aux informations que ces données « *sont censées mesurer et représenter* » (d), une « *évaluation préalable de la disponibilité, de la quantité et de l'adéquation des jeux de données nécessaires* » (e), un « *examen permettant de repérer d'éventuels biais* » (f), la détection d'éventuelles lacunes ou déficiences dans les données et la façon dont il peut y être remédié (g). **Nous relevons ici un parallèle avec les exigences de la Haute Autorité de Santé précédemment examinées**, mais ces exigences supposent que la performance du dispositif médical évalué dans une fin d'éventuelle admission du service au remboursement, soit commercialisable (donc réponde aux spécifications ici étudiées).

Dans ses §3, §4 et §5, l'article 10 met en exergue le **besoin de représentativité et de complétude des jeux de données d'entraînement**, auxquels les autorités de surveillance doivent avoir pleinement accès (art. 64), pour une finalité non précisée. On pourrait inférer cette finalité des spécifications de l'article 10 à leur endroit, que l'autorité devrait pouvoir contrôler. Mais cela ne tient-il pas plus d'une réassurance symbolique (compte tenu des moyens technologiques requis) que d'une possibilité effective de contrôle ?

[958] Tel n'était pas l'objet du règlement sur les données « Data Act ».

* Selon l'article 10 en effet, ces jeux doivent posséder « *les propriété statistiques appropriées,* ***y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels*** *le système d'IA à haut risque est destiné à être utilisé* », sachant que les données sont censées être anonymes. Pour la seule détection et correction de biais, les fournisseurs **peuvent traiter de catégories particulières de données à caractère personnel** [959] **« *lorsque l'anonymisation peut avoir une incidence significative sur l'objectif poursuivi* »** ; cela peut justifier des techniques alternatives (cryptage, pseudonymisation), sous les réserves énoncées par l'article 10§5 visant à la préservation des droits fondamentaux. L'article 54 possède un objet similaire en contexte de bacs à sable réglementaires ; mais il spécifie alors, entre autres, un but sanitaire : « ii) *la sécurité publique* ***et la santé publique, y compris la prévention, le contrôle et le traitement des maladies*** » (art. 54§1a).

La notion de « bac à sable réglementaire » n'est pas définie dans l'article 3 du texte de 2023 ; il s'agit nous l'avons vu d'un espace d'expérimentation surveillée, de géométrie variable (nationale et au-delà), pour des buts spécifiés [960]. Sous le Titre V « mesures de soutien à l'innovation », l'article 53 définit ces espaces comme « *créés par une ou plusieurs autorités compétentes des Etats membres* ***ou par le Contrôleur européen de la protection des données*** » (la création par l'autorité publique ne doit pas être confondue avec une autorisation par elle). Le but est d'offrir « *un environnement contrôlé qui facilite le développement, la mise à l'essai et la validation de systèmes d'IA innovants pendant une durée limitée avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique* ».

Paradoxalement, c'est dans ce contexte que l'article 54 est le **seul article du texte de 2023 invoquant les « données synthétiques », dont les limites (entre autres types de données dont anonymisées) peuvent justifier le recours aux données personnelles** [961]**. Les données synthétiques n'y présentent pas d'autre occurrence, et n'y sont pas définies** (bien que l'article 3 « *définitions* » possède 44 entrées, parfois subdivisées).

---

[959] « *visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679, à l'article 10 de la directive (UE) 2016/680 et à l'article 10, paragraphe 1, du règlement (UE) 2018/1725.*

[960] Sur la notion, M-D. et G. Campion, « Bacs à sable réglementaires en santé : des initiatives diversifiées à la recherche d'un cadre fédérateur au service du bien public », RGDM 2023, n°10, 233-248.

[961] Article 54§1 « *Dans le cadre du bac à sable réglementaire de l'IA, des données à caractère personnel collectées légalement à d'autres fins sont traitées aux fins du développement et du test de certains systèmes d'IA innovants dans le bac à sable, dans les conditions suivantes* (…) ».

Pas plus, elles n'étaient définies dans les règlements précédents sur les données, leur gouvernance des données, sur la protection des données personnelles, ni dans le programme du règlement 2021/694 pour une Europe numérique [962].

Or, dans ce texte, les « données synthétiques » apparaissent un recours ordinaire (non cantonné au périmètre de l'article 53), au côté d'autres techniques, de données anonymisées ou « *autres à caractère non personnel* ». Ce sont les limites de ces techniques, au vu des exigences de systèmes d'IA innovants testés dans le « bac à sable réglementaire », **qui pourraient par défaut, justifier le recours à des données personnelles** [963] de santé.

Ce qui nous intéresse (et peut inquiéter) ici, est **l'apparente banalisation de la « donnée synthétique »**, dont la production par IA soulève des questions **qui, à la date de notre rédaction, auront échappé à tous les textes européens**. Si on peut inférer, selon sa destination, que la donnée de santé « synthétique » doive répondre à des critères de « qualité » [964] de la donnée de santé, comme énoncé par la proposition de règlement EESD de 2022, sa production par synthèse (à partir de données « réelles ») ne fait pour autant l'objet d'aucune définition, ni d'aucun contrôle, alors qu'elle devient l'objet d'un marché exponentiel, *supra*.

Cela alors que le **but de la donnée synthétique en santé est de permettre de modéliser des caractéristiques individuelles / populationnelles** (non seulement de compléter des jeux de données disponibles jugées insuffisamment représentatives) pour de multiples applications, bienveillantes…ou non, intéressant jusqu'à la biosécurité sélective.

Dès lors, l'avènement d'un marché proposant des « données de santé synthétiques », **qui échappent tant aux restrictions légales d'usage des données personnelles, qu'aux conditions légales strictes de leur usage secondaire,** nous semble bien du fait de la

[962] Règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240.

[963] Ainsi selon le (b), si les données personnelles « *sont nécessaires pour satisfaire à une ou plusieurs des exigences visées au titre III, chapitre 2, lorsque ces exigences ne peuvent être satisfaites de manière efficace en traitant des données anonymisées,* ***synthétiques ou autres à caractère non personnel****;* »

[964] L'article 5.1 a) du règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 établissant le programme pour une Europe numérique et abrogeant la décision (UE) 2015/2240 souligne au titre de l'objectif spécifique « Intelligence artificielle », l'enjeu de « *développer et renforcer les ressources en matière de données de qualité et les mécanismes d'échanges correspondants* ».

sensibilité de leurs applications, **un enjeu de souveraineté**. La question critique des données de synthèse (pour entraînement d'IA) **ne pourrait-elle justifier un texte en soi** [965] **?**

Dans cette perspective, pourquoi pas un catalogue de métadonnées tenu par les producteurs déclarés, à l'instar de ce qui est proposé dans le texte (2022) relatif à l'espace européen des données de santé (art. 55§1, en l'occurrence à la charge des détenteurs des données de santé) ? pourquoi pas avec un étiquetage de qualité / d'utilité des données (art. 56 : cet étiquetage est obligatoire pour les données « *collectées et traitées avec le soutien d'un financement public national ou de l'Union* » [966]) ? **Ce point nous semble ne pas avoir été anticipé.**

SYNTHESE P2T1C2

Après l'analyse descriptive de la dynamique coopérative, qui voit l'élargissement des motifs d'un partage encore très sélectif de données de santé, ce second chapitre de notre titre I restitue des observations semi-prospectives (les textes élaborés, mais non encore adoptés) d'une dynamique cette fois intégrative. Au vu de l'expérience et de la nécessité, mais aussi de l'opportunité, la norme contraignante prend le pas sur les modèles antérieurs de coopération à base volontaire, avec un dessein beaucoup plus vase : l'affirmation d'une Europe du numérique. Dans ce contexte, nous ne considérons toujours que notre fil rouge des données.

***** dans une première section, nous relevons des balises de construction de « l'espace européen des données de santé ». En premier lieu, celle du « Data Act », qui vise à la promotion d'un cadre intersectoriel de partage, mais comporte des dispositions originales pour le traitement de situations de crise : il érige le bien public et la santé publique en motifs légitimes d'exigibilité, inédite, d'une disponibilité immédiate des données. En second lieu, le règlement sur la « gouvernance des données » (Data Governance Act), qui s'entend comme un levier au service de l'autonomie stratégique européenne, et ouvre la question des données de santé parmi celles détenues par les organismes publics. Il prévoit la possibilité d'une ouverture de

[965] Pinilla E, Megerlin F, « Les données de santé « synthétiques », Rev. Gen. Dr. Med. 2024, à paraître.
[966] L'absence de financement public n'est pas ici dirimant : il suffit de rapprocher des exigences légales de traçabilité quant à la chaîne de valeur de produits finis issus des filières agroalimentaire, pharmaceutique, etc.

ces données dont il anticipe les problématiques compétitives, et esquisse un régime généraliste d'usages secondaires, dans l'attente d'une spécification de ce régime en santé.

* Dans une seconde section, nous relevons en effet la dynamique visant à concrétiser l'« Espace européen des données de santé », volet de la « stratégie européenne pour les données ». Dans cette proposition de règlement, objet de discussions au niveau national, nous relevons comment les droits des citoyens servent de levier de transformation, par l'obligation d'infrastructures inédites pour le partage des données de santé, non sans conséquences pour le statut des technologies de l'information qui vont les abonder. Ce levier conduit à la promotion d'un objectif majeur de la stratégie européenne : la création d'un cadre juridique pour les « usages secondaires » des données de santé, lequel distingue les catégories « prioritaires » (pour les usages primaires) et « minimales » mais en fait fort développées (pour les usages secondaires). Au vu des progrès exponentiel des technologies de calcul et de la masse de donnée permettant la ré-identification potentielle, cette perspective met en exergue les limites des garanties apportées par les processus d'anonymisation, et toutes vulnérabilités induites. La « donnée synthétique » invoquée de façon croissante n'est toujours pas définie a fortiori régulée. Nous proposons d'en clarifier le régime.

SYNTHESE P2T1

Ce premier titre avait pour objet l'analyse, au travers du fil rouge de la donnée de santé, des dynamiques de recherche contemporaine par les Etats membres de l'Union, de garanties coordonnées pour les accès licites aux données de santé. Cette dynamique peut être caractérisée par deux temps : une dynamique coopérative, c'est à dire à base volontaire, des Etats membres, avant que ses effets nationaux dispersés, et surtout des manques patents apparus lors de la crise systémique issue de la pandémie de Covid19, ne stimulent une approche intégrative : à visée unifiante, celle-ci repose sur des mécanismes par définition contraignants, ce qui apparaît ambitieux dans ce contexte de susceptibilités régaliennes.

En une dizaine d'années, nous constatons une transformation considérable du partage des « données de santé » notamment personnelles, domaine de compétence des Etats jalousement maîtres de bases nationales dont ils sont, et restent, les garants de l'intégrité. La stratégie numérique de l'Europe apparaît ainsi le cadre conceptuel de mise en oeuvre de nombreuses initiatives inédites et audacieuses : elles stimulent voire ordonnent une unité de standards et de spécifications d'outils, et posent un concept de « qualité » européenne de donnée de santé, entendue en 2022 au seul sens de son appropriation pour des usages secondaires.

Ces derniers, qui supposent l'anonymat de la donnée, sont un enjeu considérable pour tous les acteurs, et un pan important de la proposition de règlement sur l'espace européen des données de santé. Cette proposition met en évidence un gisement de valeur considérable, mais aussi un terrain de jeu pour des acteurs potentiellement oligopolistiques.

Leur puissance servie par l'intelligence artificielle peut défier les Etats dans un des domaines réputés les plus protégés de la vie civile, le domaine de la santé. A la panique transformatrice de la pandémie, succède ainsi l'accélération compétitive. L'espace européen des données de santé est perçu comme une condition de réalisation en propre par l'Union européenne, de son potentiel espéré dans l'économie « numérique » au service de la maîtrise de son destin.

TITRE 2. DYNAMIQUE DES GARANTIES COORDONNEES CONTRE L'ACCES ILLICITE AUX DONNEES DE SANTE

Après avoir dans le Titre I examiné la recherche coordonnée par les Etats membres de l'Union (sous l'égide de celle-ci puis à son initiative), de garanties pour un accès licite aux données de santé, le prisme de nos observations est maintenant cette même recherche **contre des accès résultant d'ingérences d'Etat tiers**. Cette fois, il s'agit donc **d'une régulation des relations extérieures de l'Union, non plus de son marché intérieur**.

De façon générale, une ingérence désigne une immixtion non légitime dans les affaires d'autrui.

* Pourvu de multiples applications en droit interne [967], nous l'entendons ici au sens de la défense et de la sécurité nationale. Phénomène croissant source de risques délétères et systémiques, cette ingérence justifie en juillet 2021 la création, auprès du Secrétaire général de la défense et de la sécurité nationale (SGDSN), d'un **service à compétence nationale** dénommé « *service de vigilance et de protection **contre les ingérences numériques étrangères*** » [968] ; et en décembre 2021, l'autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères [969].

* En droit européen, on trouve le terme « *ingérence* » dans la Convention européenne des droits de l'homme, mais pour proscrire l'ingérence d'autorités d'un Etat partie dans les données personnelles, sauf motifs légitimes [970] ; et dans la jurisprudence de la CJUE quant à l'action d'Etat tiers dans la sphère de compétence d'Etats de/ou de l'Union, hors cadre agréé.

---

[967] On peut y distinguer des occurrences dans les Code de la Défense : « ingérences numériques étrangères » (D.1132-8 CD), il entre dans les prérogatives de la DRDS, des mesures de « contre-ingérence » ; Code de la sécurité intérieure : « prévention de toute forme d'ingérence » (L. 811-3 CSI etc.) ; Code des postes et communications électroniques : « actes d'ingérence » (L. 34-12 CPCE) ; Code pénal : le « délit d'ingérence », désormais dénommé « prise illégale d'intérêt », qui dérive d'un abus par personne assurant une fonction publique (L. 432-12 CP) ; Code de l'éducation : « ingérence » dans les établissements scolaires (L. 481-1 CE).
[968] Décret n° 2021-922 du 13 juillet 2021.
[969] Décret n° 2021-1587 du 7 décembre 2021.
[970] L'article 8, inchangé depuis le texte de 1950, dispose que (8.1) « ***Toute personne a droit au respect de sa vie privée** et familiale, de son domicile et de sa correspondance* » et (8.2) qu' « ***il ne peut y avoir ingérence d'une autorité publique** dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, **à la protection de la santé** ou de la morale, ou à la protection des droits et libertés d'autrui* **».**

* En droit international public, l'ingérence désigne le fait, pour un Etat, de porter atteinte aux droits souverains d'un autre Etat (dont la protection des droits fondamentaux de sa population). Le principe y est celui de la « non-ingérence » [971], dont l'exception est l'invocation d'un « droit d'ingérence », pour motifs humanitaires de sauvegarde de populations ; distinct, le défi est ici **l'ingérence, plus ou moins masquée**, par des moyens nouveaux dits « cyber ».

Ces ingérences peuvent **procéder d'une voie de droit** revendiquée par un Etat selon son droit national, dans des conditions qui sont à préciser et convenir pour être *éventuellement* acceptables (chap. I). *A contrario,* elles peuvent **résulter d'une voie de fait** au regard du droit applicable, revendiquée ou non par son auteur qui à cette fin la sous-traite. Dans ce cas, l'attribution n'est pas aisée, pour des raisons parfois plus politiques que techniques (chap. II).

CHAPITRE I. GARANTIES COORDONNEES FACE AUX INGERENCES D'ETATS TIERS PAR VOIE DU DROIT

En 2016, le RGPD rappelle que le transfert des données personnelles de l'Union vers des pays tiers ou des organisations internationales est **subordonné au respect de dispositions protectrices** réunies dans son Chapitre V dédié. Elles ne bénéficient pas aux seuls ressortissants des pays de l'Union [972].

Alors qu'en 1980, la question des transferts de données commence à se poser, dans un contexte de globalisation croissante des échanges, l'OCDE promeut huit principes pour prévenir la perte ou la divulgation inappropriée de données personnelles [973]. **Ces principes de portée alors non obligatoire ont été intégrés en droit européen,** dans la directive n°95/46CE sur la protection des données, puis le règlement UE 2016/679 (RGPD) qui donc lui a succédé.

---

[971] L'article 2§7 de la Charte de l'ONU qui définit le champ de compétence exclusive d'un Etat, est le fondement doctrinal du principe de non-ingérence. Voir *not*. de l'ONU, les Résolutions 2131(XX) de 1965 et 36/103 de 1981 portant sur l' « inadmissibilité de l'intervention et de l'ingérence » dans les affaires intérieures des Etats ; résolution 2625(XXV) de 1970 sur les « relations amicales » entre les Etats.

[972] Depuis 2018, le bénéfice « international » du RGPD s'étend en effet à l'Islande, au Liechtenstein et à la Norvège. La décision d'incorporation du règlement (EU) 2016/679 dans l'annexe XI de l'accord sur l'Espace Economique Européen (EEE) a été adoptée le 6 juillet 2018 et est en vigueur depuis le 20 juillet 2018.

[973] OCDE, 23 sept. 1980, C(80)58/FINAL : il s'agit des principes de limitation en matière de collecte ; de qualité des données, de spécification des finalités ; de limitation de l'utilisation ; de garanties de sécurité ; de transparence ; de participation individuelle ; de responsabilité.

Ainsi, la Commission européenne est compétente pour décider par acte d'exécution **si, après analyse de l'ordre juridique de l'Etat tiers, celui-ci assure un « *niveau adéquat* » de protection** (article 45§1)**.** Le cas échéant, le transfert de données vers son territoire devient possible sans que d'autres autorisations soient requises [974], sachant qu'existent par ailleurs un suivi permanent, et des revues périodiques de ce droit d'un Etat tiers.
De telles décisions ont été prises à l'égard d'Etats non européens [975]. Ex-membre de l'Union, le Royaume-Uni a par ailleurs fait, *en sus,* l'objet d'une décision d'adéquation spécifique, pour les échanges de données personnelles dans le domaine judiciaire [976].

Pour autant, l'accord validé par décision exécutive de la Commission européenne **n'efface pas la compétence nationale** : un transfert vers un pays tiers demeure un « *traitement* » [977], même s'il a été approuvé au niveau européen. En outre, un doute quant à l'adéquation du niveau de protection **justifie suffisamment la saisine de la Cour** de justice de l'Union.

Or, nous relevons dans ce contexte la sanction emblématique, par la CJUE, de deux décisions de la Commission autorisant le transfert transatlantique de données en 2015 puis 2020, **du fait d'un potentiel d'ingérence** au détriment des droits des personnes (section 1) ; puis nous relèverons l'accord approuvé en 2023 et **la place faite aux données de santé** (section 2).

SECTION 1. LA RECHERCHE DE GARANTIES COORDONNEES DANS LES TRANSFERTS INTERNATIONAUX DE DONNEES

En vue de l'établissement éventuel d'un tel accord entre l'Union et un pays tiers, la Commission considère tant les règles applicables aux importateurs, que les limitations et garanties relatives à l'accès éventuel à ces données, par les autorités localement compétentes (article 45§2). Le critère décisif est l'existence **de « *protections essentiellement équivalentes* » à celles du droit de l'Union** ; sa satisfaction peut conduire à agréer l'accord.

---

[974] Consid. n°103, article 45§1.
[975] Ainsi pour l'Andorre, l'Argentine, le Canada (organisations commerciales), les Iles Féroé, Guernesey, Israël, l'Ile de Man, le Japon, Jersey, la Nouvelle Zélande, la Corée (du Sud), la Suisse, le Royaume Uni, les Etats-Unis (organisations commerciales participantes au DPF approuvé en juillet 2023, *infra*), l'Uruguay. Voir l'onglet dédié incluant les examens périodiques, sur le site de la Commission : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[976] En application de l'article 46 de la directive 2016/680.
[977] Directive 95/46, article 2, b) : constitue un traitement de données à caractère personnel, « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel* » dont notamment « *la communication par transmission, diffusion ou toute autre forme de mise à disposition* ». Ce critère matériel attire dans le champ du RGPD toute opération correspondante, sous réserve d'exceptions que nous constaterons en l'occurrence non réunies.

Notre focus ici sur la relation transatlantique doit être justifié : en premier lieu, il n'existe pas de contentieux d'accords avec d'autres pays tiers [978], qui offriraient un tel matériau à l'analyse. En outre, l'existence d'un contentieux répété des accords entre Union européenne et Etats-Unis ne doit pas distraire l'attention de situations dans lesquelles un tel accord est impossible (et parfois en l'état pas même recherché), **avec des Etats dont l'ordre juridique n'offre assurément pas de « protection essentiellement équivalente »**, car leurs standards sont significativement et peut-être durablement différents en matière de droits fondamentaux.

Dès lors, nous voyons en premier lieu le cadre de l'action coordonnées européenne à la recherche de garanties en matière de transfert vers des pays tiers (§1), avant de relever la **sanction jurisprudentielle du potentiel d'ingérence par ce biais** (§2).

§1. ACTION EXECUTIVE EUROPEENNE A LA RECHERCHE DE GARANTIES COORDONNEES EN MATIERE DE TRANSFERTS DE DONNEES

L'Union étant une union de droit [979], les décisions de la Commission sont **soumises au contrôle de conformité par la CJUE** (avec les Traités, la Charte, les principes généraux du droit, etc.), contrôle d'autant plus approfondi quand sont en jeu les droits fondamentaux.

Ses décisions ici sont essentiellement de deux ordres : il s'agit d'abord de la décision qui, **après analyse de l'ordre juridique étranger de destination, constate son « *adéquation* »** avec les principes fondamentaux du droit européen (A).
En second lieu, il s'agit de décisions portant des « clauses-type » unifiées pour le transfert des données personnelles : il est en effet des cas dans lesquelles **une décision « d'adéquation » n'existe pas… ou plus** (B).

[978] Sur les Etats ayant fait l'objet de décisions d'adéquation, *infra*. Cela n'exclut pas des réflexions dans le cadre des examens, voir par exemple, CE 4 avril 2023, Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan, COM(2023) 275 final. La décision avait été prise le 23 janvier 2019.
[979] Formellement en ce sens, CJUE C-584/10P,C-593/10P et C-595/10P, Commission e . a . /Kadi, EU: C : 2013: 518, § 66 ; CJUE, C-583/11P, Inuit Tapiriit Kanatami e.a. /Parlement et Conseil EU:C:2013:625, § 91, C-274/12P, Telefónica /Commission,EU:C:2013:852, § 56).

A. LES DECISIONS EXECUTIVES ET L'« ADEQUATION » DE L'ORDRE JURIDIQUE DE DESTINATION

Cette première catégorie de décisions exécutive est l'objet de l'article 45 du RGPD, lequel trace leur cadre. Nous n'entrerons pas dans le détail du régime des transferts, très développé. Voyons donc rapidement ici le fondement (1), puis leur portée (2) sur cette base.

1. Fondement des décisions exécutives par la Commission

En application du RGPD, le transfert de données personnelles de tout pays de l'Union vers un pays tiers peut être autorisé sans autre autorisation, dès lors que la Commission européenne décide après analyse, que le droit y applicable assure un niveau de protection adéquat (45§1).

Pour cela, **il n'est pas nécessaire que le niveau de protection soit identique à celui apporté en UE** par le RGPD : selon son considérant 104, et les jurisprudences CJUE de 2015 et 2020 que nous reverrons, l'expression « *niveau de protection adéquat* » s'entend comme le fait que l'Etat de destination assure « *un niveau de protection des libertés et des droits fondamentaux* ***substantiellement équivalent*** » [980] à celui garanti par le RGPD, interprété au regard de la Charte des droits fondamentaux de l'Union européenne. Cette protection est analysée au regard de diverses considérations, lesquelles **procèdent de trois dimensions emboîtées**.

* La première est relative à l'état de droit « *y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal* ». **Il s'agit de domaines fréquents d'aménagement des principes de légalité, donc de marqueurs formels de l'état de droit.** Cette dimension intègre les règles « *relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale* », et naturellement, des droits effectifs et opposables des personnes concernées (45§2, a).

* la seconde est relative aux autorités indépendantes de contrôle, chargées du respect des règles protectrices et de leur application par des pouvoirs appropriés, « *d'assister et de conseiller les personnes concernées* », et de « *coopérer avec les autorités de contrôle des Etats membres* » (45§2, b). Nous voyons que **la mise en place de guichets centralisés n'écarte pas ces dernières du dialogue, ni du contrôle**, *infra*.

[980] Arrêt préc. Schrems I du 6 octobre 2015, § 73 (alors sous l'empire de la directive 95/46), puis Shrems II, §94

* la troisième est **relative aux engagements internationaux** pris par le pays tiers ou l'organisation internationale vers lequel les données personnelles sont transférées (45§2, c).

En conséquence, la Commission dispose d'une marge d'interprétation, sous contrôle de la CJUE, quant à la notion de « *substantiellement équivalent* ». Le but des dispositions du chapitre V est **d'assurer la continuité du niveau élevé de cette protection** en cas de transfert [981]. Dès lors, la décision de la Commission doit prévoir un « *mécanisme d'examen périodique, au moins tous les quatre ans,* ***qui prend en compte toutes les évolutions pertinentes*** *dans le pays tiers ou au sein de l'organisation internationale* » (45§3). Ceci est sans préjudice d'un suivi permanent, par la Commission européenne, des « *évolutions (...)* ***qui pourraient porter atteinte au fonctionnement*** *(sic)* ***des décisions*** » (45§4).

Or, une évolution peut conduire à ce que la protection « substantiellement équivalente » soit altérée ; dans ce cas, selon les considérants du RGPD, le transfert devrait être « *interdit* » (consid. 107). Dans l'article 45, cela s'exprime dans une palette moins abrupte de décisions : abrogation, modification ou suspension « *par voies d'actes d'exécution sans effet rétroactif* » (45§5). En outre, pour des « *raisons d'urgence impérieuses dûment justifiées* », la procédure de l'article 93 peut être activée **en vue de l'adoption de décisions immédiatement applicable, en cas de crise, crispations géopolitiques, belligérance ouverte** etc. Enfin, « *la Commission engage des consultations avec le pays tiers ou l'organisation internationale en vue de remédier à la situation donnant lieu à la décision adoptée en vertu du §5* » (§6).

Pour la suite du contentieux Schrems, retenons ici que le transfert devrait à défaut d'adéquation être « *interdit* » (RGPD, consid. 107), à moins que les exigences fassent l'objet de garanties appropriées de la part du responsable du traitement ou de son sous-traitant (RGPD, article 46§1), ceci en vue de « *compenser l'insuffisance de la protection des données dans le pays tiers* » (RGPD, consid. 108). **Ainsi, des « garanties appropriées » peuvent être décorrélées d'une décision d'adéquation, si celle-ci est absente, ou si préexistante, elle est devenue caduque** [982] : nous le verrons avec le système des clauses-type (*infra*).

[981] En ce sens, avocat général, conclusions (Schrems II), point 117.

[982] Même si le mot « caducité » n'est pas employé dans le Règlement ni par la CJUE. Selon le consid. 107, une décision a pu exister et le contexte évoluer au point que le droit applicable « ***n'assure plus*** *un niveau adéquat* » (etc), ce qui en droit est une caducité (« état d'un acte juridique valable, mais privé d'effet par la survenance d'un fait postérieur à sa réalisation »).

2. Portée contraignante des décisions à l'égard des Etats membres

La décision exécutive prise sur le fondement de l'article 45 tout comme les décisions subséquentes de modifier, suspendre, abroger la décision d'« *adéquation* », s'impose **en tous ses éléments** aux Etats destinataires et donc à leurs organes concernés (article 288.4 TFUE). Le régime des décisions est inchangé depuis la directive 95/46, et non mis en cause par la jurisprudence Schrems [983].

Dès lors, les États membres (dont leurs autorités indépendantes de contrôle) **ne peuvent prendre de mesures contraire à la décision exécutive de la Commission européenne**, tant que celle-ci n'a pas été déclarée invalide par la CJUE [984].

* Pour autant, cette force obligatoire à l'égard des Etats et de leurs organes, y inclus les autorités indépendantes, **ne s'impose pas aux personnes physiques concernées** (c'est-à-dire dont les données personnelles ont été, ou ont vocation à être transmises). Ces dernières peuvent donc saisir l'autorité nationale indépendante de contrôle, d'une réclamation en vue du respect de leurs droits personnels tirés du RGPD (article 77§1 RGPD).

* Pas plus, la force obligatoire **ne saurait réduire ni *a fortiori* effacer les pouvoirs de ces autorités nationales de contrôle**, tels que reconnus par l'article 8§3 de la Charte et par les articles 51§2 et 57§1, a) du RGPD [985]. Dès lors, l'autorité saisie doit pouvoir examiner en toute indépendance « *si le transfert de ces données respecte les exigences posées par le RGPD et, le cas échéant, introduire un recours devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision d'adéquation, à un renvoi préjudiciel (...)* » [986], point sur lequel le RGPD était muet.

Mais **il s'agit d'un pouvoir d'appréciation, non d'exécution**. Selon la CJUE, « *l'autorité de contrôle compétente ne saurait suspendre ou interdire un transfert de données à caractère personnel (...) au motif qu'elle considère,* ***contrairement à l'appréciation retenue par la***

[983] Directive 95/46, article 25§ 6, arrêt Schrems I du 6 octobre 2015, préc., point 51.
[984] Schrems II, point 118, et Schrems I, point 52.
[985] Schrems II, point 119 ; Schrems I, point 53 en ce qui concerne l'article 25, paragraphe 6, et l'article 28 de la directive 95/46.
[986] Schrems II, point 120.

***Commission dans ladite décision**, que la législation (...) régissant l'accès aux données à caractère personnel transférées (...) n'assure pas un niveau de protection adéquat* » [987].

En conséquence, les autorités nationales de contrôle conservent un pouvoir autonome d'appréciation, qui **ne saurait être borné par la décision exécutive**. La juridiction nationale compétente pour saisir la CJUE d'un renvoi préjudiciel, est **tenue de considérer les modifications du droit étranger depuis la décision** de la Commission [988], si cette dernière ne l'a pas fait dans le cadre de son examen périodique ou son suivi permanent (on verra que, dans la jurisprudence Schrems I, la CJUE détectera **un vice initial d'appréciation**, *infra*).

Dès lors, si l'autorité indépendante estime que les griefs avancés par la personne physique (ressortissant national ou non [989]) contre la décision de la Commission européenne sont fondés, elle peut introduire un recours devant les juridictions nationales en vue d'une saisine de la CJUE par renvoi préjudiciel, en appréciation de la validité de cette décision [990]. Mais, quand bien même l'autorité de contrôle estimerait le grief non justifié, **le doute de la juridiction nationale saisie du refus de l'autorité de contrôle suffit**, pour justifier un tel renvoi [991].

Dans ce contexte, par son article 3, la décision de la Commission européenne n° 2000/520 (décidant d'approuver les principes du *Safe Harbour*) avait prévu une réglementation spécifique de l'exercice, par les autorités de protection des données, de leur pouvoir, dès lors que la Commission avait constaté un niveau de protection « adéquat » [992].

---

[987] Schrems II, §156.
[988] Schrems II, § 153.
[989] L'autorité nationale de contrôle est celle territorialement compétente : ainsi l'autorité irlandaise est-elle saisie par un ressortissant autrichien, du fait du siège en Irlande de la société Facebook Europe.
[990] Schrems II, § 157. Nous verrons *infra* qu'en 2023, le Parlement européen a adopté une résolution contestant cette procédure, et militant pour un recours direct des personnes.
[991] Schrems I, § 67.
[992] Par sa décision 2000/520 CE, la Commission **prétend en effet alors réduire ce pouvoir aux hypothèses** « *a) où l'organe administratif américain visé à l'annexe VII de la présente décision, ou une instance indépendante de recours au sens du point a) du principe d'application visé à l'annexe I de la présente décision, a constaté que l'organisation viole les principes mis en oeuvre conformément aux FAQ ou b) où il est fort probable que les principes sont violés; où il y a tout lieu de croire que l'instance d'application concernée ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent en vue de régler l'affaire en question; où la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves; et où les autorités compétentes des États membres se sont raisonnablement efforcées, compte tenu des circonstances, d'avertir l'organisation et de lui donner la possibilité de répondre* ». Voir la 'décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique'.

Si les autorités nationales peuvent suspendre les flux de données, elles y apparaissent privées du pouvoir de prendre des mesures prévues à l'article 25 de la directive 95/46.
Or, le législateur européen n'avait pas prévu cette restriction de leurs pouvoirs, **la Commission a donc outrepassé sa compétence** [993].

B. LES DECISIONS EXECUTIVES PORTANT « CLAUSES-TYPE » UNIFIEES DE TRANSFERT DES DONNEES

Que se passe-t-il en l'absence d'une décision d'adéquation de l'ordre juridique étranger libérant la possibilité du transfert de données sans faisceau d'autorisations ultérieures, ou en cas de caducité d'une telle décision ? **Existe-t-il un mécanisme alternatif ?**

Après avoir esquissé le régime des décisions « *d'adéquation* » prises par la Commission en vue d'autoriser le transfert hors Union des données personnelles (article 45 RGPD), nous relevons ici l'existence d'un **régime complémentaire autonome de garanties coordonnées** (article 46 RGPD), institué en pratique à compter de 2010 [994], et qui en 2021 a été actualisé [995].
Il n'est pas lieu ici d'entrer en profondeur dans le régime de telles clauses. Relevons seulement qu'il s'agit d'un système de clauses contractuelles type approuvées par la Commission (1) ; certes applicables en l'absence (ou en cas de caducité [996]) d'une décision d'adéquation, mais avec une portée plus limitée (2).

1. Fondement autonome des décisions exécutives portant clauses type

Le but est d'uniformiser les garanties contractuelles en cas de transfert des données, dans l'hypothèse d'absence de décision d'adéquation sur le fondement de l'article 45 précité. Ces clauses **ont donc une vocation générale, et ne visent pas un pays en particulier, à la**

[993] Schrems II, §101 à 103.
[994] Décision C(2010) 593 de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil.
[995] Décision (UE) 2021/914 de la Commission du 4 juin 2021relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil.
[996] L'invalidation de la décision d'adéquation n'a pas d'incidence sur la décision portant clauses type . Les décisions étant autonomes, la décision précitée de 2010 n'a pas été atteinte par l'arrêt Schrems I. Cf. conclusions de l'avocat général, 19 déc. 2019.

différence des décisions d'adéquation [997]. En outre, **elles ne sont pas nativement conçues pour une application sectorielle.** Cela impose le cas échéant une renégociation et approbation complémentaire, notamment en matière de données de santé [998].

Cette approche « par défaut » des clauses-type n'en suppose pas moins « ***des garanties appropriées et à la condition que*** *les personnes concernées disposent de droits opposables et de voies de droit effectives* », entendu au regard des garanties données par le co-contractant : les garanties n'auraient pas de signification, sans les voies de recours effectives qui dépendent du droit national du pays tiers vers lequel les données seront transférées.

Mettons de côté les voies locales de recours, lesquelles relèvent du droit national. Il n'est pas lieu ici de passer en revue le régime des garanties type **visant une protection uniforme par vecteurs multiples** ; notons seulement que l'article 46 indique que :

*** certaines peuvent être fournies « *sans que cela ne nécessite une autorisation particulière d'une autorité* (nationale) *de contrôle* »** (46§2). Ces outils variés peuvent consister en :

« a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics;

b) des règles d'entreprise contraignantes conformément à l'article 47;

c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;

d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;

e) un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées; ou

f) un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-

[997] Voir l'annexe à la Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil.

[998] L. Bardford, M. ABoy, K. Liddell, « Standard contractual clauses for cross-border transfers of health data after *Schrems II », Jl of Law and the Biosciences*, Volume 8, Issue 1, January-June 2021, lsab007.

traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées »

* en contraste, d'autres garanties proposables **nécessitent une autorisation de l'autorité de contrôle (territorialement) compétente (article 46§3).** Ce prérequis de l'autorisation est justifié par le « *mécanisme de contrôle de la cohérence* », lequel vise à l'absence d'écart ou distorsion entre appréciations nationales d'une même garantie proposée [999]. Sont concernés :
« a) des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale; ou
b) des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées ».

Rappelons encore que l'adoption de telles clauses-type relève d'un régime propre : par définition, elles ne visent pas un pays tiers, **bien que des clauses type puissent être énoncées en annexe de décisions d'adéquation** (ainsi celles en annexe de la décision *Safe Harbour)*.

Dès lors, la CJUE a eu l'occasion dans l'affaire Schrems II, de souligner qu'« ***il ne saurait être inféré de l'article 46*** (§1 et §2, c) *du RGPD* ***que la Commission serait tenue de procéder,*** *avant l'adoption d'une telle décision* (portant clauses type)*,* ***à une évaluation du caractère adéquat du niveau de protection assuré par les pays tiers*** *vers lesquels des données à caractère personnel pourraient être transférées* ***sur le fondement de telles clauses*** » [1000]. Le mécanisme repose sur la responsabilisation des opérateurs.

2. La portée limitée des clauses-type cadrant le transfert de données

Nous esquissons rapidement ici les limitations proprement juridiques, puis les limitations sectorielles propres aux données de santé.

* La première limitation de leur portée réside dans le fait que, **même en présence d'une décision portant clauses-type**, un Etat membre peut **en l'absence d'une décision**

[999] L'article 63 RGPD titré « Mécanisme de contrôle de la cohérence », dispose que « *Afin de contribuer à l'application cohérente du présent règlement dans l'ensemble de l'Union, les autorités de contrôle* ***coopèrent entre elles et, le cas échéant, avec la Commission*** *dans le cadre du mécanisme de contrôle de la cohérence établi dans la présente section* ».
[1000] Schrems II, §130.

d'adéquation, limiter « *pour des motifs importants d'intérêt public* » le transfert de catégories particulières de données vers un pays tiers ou une organisation internationale.

Par définition, les clauses types de protection adoptées sur le fondement de l'article 46 §2 c) ne visent qu'à fournir des garanties contractuelles uniformes, indépendamment du niveau de protection garanti par les pays tiers.
Dès lors, elles ne peuvent **qu'obliger le contractant à veiller au respect du niveau de protection requis, et notifier son impossibilité**. Selon la situation du pays de destination, des mesures supplémentaires peuvent devoir être adoptées [1001].

En ce sens, l'avocat général a relevé dans ses conclusions dans l'affaire « Schrems II », que **le mécanisme reposait sur la responsabilisation** du responsable du traitement des données, ou de son sous-traitant établi dans l'Union ; à titre subsidiaire, de la responsabilisation de l'autorité de contrôle compétente [1002].
Mais la clause-type ne constate pas l'adéquation d'un droit : elle vise à compenser son inadéquation éventuelle ; **elle ne lie pas l'autorité publique, seulement le co-contractant,** et ne possède pas d'effet sur l'ordre juridique de l'Etat tiers.

En conséquence, il appartient au responsable du traitement des données ou son sous-traitant établi dans l'Union, **de vérifier si le droit du pays tiers de destination des données en assure une protection appropriée**, et de fournir des garanties supplémentaires si nécessaire. A défaut, ils ou l'autorité de contrôle compétente, **doivent suspendre ou arrêter le transfert**.

Or, le cas de défaut peut découler du fait que le destinataire du transfert de données **se voit imposer ex post par le droit local, des obligations légales, administratives ou juridictionnelles** contraires aux clauses précitées, anéantissant la garantie de protection [1003].

Dès lors, la clause type doit prévoir que le destinataire du transfert de données **s'oblige à informer le responsable du traitement établi dans l'Union, s'il n'était pas ou plus en mesure** de s'acquitter de ses obligations.

[1001] Schrems II, § 133.
[1002] Conclusions de l'avocat général dans l'affaire Schrems II, § 126.
[1003] Nous verrons que, alors qu'une décision d'adéquation a été adoptée par la Commission, cela est exactement le cas de figure existant aux Etats-Unis jusqu'aux principes *Privacy* Shield qui rendent compte d'un nouvel, mais insuffisant, état du droit américain, ce que sanctionnera la jurisprudence Schrems II.

Le cas des clauses type adoptées en annexe de la décision CPT est sur ce point intéressant : le destinataire des données doit y certifier **qu'« *il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les obligations* *lui incombant conformément au contrat conclu et* *il s'engage à communiquer au responsable du traitement, sans retard après en avoir pris connaissance,* *toute modification de la législation nationale le concernant qui est susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses types de protection des données* (…) » [1004].

* Sur un plan appliqué (champ des données de santé) et non seulement général, force est de constater que les clauses types ont été élaborées pour couvrir tous types de transferts, **pas spécifiquement le transfert des données de santé**. Les parties ne peuvent parfois en négocier des modifications sans une approbation des autorités de contrôle compétentes, nous venons de le voir *supra* [1005] .

§2. SANCTION JURIDICTIONNELLE AU FOND, DU POTENTIEL D'INGERENCE ETATIQUE TIERCE

Pour les buts et dans le cadre *supra*, la sanction par la CJUE de l'action de la Commission **s'exprime de façon emblématique dans deux jurisprudences successives,** déjà citées de façon perlée : les arrêts « Schrems I » (2015) et « Schrems II » (2020).

Ces arrêts ont en commun le requérant, monsieur Schrems, citoyen autrichien : étudiant en droit, il est alors utilisateur du réseau social Facebook, société américaine dont le siège européen est en Irlande, d'où les données personnelles des utilisateurs européens sont transférées vers les Etats-Unis. M. Schrems porte plainte auprès du *Data Protection Commissioner* irlandais (territorialement compétent), du fait de l'exposition, de ce fait, de ses données personnelles au droit américain [1006].

Suite au refus de l'autorité irlandaise d'enquêter sur sa plainte, monsieur Schrems saisit la juridiction irlandaise, laquelle interroge la CJUE par voie préjudicielle sur l'interprétation des articles 7, 8 et 47 de la Charte des droits fondamentaux, des articles 35§6 et 28 de la directive

[1004] Voir la clause 5 sous b), parmi les clauses type de protection en annexe de la décision CPT.
[1005] Sur le sujet, pour un exemple de point de vue américain, C. Mitchell, J. Ordish, A. Hall, « Genomic Medicine and research: how does the GDPR apply ? », 20 (2020) www.phgfoundation.org.
[1006] Nous verrons plus bas en quoi cette jurisprudence **n'est pas une surprise, mais un aboutissement**, car les institutions européennes s'interrogeaient déjà de façon croissante et sonore sur le contenu du droit américain à compter du raidissement de 2001, bien que la décision sur les principes soit pourvue dès avant d'un vice initial.

95/46CE (alors applicable, mais le RGPD 2016 contient les mêmes dispositions à cet égard) ; et sur la validité de la décision par laquelle la Commission a en 2000 approuvé l'accord *Safe Harbour* : tel est le point de départ d'un contentieux à libération prolongée.

Cette affaire a été abondamment commentée par la doctrine, quant aux droits fondamentaux. Mais le seul terrain qui nous intéresse ici, n'est pas celui des voies de recours et de l'effectivité des droits individuels : c'est le **potentiel d'ingérence étatique**, **et la façon dont son expression formalisée en droit américain en permet l'étude**.
Rappelons que le contentieux Schrems n'existe que du fait de l'existence formalisée de ce droit, de la possibilité de le connaître et faire contrôler. Or, cela est **l'apanage des systèmes démocratiques ;** un tel raisonnement reste impossible avec/dans nombre d'autres pays.

Dès lors, nous concentrons l'attention sur deux types d'ingérences potentielles organisées par le droit fédéral américain, relevées par la CJUE parmi les causes d'invalidation des accords. Dans sa jurisprudence dite « Schrems I », il s'agit de potentielles ingérences dont la portée n'était pas précisée en droit (A) ; puis, dans sa jurisprudence dite « Schrems II », de potentielles ingérences dont la portée aura été précisée, mais insuffisamment circonscrite (B).

A. SANCTION DE POTENTIELLES INGERENCES DE PORTEE NON PRECISEE (SCHREMS I)

A partir de 1998 (en application alors de la directive 95/46CE), un accord a été négocié entre l'Union et les Etats-Unis [1007]. Conformément à son article 25§6, la Commission décide en 2000 que **les entreprises certifiant leur engagement au respect des principes convenus peuvent transférer des données** de l'Union aux Etats-Unis : c'est l'accord dit « *Safe Harbour* » [1008], dont les principes sont « *destinés à combler le fossé séparant les régimes américains et européen de protection de la vie privée* » [1009]. Les mots sont forts, mais justifiés : dans l'introduction de notre recherche, nous avons noté les écarts en droit comparé.

Des auteurs soutiennent alors l'ambition de construire les fondations internationales du commerce électronique par une « institution hybride », à rebours des théories du rôle

[1007] La désignation complète est l'accord sur les « *international safe harbour privacy principles* » ; négocié pour le compte de l'Union, par l'entremise du groupe de travail dit « de l'article 29 » précité.
[1008] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles (2000/520/EC).
[1009] Annexe IV de la décision 2000/520 de la Commission, voir B, rapporté au §10 de la décision.

dominant des acteurs privés [1010]. Mais au motif que cet accord ne permettait pas de se prémunir contre certaines dispositions du droit américain **conférant un pouvoir invasif et non contrôlable à l'autorité publique**, la CJUE invalide en 2015 l'accord « *Safe Harbour* ». Relevons la dynamique du contexte (1) avant de relever l'imprécision des buts (2).

1. La censure du *Safe Harbour* par la décision « Shrems » I n'est pas une surprise

La décision consacrant le *Safe Harbour* a été adoptée en 2000. Des commentaires parfois idéologisés de l'arrêt qui s'en suit notent rarement que, si monsieur Schrems est passé à la postérité, plusieurs réserves formalisées étaient apparues bien auparavant, dont celles de la Commission européenne même : **il serait donc injuste, même s'il est devenu commun [1011],** de voir en l'arrêt Schrems I la censure d'une Commission européenne naïve (ou pire) dans l'environnement sécuritaire exacerbé auquel, notamment depuis les attentats de sept. 2001, le monde allait être confronté, suite à la vigueur tous azimuts de la réaction fédérale américaine.

Suite à l'attentat de septembre 2001, les Etats-Unis adoptent en effet, en octobre 2001, une loi antiterroriste dite « *Patriot Act* » [1012] : entre autres applications, elle permet aux autorités fédérales d'accéder aux bases de données sises aux Etats-Unis (à distinguer : le *Cloud Act* de 2018 a une portée extraterritoriale, et en principe personnelle [1013]).

Dès lors, elle ne permet plus aux entreprises de garantir le respect des engagements pris au titre du *Safe Harbour* [1014]. Il ne s'agit certes là que d'une objectivation de pratiques qui ont pu préexister épisodiquement [1015]. Mais à compter de 2001, ces pratiques relèvent d'une échelle massive, dans un **cadre juridique contraignant, formalisé, revendiqué et assumé.**

[1010] H. Farrell, « Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement », Cambridge University Press, 15 avril 2003. L'auteur relève que de nombreux chercheurs académiques arguaient jusque là, que les Etats étaient incapables de contrôler le commerce électronique.

[1011] Le retentissement médiatique et sur les réseaux sociaux de l'affaire E. Snowden (lequel ressortissant américain ex-employé d'une Agence fédérale a révélé le programme PRISM de surveillance) y est pour beaucoup, *infra*. Ces nombreux commentaires ont surtout invoqué cette affaire, qui éclate à partir de 2014 ; mais il s'agit rarement d'analyses juridiques, nous ne les citerons donc pas : voir les très nombreuses références en ligne.

[1012] US Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) Public Law 107-56.

[1013] Clarifying Lawful Overseas Use of Data Act ou CLOUD Act (H.R. 4943). En théorie, les citoyens américains et résidents aux Etats-Unis sont seuls concernés.

[1014] Not. Z. Whittaker, « Microsoft admits Patriot Act can access EU-based cloud data », préc.

[1015] Au travers du mécanismes des « honorables correspondants » sollicités ou spontanés.

* Dès 2002, pointent donc des **réserves d'un groupe de travail européen, quant à la pertinence du système d'auto-certification des entreprises** américaines au regard du *Safe Harbour*, et à l'absence de mécanisme de règlement des différents [1016] ; en 2008, celles d'une société australienne de conseil, qui recommande à la Commission de le renégocier [1017]. En 2013, la communication COM(2013) 846 souligne l'importance de « *rétablir la confiance dans les flux des données entre l'Union européenne et les États-Unis d'Amérique* » [1018].

Or, cette communication est accompagnée d'un rapport d'un groupe de travail mixte euro-américain sur la protection des données, « *à la suite de la révélation de l'existence, dans ce pays, de plusieurs programmes de surveillance* ***incluant la collecte et le traitement à grande échelle de données à caractère personnel*** » [1019] (*infra*). Ce rapport contient une analyse détaillée de l'ordre juridique des Etats-Unis, tel qu'il résulte des nouvelles dispositions issues notamment du *Patriot Act*, adopté en 2001, après la décision exécutive européenne de 2000.

Pourtant, dès l'annexe IV de cette décision 2000/520, il était noté **que, en cas d'obligations conflictuelles, les devoirs nationaux des entreprises américaines l'emporteraient** sur les principes du *Safe Harbour* (ce qui n'est pas une surprise : des dispositions équivalentes existent en Europe). Notons, ce point y est exprès, que si une loi américaine autorise une entreprise à fournir des données personnelles à des organismes gouvernementaux **sans le consentement de l'intéressé**, cela vaut « autorisation explicite » d'enfreindre les principes du *Safe Harbour*, à la condition du respect de proportionnalité [1020].

Or, de façon emblématique, **l'unique exemple fourni est emprunté au monde de la santé** : « *un texte de loi autorisant les médecins à fournir les dossiers médicaux de leurs patients aux fonctionnaires sanitaires sans l'autorisation préalable de ces patients* ***pourrait permettre une exception aux principes de notification et de choix****. Cette autorisation ne laisserait pas la possibilité à un médecin de fournir les mêmes dossiers médicaux aux caisses de maladie ou aux laboratoires de recherche pharmaceutique,* ***car cela irait au-delà de l'objectif autorisé***

[1016] Commission Staff Working Paper du 13 février 2002, The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant toDirective 95/46 (SEC (2002) 196).
[1017] C. Conolly, « The US Safe Harbor - Fact or Fiction? » Privacy Laws & Business Int. n°96, déc. 2008, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/08_galexia_safe_harbor_/08_galexia_safe_harbor_en.pdf
[1018] C'est le titre même de la communication COM(2013) 846 final.
[1019] Daté 27 nov. 2013, « Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection»
[1020] On verra que l'absence de définition de ce principe, imposera la modification du droit américain en 2022.

par la loi et donc au-delà du champ de l'exception » [1021] . Cet exemple de « proportionnalité » est peut-être édulcoré : s'il touche à des données emblématiques par leur sensibilité, il n'évoque, de façon rassurante, que l'action de fonctionnaires **sanitaires**.

* En outre, dans sa communication 846 de 2013, la Commission relève les inquiétudes croissantes quant au niveau de protection des données personnelles transférées vers les Etats Unis, du fait qu'elles peuvent y « *être consultées et traitées par les autorités américaines* ***d'une manière incompatible avec les motifs pour lesquels elles avaient été initialement collectées*** *dans l'(Union) et avec les finalités de leur transfert vers les Etats-Unis* » [1022]. Outre un relevé de faiblesses juridiques et techniques qu'il n'est pas lieu de citer ici, la Commission y note que la « *sphère de sécurité sert également d'interface pour le transfert de données à caractère personnel de citoyens européens, de l'[Union] vers les États-Unis, par les entreprises* ***qui sont tenues de remettre des données aux agences américaines de renseignement dans le cadre de programmes américains de collecte de renseignements*** ».

Enfin, dans une communication distincte (847), également datée du 27 nov. 2013, la Commission relève que « ***toutes les entreprises participant au programme PRISM*** *[1023], qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux États-Unis* ***semblent être certifiées dans le cadre de la sphère de sécurité*** » ; que cette dernière « *est donc devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'(Union)* » (§7) [1024]. Dans la foulée, elle relève parmi les entreprises auto-certifiées au titre du *Safe Harbour*, les sociétés Google, Facebook, Microsoft, Apple et Yahoo (§ 8).

Or, la Commission souligne que cela soulève « ***de graves questions sur la continuité de la sauvegarde des droits des citoyens européens*** *en matière de protection des données lorsque des données les concernant sont transférées aux Etats-Unis* », d'autant qu' « *il n'existe (...) aucune possibilité (...) d'obtenir l'accès, la rectification ou la suppression de données ou d'exercer des voies de droit administratives ou judiciaires* ***si, dans le cadre des programmes de surveillance des États-Unis, des données à caractère personnel les concernant sont***

[1021] Voir l'annexe B de l'accord *Safe Harbour*.
[1022] Communication COM(2013) 846 final, point 2.
[1023] Programme de collecte de renseignements à grande échelle, des explications seront données *infra*.
[1024] Communication COM(2013) 847 final.

collectées et traitées ultérieurement **»** (§ 7.2). Cette communication 847 contient par ailleurs 13 recommandations en vue de pourparlers devant servir à renforcer le *Safe Harbour*.

En 2015, la CJUE invalide la décision de la Commission approuvant le *Safe Harbour* [1025]. Mais cela ne sanctionne pas une inconscience des institutions, **nous venons de le voir : cela n'est qu'une accélération de l'agenda de renégociation bilatérale.**

2. Les principes *Safe Harbour* ne s'appliquaient pas aux autorités publiques américaines

Rappelons que dans sa décision « Schrems I », la CJUE a jugé que les autorités nationales en charge de la protection des données **n'étaient pas libérées de leurs devoirs** à l'égard de leurs citoyens, par l'existence d'un accord approuvé par la Commission européenne (§59) ; que la Commission **ne pouvait, sans outrepasser ses pouvoirs, borner le contrôle,** par les autorités nationales compétentes, de ses propres constats (§66) ; que la CJUE a relevé qu'en matière de droits fondamentaux, le pouvoir d'appréciation nécessairement réduit de la Commission **appelait un contrôle strict des exigences du droit européen** (§78) [1026].

Qu'en est-il donc au fond ? L'article 1 de la décision est le cœur du sujet : la Commission y considère, sur la base de son analyse juridique et des réponses des autorités américaines éclairant l'application des principes du *Safe Harbour* [1027], que ces principes assuraient un niveau adéquat de protection des données personnelles transférées vers les Etats-Unis.

***** En fait, **le fond n'est pas défini dans les articles de la décision, mais dans ses annexes**. Les « *principes de la sphère de sécurité relatifs à la protection de la vie privée* » sont ainsi l'objet de l'annexe I. Elle constate que les Etats-Unis et l'Union européenne, s'ils partagent l'objectif de « *protéger davantage la vie privée de leurs citoyens* », ont des approches différentes. Tandis que le RGPD est un corpus unifié applicable à tous secteurs [1028], les Etats-Unis ont un système sectoriel régulé de façon disparate, et des **codes d'auto-réglementation des organisations** (al 1) ; cela conduit à ce qu'une infraction au principes auxquels l'organisation s'est déclarée adhérer, « *doit être sanctionnée conformément à la section 5 du Federal Trade Commission Act, qui interdit les pratiques déloyales ou frauduleuses* » (al 2).

[1025] Case C-362/14, Maximilian Schrems v.Data Protection Commissioner, ECLI:EU:C:2015:650, § 73.
[1026] Pour un précédent, CJUE 8 avril 2014 Digital Rights Ireland C-293/12 et C-594-12, EU :C :2014 :238, §47s.
[1027] Réponse aux « Questions souvent posées » (FAQ) ; Annexe II de la décision 2000/520/CE préc.
[1028] Hors secteurs réservés, notamment sécurité et défense nationale.

La CJUE ne met pas en cause en soi le principe d'adhésion d'une organisation au *Safe Harbour* par auto-certification (§80) ; mais elle note que la fiabilité de cette approche **repose sur des mécanismes efficaces de détection et contrôle, qui permettent d'identifier et de sanctionner d'éventuelles violations des principes** (§81). Or, les principes de l'annexe I ne sont applicables qu'aux seules organisations américaines acteurs des transferts : il n'y est pas exigé que les autorités publiques américaines mêmes y soient tenues (§82).

Ainsi, la décision ne concerne que le caractère adéquat de la protection par les principes ; **elle est mutique quant aux mesures prises par les autorités publiques américaines mêmes**.

Seul le 4ème alinéa des « principes », en annexe I, les évoque lapidairement : l' « *adhésion aux principes* » [1029] du *Safe Harbour* peut ***« être limitée par : a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis;*** *b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles* ***qui créent des obligations contradictoires ou prévoient des autorisations explicites (…)*** *; c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables. Conformément à l'objectif d'un renforcement de la protection de la vie privée, les organisations doivent s'efforcer d'appliquer ces principes de manière complète et transparente,* ***y compris en indiquant - dans leurs codes de protection de la vie privée - dans quels domaines les exceptions visées au point b) ci-dessus s'appliqueront de façon régulière.*** *Pour la même raison, lorsque les principes et/ou les lois des États-Unis permettent aux organisations de faire un choix, celles-ci sont invitées à opter, dans la mesure du possible, pour le niveau de protection le plus élevé ».* Si la fréquence d'application des exceptions citées au point b) est mise en exergue, tel n'est pas le cas pour celles du point a), qui demeure dans l'obscurité [1030].

* En conséquence, la base de raisonnement n'apparaît que dans l'alinéa 4 des « *principes de la 'sphère de sécurité' relatifs à la protection de la vie privée* » de l'annexe I, sans plus de précision, sinon qu'ils sont soumis au droit américain et interprétés selon celui-ci (alinéa 6).

[1029] L'adhésion s'entend probablement ici de l'anglais « adhérence », soit « observance » au sens du respect de principes auquel on s'est déjà engagé. Il ne s'agit pas d'un limitation formelle de l'adhésion initiale.
[1030] Cela n'est-il pas somme toute, que l'expression d'une réserve de souveraineté nationale ? On peut imaginer que, à front inversé des transferts de données, elle eût été réciproque !

Dans son annexe II, le thème de l'article 1 alinéa 4 a) est absent des « questions posées fréquemment » (*Frequently Asked Questions*–FAQ), en l'occurrence publiées par le ministère du commerce des Etats-Unis [1031]. Aucun éclairage sur ce point n'a été produit d'office, ni ne semble avoir été requis, à la différence, par exemple, **de multiples questions sur les produits pharmaceutiques, les technologies médicales, la recherche en matière biomédicale** [1032].

Dans son annexe IV titrée « *Confidentialité et dommages-intérêts, autorisations légales et fusions et acquisitions suivant la législation des Etats-Unis* », se niche un B rappelant que, en cas de conflit d'obligations entre les principes du *Safe Harbour* et la législation américaine (présente et à venir), **les obligations nationales priment pour toutes organisations américaines,** même si elles sont parties de la « sphère de sécurité ».

Dès lors, la CJUE relève que la dérogation prévue à l'annexe I rend **« *possible des ingérences, fondées sur des exigences relatives à la sécurité nationale et à l'intérêt public ou sur la législation interne des États-Unis,* ***dans les droits fondamentaux des personnes dont les données à caractère personnel sont ou pourraient être transférées depuis l'Union vers les Etats-Unis*** ». Cela est ici affaire de principe : le caractère sensible (de santé, notamment [1033]) ou non des données personnelles, tout comme l'existence ou non d'un « inconvénient » résultant de l'ingérence publique, **sont indifférents** (§87) [1034]. En outre, la CJUE note l'absence de relevé, dans la décision 2000/520, de règles étatiques visant à encadrer de telles ingérences (§88), et l'absence de protection juridique des intéressés contre celles-ci (§89) [1035].

Ainsi, les autorités américaines pouvaient accéder aux données y compris de santé et les traiter, d'une façon non compatible avec les finalités de leur transfert, **au-delà de ce qui était « *nécessaire et proportionné* » à la protection de leur sécurité nationale** ; de ces éléments de fond, outre de procédure, résulte l'invalidation en 2015 par l'arrêt « Schrems I ».

[1031] Sachant que les FAQ ont essentiellement été posées par les opérateurs américains du fait des différences d'approche juridique, avaient « *fait part de leur incertitude quant à l'incidence d'un "niveau de protection adéquat" sur les transferts de données à caractère personnel de l'Union européenne vers les Etats-Unis* », ibid., alinéa 1.

[1032] FAQ 14 « produits pharmaceutiques et médicaux », 7 questions sur les données issues de la recherche, sur les conséquences de retrait d'essais, la surveillance des marchés, etc. On le reverra *infra*.

[1033] **Première donnée citée parmi les informations sensibles dans l'annexe II** qui traite des choix d'opposition à communication ; et seul exemple cité, en annexe IV, pour les « *autorisations légales explicites* ».

[1034] Ce que la CJUE avait déjà jugé peu auparavant : CJUE préc. 8 avril 2014 Digital Rights Ireland C-293/12 et C-594-12, point 33.

[1035] Dans ses conclusions, l'Avocat général a relevé qu'il existait bien des mécanismes de règlement des litiges, mais limités à des litiges commerciaux avec des entreprises, ne couvrant donc pas le contrôle de légalité d'ingérences qui relèveraient de l'action publique : Conclusions Avocat général, points 204 à 206, sur la base des réponses américaines à la FAQ 11 figurant à l'annexe II de la décision 2000/520.

Cela n'est pas une surprise : si la réserve de sécurité et défense nationale est légitime (il ne s'agit pas moins d'un intérêt public pour les Etats membres de l'Union, article 23 RGPD), la Commission avait elle-même noté ces points dans ses communications précitées ; ses recommandations ont d'ailleurs servi de base de renégociation avec les autorités américaines [1036] ; la Commission n'aura donc qu'été prise de vitesse.

Mais sa décision portant le *Privacy Shield*, censé corriger les faiblesses du *Safe Harbour*, va être également sanctionnée.

B. POTENTIELLES INGERENCES DE PORTEE PRECISEE, MAIS NON SUFFISAMMENT LIMITEE (SCHREMS II)

Le débat de fond qui aura anticipé l'arrêt « Schrems I » rendu en octobre 2015, explique l'adoption rapide (juillet 2016) de la décision approuvant le *Privacy Shield* [1037]. L'enjeu est de pallier l'incertitude dans laquelle l'invalidation du *Safe Harbour* a plongé les opérateurs européens autant qu'américains, sur fond de transferts de données personnelles devenus massifs dans la nouvelle économie numérique, incluant le traitement sophistiqué des données.

Mais **la décision *Privacy Shield* ne marque pas la fin du débat** sur le cadre des transferts de données personnelles, au contraire. En 2017, une communication de la Commission sur le transfert global, au-delà du contexte transatlantique, est publiée [1038], suivie en janvier 2018 d'une réflexion du groupe de travail sur la protection des données [1039]. Elle est ravivée par l'adoption en mars 2018 aux Etats-Unis du CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*), d'objet différent du Patriot Act [1040], etc. Le contexte reste ainsi très dynamique (nous verrons *infra* le panorama en 2023), son analyse n'est pas en soi l'objet de notre recherche.

[1036] COM(2013) 846 final et COM(2013) 847 final ; notamment les 13 recommandations dans cette dernière.
[1037] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.
[1038] Communication from the Commission to the European Parliament and the Council, « Exchanging and Protecting Personal Data in a Globalised World », COM(2017)7 du 10 janvier 2017.
[1039] European Data Protection Board (groupe de travail de l'article 29), « Adequacy Referential », WP 254 rev. 01 adopté le 28 nov. 2017, version révisée adoptée le 6 févr. 2018.
[1040] Cette loi permet en substance l'accès, par des administrations publiques autorisées par une juridiction, à des données relatives aux citoyens ou aux résidents américains qui sont hébergées dans des serveurs d'autres pays.

Il suffit ici de relever que le 16 juillet 2020, la CJUE invalide la décision de la Commission portant le *Privacy Shield*, suite à un recours préjudiciel soulevé dans un nouveau contentieux initié par M. Schrems [1041]. Nous n'entrerons pas dans les détails de l'affaire à l'origine de cet arrêt « Schrems II », et nous en tiendrons au **raisonnement de la juridiction sur la question de l'adéquation de la protection** offerte par les principes, au regard des exigences tant du RGPD que de la Charte européenne des droits fondamentaux.

Alors que la CJUE avait reproché au *Safe Harbour* son laconisme, *le Privacy Shield* donne lieu, de la part de la Commission européenne, à une **justification approfondie et documentée de l'ingérence potentielle des autorités américaines dans les données personnelles transférées** vers les Etats-Unis. Les fondements légaux des programmes de renseignement et doctrines des agences américaines etc. y sont détaillés ; le tout a donné lieu aux Etats-Unis à publication en miroir, pour une pleine opposabilité aux acteurs et autorités.

Pour autant, la décision est une nouvelle fois annulée (nous en resterons au point d'intérêt dans le cadre de notre recherche) : si la finalité sécuritaire de l'ingérence est reconnue légitime (1), le potentiel d'ingérence n'est pas circonscrit dans des termes satisfaisants (2).

1. La reconnaissance de la finalité non illégitime des programmes de surveillance

Notre intitulé est elliptique, car la CJUE **ne qualifie expressément ces programmes, ni de « légitime », ni de « non illégitime »** : cela résulte d'un raisonnement par inférence. En outre, la notion d'« intérêt public » (sécurité et défense nationales) existe également nous l'avons vu en droit européen, comme motif de dérogation au principe du consentement au traitement.

* Dans sa décision *Privacy Shield* de 2016, la Commission considère à nouveau que les Etats-Unis offrent un niveau adéquat de protection des droits fondamentaux des personnes quant à leurs données personnelles. Pour ce faire, elle se livre une nouvelle fois, à une analyse détaillée des limitations et des garanties prévues en droit américain [1042].

Mais, en contraste de sa décision *Safe Harbour* laconique sur ce point, la décision d'adéquation pour le *Privacy Shield* **rapporte largement les fondements et le cadre**

[1041] CJUE 16 juill. 2020, Aff. C-311/18 préc.
[1042] Considérants 67 à 135 de la décision *Privacy Shield* préc.

juridique de l'ingérence [1043] potentielle des autorités américaines. En outre, la Commission y veille à une motivation précise et approfondie de son appréciation, dans un copieux chapitre de considérants dédiés [1044], lequel vient cette fois *en sus* des nombreuses annexes intégrant les correspondances et les déclarations des institutions américaines impliquées.

Les textes fédéraux en cause sont le *Foreign Intelligence Surveillance Act* (FISA) [1045], dont depuis 2008, l'article 702 autorise l'acquisition de renseignement sur les citoyens non américains résident hors des Etats-Unis ; *l'Executive Order 12333* (EO 12333) [1046], (*infra*) ; enfin, la *Presidential Policy Directive 28* (PPD-28) [1047], pour partie modifiée en 2022, pour permettre le nouvel accord transatlantique [1048] . Ces textes fondent et encadrent l'action des services américains sur ces points. Tous sont ici considérés **selon leur contenu d'alors**.

Ainsi, il est acté que les exigences nationales puissent primer les principes du *Privacy Shield* ; mais la Commission de souligner **une réserve qui n'apparaissait qu'en filigrane dans sa décision *Safe Harbour*** : les ingérences « *des autorités publiques américaines dans l'exercice des droits fondamentaux des personnes (...) pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois et, partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes* ***seront limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective*** *contre des ingérences de cette nature »* : cela constitue la réponse de la Commission aux deux axes de critiques de la CJUE dans son arrêt « Schrems I », *supra*.

Mais c'est là une pétition de la Commission, non une disposition du droit fédéral américain, lequel n'a pas alors consacré formellement le principe de nécessité/proportionnalité (qui ne figure qu'implicitement, par inférence des textes).

[1043] Rappelons que nous utilisons ce terme dans le seul sens de son usage par la CJUE.
[1044] Section dédiée de considérants sous le titre « Accès aux données à caractère personnel transférées dans le cadre du bouclier de protection des données UE - Etats-Unis et utilisation de ces données par les autorités publiques américaines », §64 à §135.
[1045] Adopté en 1978, pour réguler la surveillance physique et électronique des communications pour un but de renseignement extérieur. Il a été plusieurs fois amendé, notamment par le USA PAtriot Act (2001), FISA AMendments Act (2008), USA Freedom Act (2015).
[1046] Signé en 1981 par le président Reagan, qui étend le pouvoir et les responsabilités des agences américaines ; il a été amendé par l'EO 13355 (2004) pour le management de l'action des agences, puis par l'EO 13470 (2008) pour renforcer le rôle du directeur du renseignement national (DNI).
[1047] Adopté le 17 janv. 2014, Presidential Policy Directive 28 (PPD-28) Signals Intelligence Activities.
[1048] Signé le 7 octobre 2022 par J. Biden, titré « Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities ».

* La CJUE relève que les principes du *Privacy Shield* contiennent une dérogation à caractère général (§165). Elle prend acte de l'explicitation, par la Commission européenne, des programmes de surveillance mis en œuvre en application de l'article 702 du FISA : il s'agit du programme PRISM (requalifié downstream en 2017) [1049], du programme UPSTREAM [1050] ; ainsi que de l'EO 12333. Ces programmes **fondent la non-application des principes au respect desquels les entreprises américaines se sont engagées par le système de l'autocertification** ; ils confèrent une immunité légale en cas d'obéissance aux (seuls cas de) demandes gouvernementales. La question est ici celle de la qualification de la finalité.

Selon la CJUE, une telle dérogation aux principes du *Privacy Shield* peut s'entendre du fait que les articles 7 et 8 de la Charte des droits fondamentaux de l'Union Européenne **n'apparaissent pas des prérogatives absolues des individus : il doivent être considérées selon leur fonction dans la société qui les protège** (§172) [1051].

En effet, l'article 8 de la Charte prévoit une exception au consentement de la personne au traitement : celle d'un « *fondement légitime prévu par la loi* ». Ce fondement est ici prévu par la loi américaine, et n'apparaît pas illégitime [1052] ; encore faut-il, selon nos principes de finalité et proportionnalité, que les limitations légales aux droits fondamentaux **soient nécessaires et répondent effectivement à des objectifs d'intérêt général** (Charte, article 52§1), et que ces ingérences, légalement prévues, soient elles-mêmes explicitement limitées.

Nous serons bref : la CJUE constate que la limitation des droits fondamentaux procède de la législation américaine examinée par la Commission. L'examen de celle-ci la conduit à ne pas mettre en cause le principe même des programmes de surveillances décrits (lequel n'est pas en soi incompatible avec l'article 52§1 de la Charte).

La finalité est admissible, **le problème est celui de la proportionnalité de l'ingérence.**

[1049] Egalement appelé « US-984XN ». Programme de surveillance électronique pour collecte d'informations via internet et des fournisseurs de services numériques (comme les GAFAM) créé en 2007 par le *Protect America Act*, en remplacement du contesté *Terrorist Surveillance Program* mis en place en 2001. Le programme PRISM est connu pour avoir été dénoncé par E. Snowden.

[1050] Programme de surveillance électronique, lequel, en contraste du programme PRISM, vise essentiellement les communications transitant par internet.

[1051] Et jurisprudences citées, dont CJUE Aff. C-92/09 et C-93/09 du 9 nov. 2010, Volker und Markus Schecke et Eifert, EU:C:2010:662 §48 ; Aff. C-291/12 du 17 oct. 2013 Schwarz, §33, EU:C:2013:670.

[1052] Rappelons que la CJUE ne le dit pas ainsi. Mais ce fondement n'est que le pendant des intérêts publics nationaux des Etats membres, lesquels peuvent faire obstacle à l'application du droit commun dans l'Union.

2. La dénonciation d'une absence d'exigence de proportionnalité dans l'atteinte aux droits

L'analyse de proportionnalité **appelle l'examen des exigences internes de mise en œuvre de ces programmes fédéraux**, ces exigences étant censées assurer *« dans le respect du principe de proportionnalité, une niveau de protection substantiellement équivalent à celui garanti par l'article 52§1 seconde phrase* » de la Charte (§178).

Or, l'examen de l'article 702 du FISA conduit à relever que le FISC (*Foreign Intelligence Surveillance Court*) *« n'autorise pas de mesures de surveillance individuelle, mais plutôt des programmes de surveillance (comme PRISM ou UPSTREAM)* ».
Si le contrôle exercé par le FISC vise à vérifier que ces programmes ont bien pour objectif l'acquisition d'informations en vue du renseignement extérieur (et pas d'autre objectif, qui serait illégitime – mais le champ est déjà vaste), ce contrôle **ne vise donc pas à vérifier que « *les personnes sont correctement ciblées* *pour se procurer des informations en matière de renseignement extérieur* »** [1053], nous n'entrerons pas dans le détail.

Dès lors, il en résulte pour l'avocat général [1054], suivi par la CJUE (§180), que cet article 702 du FISA **ne permet pas d'assurer le niveau substantiellement équivalent de protection requis** en application de la Charte, en l'absence de « *règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales* » (ibid.).

Cela est confirmé par une analyse complémentaire. Certes, la mise en œuvre des programmes prévus par l'article 702 FISA doit respecter les prescriptions de la PPD-28 (*Presidential Policy Directive 28*), laquelle vise à encadrer les activités de renseignement [1055].

Mais celle ci permet **la collecte « en vrac »** (*bulk collection*) de volumes importants d'informations d'origine électronique, **quand un identifiant ne peut être associé à une cible spécifique** [1056].

[1053] Considérant 109 de la décision *Privacy Shield*, CJUE Schrems II, § 179.
[1054] Conclusions de l'avocat général, points 291, 292 et 297.
[1055] Adoptée en janvier 2014, partiellement révoquée en octobre 2022 (« National Security Memorandum on Partial Revocation of Presidential Policy Directive 28 »). La PPD-28 établit des politiques et procédures de restrictions quant à la collecte de renseignement par les services américains.
[1056] Selon la lettre du 21 juin 2016 du bureau du directeur du renseignement national (Office of the Director of National Intelligence), voir VI de la décision *Privacy Shield*.

Or, selon l'EO 12333, cette pratique est applicable à des données en transit vers les Etats-Unis, mais sans surveillance judiciaire ni encadrement satisfaisant (§183). Enfin, ni le PPD-28, ni l'EO 12333, ne confèrent aux personnes concernées de droits opposables devant les tribunaux (§181 et §182), ce en contradiction avec l'article 45§2, a) du RGPD.

En conséquence, la CJUE juge que, « *ni l'article 702 du FISA ni l'E.O. 12333, lus en combinaison avec la PPD-28, ne correspondent* ***aux exigences minimales attachées, en droit de l'Union,*** *au principe de proportionnalité, si bien* ***qu'il n'est pas permis de considérer que les programmes de surveillance fondés sur ces dispositions sont limités au strict nécessaire*** **»** (§184).
A cette réserve majeure sur la (nécessité et) proportionnalité, s'ajoute la critique récurrente de l'absence de possibilité de contrôle juridictionnel effectif (requis à l'article 47 de la Charte), question de procédure fondamentale, mais hors de notre sujet [1057].

Ces motifs fondent l'invalidation par la CJUE de la décision *Privacy Shield* ; cela **impose la recherche d'un nouveau cadre** pour le transfert transatlantique des données personnelles. Dans la période transitoire (relais par les clauses) ; cela a mis les *Data Protection Officers* de part et d'autre de l'Atlantique sous pression, pour expliquer les conséquences et permettre la continuation des transferts : on le reverra *infra* en matière de données de santé [1058].

De ce fait, les enjeux économiques et politiques des transferts de données **vont conduire à la modification du droit américain**, **lequel ne permettait pas, à droit constant**, une nouvelle décision européenne d'adéquation.

Sur le terrain de la souveraineté, cela marque un remarquable positionnement européen, au moins en termes de logique formelle : voyons-le dans la décision de 2023, et ses préalables.

[1057] CJUE Schrems II, § 186 à § 197.
[1058] Dès ici signalons L. Bradford, M. Aboy, K. Lidell, « Standard contractual clauses for cross-border transfers of health data after *Schrems II* », *Journal of Law and the Biosciences*, Volume 8, Issue 1, January-June 2021, lsab007 ; J. Liss, D. Peloquin, M. Barnes, B.E. Bierer, « Demystifying *Schrems II* for the cross-border transfer of clinical research data », *Journal of Law and the Biosciences*, Volume 8, Issue 2, July-December 2021, lsab032.

SECTION 2. LA MODIFICATION DU DROIT AMERICAIN REQUISE PAR LA RECHERCHE DE GARANTIES COORDONNEES

Pour la Commission, il est contrariant que ses décisions soient par deux fois désavouées par la CJUE pour des motifs non si éloignés. Toutes les précautions semblaient avoir été prises ; mais c'était sans compter **l'absence de formalisation, en droit américain, des critères** de « nécessité » et de « proportionnalité » qui dominent explicitement en droit européen. Dès lors, **la décision d'adéquation ne peut être prise à droit américain constant.**

Certes, il en résulte une onde de choc en Europe , mais plus encore aux Etats-Unis : elle met en exergue des protections normatives et garanties juridictionnelles des citoyens en matière de protection des données dont jusqu'à peu, « *les Etats-Unis s'estimaient leaders mondiaux* » [1059].

Cessant d'être méconnu du grand public, **l'enjeu des transferts de données personnelles est ainsi devenu polarisant au plan national,** avec parfois des conséquences sonores, notamment sur le régime des bases de données de santé (*supra*).
Dès lors, c'est aussi de façon publique, non plus seulement dans les cercles avertis, que **la question de la souveraineté européenne en matière de serveurs pour les bases de données en général (en santé en particulier), complète la question des droits fondamentaux individuels**, mais ceci n'est pas le sujet de notre recherche.

Nous relevons ici la façon dont l'élaboration du nouveau cadre de transfert transatlantique des données personnelles, titré *Data Privacy Framework Principles,* approuvé par décision de la Commission en juillet 2023, a donné lieu à une forte mobilisation transatlantique (§1) ; cela avant d'examiner la place particulière acquise par les données de santé dans ce contexte (§2).

[1059] F.D. Bellamy, « US data privacy laws to enter new era in 2023 », Reuters, 12 janvier 2023. Par ailleurs, dans le sillage de la Californie, quatre Etats (Colorado, Connecticut, Utah, Virginia) vont en 2023 commencer à mettre en œuvre leur législation inspirée du RGPD.

§1. LES CONDITIONS DE L'AVENEMENT DU « *EU-US DATA PRIVACY FRAMEWORK PRINCIPLES* » DE 2023

Dans son arrêt Schrems II, la CJUE a jugé que les garanties et limitations quant à l'accès par l'autorité publique américaine aux données personnelles transférées aux Etats-Unis, n'étaient pas établies d'une façon suffisante (§185), et que les intéressés ne disposaient pas de droits ni voies de recours effectifs devant l'autorité américaine dans ce cas (§197).

Mais la finalité même de l'ingérence étatique par voie de droit revendiquée n'est pas en cause : l'exception au consentement des personnes pour des motifs d'intérêt public supérieurs (sécurité nationale, défense nationale, sécurité publique) est également prévue dans le RGDP [1060]. Ce n'est donc pas tant la nécessité, que la proportionnalité et les garanties de droits et recours effectifs, qui sont contestés.

Ce deuxième jugement invalidant le *Privacy Shield*, a aussitôt conduit à **de nouveaux pourparlers entre la Commission européenne et le gouvernement américain [1061]**, en vue d'examiner les conditions d'une nouvelle décision.
En mars 2022, la présidente von der Leyen et le président Biden sont convenus d'un accord de principe, lequel « ***marque un engagement sans précédent de la part des États-Unis*** *à mettre en œuvre des réformes qui renforceront les mécanismes de protection de la vie privée et les libertés civiles applicables aux activités américaines de renseignement d'origine électromagnétique* » [1062]. Dès décembre, un projet de décision d'adéquation était présenté par la Commission, pour soumission à l'avis du CEPD (*infra*) [1063], puis adopté en juillet 2023 [1064].

Nous ne traiterons à nouveau ici que de la dynamique des garanties quant à la proportionnalité de l'ingérence étatique, non des droits et voies de recours individuels. **Dans cette recherche de garanties contre les accès illicites, l'effet de levier obtenu par l'Union pour ses 27**

[1060] Pour rappel, le RGPD prévoit (art. 23§1) que si dans l'intérêt public, le droit de l'Union ou d'un Etat membre peut limiter la portée des droits et obligations qu'il consacre, « *une telle limitation (doit respecter) l'essence des libertés et droits fondamentaux et* (constituer) *une mesure nécessaire et proportionnée dans une société démocratique pour garantir : a) la sécurité nationale, b) la défense nationale, c) la sécurité publique (etc)* ».
[1061] Leaders (US) la secrétaire d'État au commerce G. Raimondo, et (UE) le commissaire à la justice D. Reynders.
[1062] Déclaration conjointe de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles, 25 mars 2022 ; voir la fiche technique (une page) de la Commission européenne synthétisant les mérites du nouveau « Trans-Atlantic Data Privacy Framework », mars 2022.
[1063] Draft Adequacy Decision, 13 décembre 2022.
[1064] Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023) 4745 final.

Etats membres, est ainsi remarquable : il n'aurait pu être obtenu de façon dispersée par les Etats, par défaut de taille critique et d'importance relative dans le commerce international.

Ainsi préparé, le nouvel accord vient d'être, en juillet 2023, considéré comme « *adéquat* » par la Commission ; mais il était, et reste subordonné à l'adaptation par les Etats-Unis de leurs propres normes (A). Il en résulte dans l'accord, un *corpus* détaillé (B).

A. UNE ADEQUATION SUBORDONNEE A L'ADAPTATION EN 2022 DES NORMES FEDERALES AMERICAINES

L'analyse en profondeur du droit fédéral spécialement applicable aux ingérences de l'autorité américaine en matière de données personnelles transférées sur son territoire (article 702 FISA ; PPD 28 ; E0 12333 préc.), avait en 2020 conduit la CJUE a considérer ses garanties et limitations comme insatisfaisantes, au regard de la Charte, soulevant de nombreuses inquiétudes, en matière notamment de transferts de données de santé, *infra*.

Dès lors, l'importance de ce cadre pour les échanges transatlantiques sécurisés et fluides (mais aussi pour le témoignage de la force de la « *communauté de démocraties* » [1065]) a conduit en octobre 2022 à une modification nécessaire du droit américain (1), libérant l'approfondissement des délibérations européennes (2). Le but est l'obtention d'un cadre justifié, approuvé donc en 2023 par la Commission… munie de toutes ces précautions.

1. La modification provoquée en octobre 2022 du droit fédéral américain

Nous avons vu que la lettre du droit américain n'était pas satisfaisante (en logique formelle, indépendamment de toute pratique), et que le principe de la nécessité et proportionnalité de l'ingérence **était une pétition européenne, non une disposition littérale du droit fédéral.**

Or, les discussions entre la Commission européenne et le gouvernement fédéral américain ont aboutit, d'une part, à l'adoption le 7 octobre 2022 par le président Biden d'un nouveau décret exécutif, l'EO 14086, **visant à renforcer les garanties en matière d'activités de renseignement** [1066], dont l'objet est essentiellement satisfaire aux attentes de la partie européenne, nous allons y revenir. D'autre part, en application de cet EO 14086 (mais publié

[1065] Déclaration conjointe du 25 mars 2022, préc.
[1066] EO 14086 « *Enhancing Safeguards for United States Signals Intelligence Activities* », E.O. 14086 of Oct 7, 2022 ; FR doc. 2022-22531.

le même jour, l'établissement par le procureur général des Etats-Unis **d'une juridiction d'appel dédiée, la *Data Protection Review Court*** : elle sera compétente pour l'examen indépendant des décisions prises en amont par l'officier en charge de la protection des libertés civiles auprès du bureau du directeur national du renseignement américain [1067].

Nous ne reviendrons pas sur cette organisation juridictionnelle en application de l'EO 14086, lequel remplace dans une large mesure le PPD-28 précité [1068]. **En revanche, ce dernier introduit en 2022 les concepts (formellement) inédits en droit fédéral, de nécessité et de proportionnalité dans l'acquisition de renseignement électronique**, ce qui conduit à de forts développements du texte.
Relevons seulement le contenu de sa section 1, laquelle énonce le but de cet EO, en mariant les considérations publiques et privées, nationales et internationales :

* « *the United States collects signals intelligence so that its national security decisionmakers have access to the timely, accurate, and insightful information necessary to advance the national security interests of the United States and to protect its citizens and the citizens of its allies and partners from harm. Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment* (…) ».
L'accent est politiquement mis sur la protection des citoyens des Etats-Unis, des citoyens de ses alliés et partenaires. Cette protection n'est naturellement pas l'unique fin d'un tel système ; mais elle était le point de focale de tous les textes et jurisprudences européennes sur le cadre du transfert. **Sans citer l'Union, cela est un signal clair dans sa direction**.

* En outre, *« (...) the United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners. At the same time, the United States recognizes that signals intelligence activities must take into account* ***that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information****. Therefore, this order establishes safeguards for such signals intelligence activities* ».

[1067] AG Regulation Establishing the DPRC, de l'Attorney General Merrick Garland. 28 CFR Part 302. (CFR = Code of Federal Regulations).
[1068] La section 5(f) de cet EO explique qu'il a le même champ d'application que le PPD-28 (à l'exception des activités de renseignement électronique entreprises pour tester ou développer des capacités en la matière.

Si l'Union européenne se félicite de façon sonore (enjeu de politique intérieure et de prestige international), d'un effort sans précédent de la part des Etats-Unis, au profit de cette relation transatlantique [1069], la motivation de l'EO 14086 reste pudique, quant aux raisons de cette transformation importante du droit fédéral américain : **aucun souverain ne reconnaîtra modifier son droit sous la pression d'un autre**, sa politique intérieure est en jeu.

Mais l'analyse de la décision exécutive de la Commission de juillet 2023 met en évidence que ces deux modifications significatives du droit fédéral américain **ne suffisent pas à établir l'adéquation au sens de l'article 45 RGPD.** En effet, il y est précisé que la pleine « adéquation » **s'entend sous la réserve d'une adaptation complémentaire vérifiable à court terme, d'autres normes internes du droit américain**.

Ainsi, dans la décision exécutive de la Commission européenne du 7 juillet 2023, il est relevé que, d'une part, les exigences de l'EO 14086 s'applique à toute la communauté du renseignement aux Etats-Unis ; que, **d'autre part et surtout,** elles doivent « *be further implemented through agency policies and procedures* ***that transpose them into concrete directions*** *for day-to-day operations. In this respect, EO 14086* ***provides U.S. intelligence agencies with a maximum of one year to update their existing policies and procedures*** *(i.e. by 7 October 2023) to bring them in line with the EO's requirements* » (considérant 126).

Le même considérant européen de relever (alors que c'est là affaire de compétence américaine), les processus internes d'actualisation des politiques et procédures [1070].

Il en résulte que la décision d'adéquation de juillet 2023 est, **de façon inédite, une décision d'adéquation conditionnelle, mécanisme que ne prévoit pas explicitement l'article 45 RGPD.**

Mais **cette condition n'est pas dirimante**, car elle ne porte que sur des éléments complémentaires : ainsi, la Commission européenne peut-elle montrer à la CJUE (et aux opinions publiques européennes) qu'elle les aura bien perçus… à toutes fins utiles.

[1069] Déclaration conjointe du 25 mars 2022, préc.

[1070] Sur ces processus, cf. la publication le 3 juillet 2003 sur le site gouvernemental https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures- implementing-new-safeguards-in-executive-order-14086.

2. La prise en compte des délibérations européennes formulées au printemps 2023

Les enjeux juridiques, économiques et politiques, les péripéties jurisprudentielles des cadres de transfert *Safe Harbour* puis *Privacy Shield*, et le degré de garanties requis ayant imposé l'adaptation du droit fédéral américain, ont conduit à un **approfondissement important de la réflexion**, dont on citera ici deux étapes emblématiques : l'avis du contrôleur européen des données (CEPD) rendu le 28 février 2023 sur le projet de cadre, où il exprime des soucis résiduels ; puis la résolution du Parlement européen du 11 mai 2023, qui reste critique.

* L'avis du CEPD accueille favorablement le projet de cadre, en saluant spécialement l'introduction par l'EO 14086 d'exigences spécifiques à la nécessité et proportionnalité dans les actions de recueil de renseignement électronique.

Mais il note que des dispositions de mise en œuvre pratique interne aux Agences américaines sont requises, **pour la mise en place effective de tels principes de nécessité et proportionnalité inédits en la matière aux Etats-Unis**. La question de la collecte massive non sélective de données électroniques (*bulk collection*), puis la rétention et dissémination des données ainsi collectées, demeurent pour le CEPD parmi les points d'attention [1071].

En outre, le CEPD s'exprime soucieux de l'absence d'exigences d'une autorisation préalable par une autorité indépendante pour ce qui est de cette collecte massive non sélective (*bulk*) en application de l'EO 12333, et de l'absence d'examen systématique indépendant *a posteriori* par une juridiction ou par un organisme équivalent.

En ce qui concerne l'autorisation préalable indépendante en application de l'article 702 du FISA, le CEPD regrette également que la FISC [1072] **n'examine pas la « *compliance* »** [1073] de la certification des programmes autorisant le ciblage de citoyens non américains, à l'égard de l'EO 14086.

Si nous citons ces réflexions ici, c'est **car le degré d'examen du droit fédéral américain par le CEPD (et par inférence, de ses recommandations) est frappant : cette immixtion apparaît inédite dans une matière de souveraineté ombrageuse**, alors que le droit américain vient de surcroît d'être modifié en 2022. D'un point de vue technique, il met aussi

[1071] Un autre est le mécanisme juridictionnel du DPCR, qui échappe à notre champ de recherche.
[1072] Pour rappel, *Foreign Intelligence Surveillance Court*, mise en place par le FIS Act, *infra*.
[1073] Nous ne traduisons pas ici le mot « compliance », lequel ne porte pas de contenu conceptuel précis en droit français : il oscille entre conformité à un standard formalisé, et respect de règles non nécessairement explicites.

en exergue que, à l'approche historique de la recherche par ciblage souvent complexe et/ou coûteux des personnes, les technologies nouvelles à coûts décroissants et puissance exponentielle ont ouvert (depuis quelques années déjà) **un changement de paradigme.**

* Le Parlement européen a également émis un avis le 11 mai 2023 quant à l'adéquation de la protection assurée par le cadre proposé, sous la forme d'une résolution [1074]. Ce n'est pas sa première implication politique en la matière : **cette implication débute en 2014 avec son rapport sur les révélations de E. Snowden, concernant la surveillance électronique de masse** des citoyens de l'Union [1075]. Il s'en est suivi une résolution en mai 2016 sur les flux de données transatlantiques [1076], puis deux résolutions en avril 2017 [1077] (publiée JO en 2018), puis en juillet 2018 (publiée JO en 2020) [1078] sur l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis ; suivies de sa résolution de mai 2021 (publiée au JO en 2022) suite à l'arrêt de la CJUE « Schrems II » [1079].

Il n'est pas lieu ici de détailler leur contenu, hors champ de notre recherche. **Ces résolutions successives, et souvent vives, témoignent de la forte sensibilité politique du sujet**.

Notons seulement que le Parlement y rappelle, en conclusion de sa résolution de mai 2023, qu'il avait dans sa résolution de mai 2021 invité la Commission **à ne pas adopter de nouvelle décision d'adéquation à l'égard des Etats-Unis à moins de réformes significatives** (la victoire est acquise depuis 2022…). Mais il « *estime que le décret* (EO) *14086 n'est pas suffisamment constructif* » (reprenant les remarques précitées du CEPD).

En outre, il « *réaffirme que la Commission ne devrait pas laisser à la Cour de justice de l'Union européenne la mission de protéger les droits fondamentaux des citoyens de l'UE à la suite de plaintes déposées par ces citoyens à titre individuel* » (§15). **On peut s'en étonner**,

---

[1074] P9_TA(2023)0204Adéquation de la protection assurée par le cadre de protection des données UE–Etats-Unis : Résolution du Parlement européen du 11 mai 2023 sur l'adéquation de la protection assurée par le cadre de protection des données UE–États-Unis (2023/2501(RSP)).

[1075] Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)), Document 52014IP0230.

[1076] Résolution du Parlement européen du 26 mai 2016 sur les flux de données transatlantiques (2016/2727(RSP)), Document 52016IP0233.

[1077] Résolution du Parlement européen du 6 avril 2017 sur l'adéquation de la protection offerte par le bouclier de protection des données UE-États-Unis (2016/3018(RSP)), Document 52017IP0131.

[1078] Résolution du Parlement européen du 5 juillet 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE–États-Unis (2018/2645(RSP)), Document 52018IP0315.

[1079] Résolution du Parlement européen du 20 mai 2021 sur l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems (« arrêt Schrems II ») (2020/2789(RSP)), Document 52021IP0256.

car la modification des voies de recours relève nécessairement de la compétence législative, non exécutive [1080] etc.

Le tout pour conclure que « ***le cadre de protection des données UE–États-Unis ne crée pas d'équivalence substantielle du niveau de protection »,*** et qu'il *« invite la Commission à poursuivre les négociations avec ses homologues américains (…)* » (§19).

Ce contexte ainsi brossé, ayant sans doute éclairé les rédacteurs (nous avons *supra* relevé le mécanisme inédit de décision d'adéquation conditionnelle), passons à l'évocation du *corpus* de la décision de juillet 2023, non sans souligner **frappant que les préventions ici exprimées, ne le soient que dans le corridor transatlantique** : le risque ne s'y limite pas. Il existe face à d'autres Etats dont les desseins stratégiques et le potentiel technologique mettent plus profondément et immédiatement en question notre conception des droits fondamentaux des personnes et de la souveraineté, *infra*.

B. UN CADRAGE TRES DETAILLE SUR LE REGIME DES INGERENCES ETATIQUES AMERICAINES

Nous serons d'autant plus court ici, que la décision est longue, en contraste des précédentes décisions d'adéquation cadrant le transfert euro-américain des données. Cette longueur n'a en effet cessé de croître, **du fait de l'importance des précisions et justifications appelées par** les contentieux successifs, par les avis critiques du CEPD, la pression du Parlement, la politisation du débat… et la probabilité d'un nouveau recours préjudiciel devant la CJUE [1081].

Ainsi, cette décision contient 4 articles (6 dans la décision *Privacy Shield,* mais sans différence significative de contenu), sur moins d'une page et demi. En revanche, elle contient en préalable 223 considérants (155 dans la décision *Privacy Shield*), lesquels occupent 60 pages, et s'achève avec 7 annexes qui occupent 73 pages. **L'avis du CEPD de mars 2023 et la résolution du Parlement européen de mai 2023 n'y sont pas rapportés** ; en contraste, la consultation du CEPD avait été rapportée dans la décision 2016/2050 *Privacy Shield*.

[1080] Ce point ne nous semble pas avoir sa place dans la délibération, étant hétérogène au problème de l'ordre juridique américain ; Soulignons qu'en 2019, le Tribunal de l'Union a certes ouvert une nouvelle voie de recours pour la protection des données personnelles, introduisant la possibilité qu'un particulier soit requérant ; **mais cela dans le contexte spécifique du règlement 2018/1275**, lequel ne traite que des données des personnes employées par les institutions de l'UE : Aff. T-903/16, 14 février 2019, ECLI: ECLI:EU:T:2019:96.

[1081] Nous venons de noter que le Parlement européen souhaiterait (résolution de mai 2023) une autre approche, par recours direct des personnes concernées devant une autre juridiction ; cela pourrait modifier profondément l'équilibre du système, et priver du filtre du recours préjudiciel fondé sur le doute de la juridiction nationale.

Les articles ne sont que des dispositions constatant l'approbation du cadre et organisant son entrée en vigueur. La substance du DPF est donc dans les considérants (1) et les annexes (2).

1. Sur les considérants de la décision d'adéquation du DPF / CPD

Nous ne développerons pas les considérants riches et précis sur le plan juridique/technique, **qui constatent l'évolution du droit fédéral américain dans le sens voulu.** Ils visent tant à l'étai juridique maximal d'une décision qui sera très scrutée ***(objet d'ailleurs d'un nouveau recours en septembre 2023 devant la CJUE)***, qu'à son explication didactique pour les « utilisateurs » citoyens, mais aussi et surtout les entreprises, dont leurs *Data protection Officers*. Cela suppose en effet une compréhension développée du contexte, compte tenu des changements d'environnement juridique que la décision a appelé aux Etats-Unis ; ils **peuvent y avoir des conséquences sur les organisations commerciales, non seulement sur les administrations gouvernementales**.

En effet, les considérants actent l'introduction en droit américain par l'EO 14086, des **principes de nécessité et de proportionnalité** de l'ingérence étatique dans les données personnelles sur le fondement de l'intérêt public.

Or, ancrée en droit européen, cette articulation était formellement inédite dans ce droit fédéral américain, de tradition beaucoup plus jurisprudentielle. De sa consécration résulte, non seulement l'obtention de la décision d'adéquation au plan européen, mais aussi potentiellement au plan américain, un **changement de paradigme aux conséquences systémiques,** alors que des réformes au niveau des Etats (fédérés) sont en cours.
Mais la publication de la décision complète en version définitive (juillet 2023) est à la date de notre rédaction encore trop récente, pour avoir donné lieu à des analyses substantielles à cet égard : en l'état, les réactions dominantes sont celles des avocats d'affaires, plus que des politologues internes (et la future campagne présidentielle occupe déjà tous les esprits) [1082].

[1082] Pour un aperçu de réactions à chaud, sans encore d'expression doctrinale approfondie, voir R.W. Del Selto, A.Spies, J. Guo, « How to Comply with the New EU-US Data Privacy Framework », 24 juillet 2023, sur https://www.morganlewis.com/pubs/2023/07/how-to-comply-with-the-new-eu-us-data-privacy-framework ; J. Sullivan, R. De Souza, H. Waem et al. « European Commission adopts new adequacy decision for EU-US data flows », 11 juillet 2023 DLA Piper, https://blogs.dlapiper.com/privacymatters/european-commission-adopts-new-adequacy-decision-for-eu-us-data-flows/ ; P. Church, « EU & US – The new EU-US Data Privacy Framework: Third time lucky ? » 17 juillet 2023, Linklaters, https://www.linklaters.com/en/insights/blogs/digilinks/2023/july/eu-and-us--the-new-eu-us-data-privacy-

Le point est que la **sélectivité d'une recherche d'information** (pour répondre aux critères de nécessité et proportionnalité) peut avoir pour conséquence, non souhaitable, d'informer implicitement son fournisseur. En outre, la question pourrait se poser de la compatibilité de ces principes, avec la pratique de la collecte massive de renseignement électronique, on l'a vu. Mais il n'est pas impossible que d'autres technologies, dont celles agiles d'« intelligence artificielle » fondées sur des capacités de calcul de puissance et vitesse exponentielle, soient capables d'une sélectivité alerte sans transfert de données, *infra*.

2. Sur les annexes de la décision d'adéquation du DPF / CPD

L'autre point notable, sur un plan méthodologique et politique, est la production en annexe de **lettres d'engagements officiels détaillés d'institutions américaines** pour les champs couverts [1083]. Elles sont transmises par la lettre du secrétaire d'Etat, *US Department of Commerce*, datée du 6 juillet 2023 (la veille donc, de la décision d'adéquation de la Commission; mais les lettres sont antérieures, leur contenu avait été négocié). Si ces lettres contiennent des dispositions techniques, la lettre de madame G. Raimondo [1084] est politique. Son évocation brève permettra de mettre en perspective le raisonnement qui précède :

Ainsi, « *On behalf of the United States, I am pleased to transmit herewith a package of EU-U.S. Data Privacy Framework materials that, combined with Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities" and 28 CFR part 201 amending Department of Justice regulations to establish the "Data Protection Review Court",* ***reflects important and detailed negotiations to strengthen privacy and civil liberties protections. These negotiations have resulted in new safeguards to ensure that U.S. signals intelligences activities are necessary and proportionate in the pursuit of defined national security objectives*** *and a new mechanism for European Union (« EU ») individuals to seek*

framework--third-time-lucky ; Deloitte, « Adequacy decision on the EU-US Data Privacy Framework » 25 juillet 2023, https://www2.deloitte.com/lu/en/pages/investment-management/articles/adequacy-decision-eu-us-data-privacy-framework.html ; etc.

[1083] Letter from the Department's International Trade Administration, (which administers the Data Privacy Framework program, describing the commitments that our Department has made to ensure that the EU-U.S. Data Privacy Framework operates effectively) ; Letter from the Federal Trade Commission (describing its enforcement of the Principles) ; Letter from the Department of Transportation (idem) ; Letter prepared by the Office of the Director of National Intelligence (regarding safeguards and limitations applicable to U.S. national security authorities) ; Letter prepared by the Department of Justice (regarding safeguards and limitations on U.S. Government access for law enforcement and public interest purposes).

[1084] Leader pour la partie américaine, de la négociation avec le commissaire européen D. Reynders

redress if they believe they are unlawfully targeted by signals intelligence activities, which together will ensure the privacy of EU personal data. The EU-U.S. Data Privacy Framework ***will underpin an inclusive and competitive digital economy****. We should both be proud of the improvements reflected in that Framework, which will enhance* ***the protection of privacy around the world*** ». Cette pétition est ambitieuse.

Publiées sur le site dédié du *Department's Data Privacy Framework* (lequel réunit deux cadres distincts de transfert de données : ceux avec l'Union, et avec la Suisse), ces lettres sont juridiquement consubstantielles au cadre DPF du transfert des données [1085]. Ainsi, elles valent **positionnements opposables, tel un « rescrit »** [1086], **aux administrations fédérales qui ont produit ces intentions précisées et détaillées**. Ceci est utile dans l'attente de leur transposition, quand requise, dans les procédures internes de leurs organes respectifs, *supra*.

Après ce riche retour d'expérience sur le plan méthodologique, de la renégociation européenne de garanties coordonnées dans le cadre institutionnel de transfert des données personnelles [1087], revenons à la question des données de santé.

§2. LES CONSEQUENCES DE L'AVENEMENT DU DPF DE 2023 POUR LES « DONNEES DE SANTE »

Nous avons vu en introduction de cette thèse, que la gouvernance des données personnelles à l'échelle mondiale était particulièrement sensible : **son étude en droit comparé a révélé de forts contrastes** [1088], mettant en exergue la question des infrastructures souveraines (serveurs) et capacités de traitement (par « intelligence artificielle »).
Le cadre de transfert doit ainsi prendre en compte la **singularité des données personnelles « de santé », qui n'ont à ce jour pas donné lieu à des accords dédiés**, puisqu'elles participent du régime protecteur globalisé des données de santé personnelles sensibles.

[1085] https://www.dataprivacyframework.gov/s/ contenant tous les éléments de pratique.
[1086] « acte administratif donné par écrit par une autorité dans son domaine de compétence propre, qui fournit une réponse à une question écrite ». A l'époque impériale romaine, les rescrits avaient une force exécutive. En France, on les trouve essentiellement en matière fiscale, pour sécuriser la relation administrés/administration par une position formelle opposable à l'administration.
[1087] Les autres décisions précitées d'adéquation en application de l'article 45 RGPD, ont suscité beaucoup moins de difficultés ; mais des révisions périodiques sont parfois en cours, et les examens intéressants, voir leur actualisation (notamment Japon et Corée).
[1088] Récemment, A. Bernier, F. Monar-Gabor, B.M. Knoppers, « The international data governance landscape », *Journal of Law and the Biosciences*, Volume 9, Issue 1, January-June 2022, lsac005.

Pour autant, nous avons vu, dans le cadre du *Safe Harbour* approuvé par la décision de la Commission 2000/520 EC, que parmi les « *Frequently Askeq Questions* » (FAQ), nombreuses étaient celles **portant spécifiquement sur les données de santé**, car elles jouent un rôle important dans la recherche scientifique, les stratégies industrielles et commerciales [1089].

En contraste, dans le cadre *Privacy Shield* approuvé par la décision de la Commission 2016/1250, le détail des questions et des réponses **ne relève plus de FAQ : il est formalisé dans l'annexe II,** titrée « *Principes du cadre «bouclier de protection des données UE-Etats-Unis» publiés par le ministère américain du commerce* ». L'ensemble est présenté au titre de « principes complémentaires », lesquels recouvrent les applications sectorielles [1090].

Nous allons voir ce qu'il en est dans le DPF approuvé par la décision C(2023) 4745 final [1091] en juillet 2023 (A), avant de relever quelques problématiques qui, sans participer directement du transfert, sont exacerbées par la massification du traitement qui peut en résulter (B).

A. APPORT DE LA DECISION D'ADEQUATION DU DPF EN MATIERE DE DONNEES DE SANTE

Dans la décision *Privacy Shield* de 2016, les données de santé avaient été traitées sous *l'item* « produits pharmaceutiques et médicaux ». Il y est alors souligné que les données issues d'études médicales ou pharmaceutiques (question posée sans précision quant à leur statut : interventionnel ou observationnel, « RIPH » ou non [1092]), le cas échéant rendues anonymes (FAQ14, R1), **sont susceptibles d'utilisation pour un autre usage par l'organisation vers laquelle elles ont été transférées** « *s'il a été prévu au départ une notification et un choix appropriés* » (FAQ14, R2). Cela caractérise un enjeu lancinant, et très discuté.

Ainsi, dans la décision d'adéquation du DPF en juillet 2023, la place des données de santé est *quasi* identique à celle tenue dans la décision *Privacy Shield*, **quoiqu'avec une emphase nouvelle sur le consentement** (1). Cela n'apparaît pas de nature à satisfaire les acteurs qui s'étaient inquiétés de l'impact de l'arrêt « Schrems II » sur le transfert des données de santé, et/ou qui **proposaient une approche d'inspiration américaine plutôt qu'européenne** (2).

[1089] Réponses regroupées sous la FAQ n°14 « *Produits pharmaceutiques et médicaux* ».
[1090] Le développement n'est plus sous forme de FAQ, mais rédigé en distinguant « *b) recherche scientifique future ; c) retrait d'un essai clinique ; transfert à des fins de réglementation et de contrôle ; e) études masquées* (aveugles) *; f) contrôle de la sécurité et de l'efficacité du produit ; g) données codées ».*
[1091] Le système de référencement n'est pas homogène, car la nomenclature des décisions exécutives a changé.
[1092] Ce sont là surtout des catégories du droit français, dont l'utilité est discutée, cf. Ière partie de la thèse.

1. Les dispositions particulières de 2023 sur les « données personnelles de santé »

Dans la décision de 2023 relative au DPF EU-US [1093], les « données de santé » tiennent-elles une place particulière ? Comme dans les cadres précédents de transferts, et dans les mêmes termes, le considérant § 2.2.2 qui présente les « données sensibles » met en exergue l'exigence de garanties spécifiques, pour des catégories particulières de données.

Or, de façon emblématique, la liste des « informations sensibles » **donne pour premier exemple les données personnelles précisant un état médical ou de santé** (« *personal data specifying medical or health conditions* »), avant donc la question des origines raciales ou ethniques (exigences qui sont propres au droit européen [1094]), les opinions politiques, religieuses ou philosophiques, l'appartenance syndicale, les préférences sexuelles « *or any other information received from a third party that is identified and treated by that party as sensitive* » [1095].
C'est dire, selon les termes de la décision (considérant §17), que **toute information qui serait considérée sensible selon le RGPD, sera traitée comme telle par les organisations américaines** parties au cadre [1096], ce qui re-soulève la question de l'extension conceptuelle de la « donnée de santé », objet de la première partie de notre thèse.

Dans ce contexte général du DPF, l'item « produits pharmaceutiques et médicaux » est à nouveau développé (sous un même n° 14, et avec le même contenu que dans le *Privacy Shield,* sans donc de développements depuis) *:* « *b) recherche scientifique future ; c) retrait d'un essai clinique ; transfert à des fins de réglementation et de contrôle ; e) études masquées* (aveugles) *; f) contrôle de la sécurité et de l'efficacité du produit ; g) données codées ».*

[1093] Référencée C(2023) 4745 final. Le système de référencement n'est pas homogène, car la nomenclature des décisions exécutives a changé.
[1094] Les données quant à l'origine ethnique ou raciale sont on l'a vu, largement rapportées et traitées parmi les données non sensibles, voire qui doivent être ostensibles, en droit américain ; ceci au point de donner lieu à des questionnements qui en Europe peuvent apparaître surréalistes : H. Schmidt, L.O. Gostin, M. A. Williams, « The Supreme Court's Rulings on Race Neutrality Threaten Progress in Medicine and Health », JAMA 10 juill. 2023 (seulement en ligne à la date de cette rédaction, doi:10.1001/jama.2023.13749).
[1095] Annexe I, section II, 2.c. de la décision de 2023.
[1096] Le §17 de spécifier que les données sensibles au sens du RGPD « *incluent les données sur l'orientation sexuelle, les données génétiques et biométriques* », ce qui semblait aller de soi mais est souligné ici.

Mais le texte n'est pas seulement remonté dans l'annexe I énonçant les principes, où il figure parmi les « principes supplémentaires » [1097] : le **corps même du considérant 27 de la section « *Transparency* »** fait référence à l'enjeu propre à la santé : ce dernier renvoi en effet, en bas de page, à l'annexe I pour des dispositions particulières au traitement des données dans le contexte de la recherche en santé et des essais cliniques, **avec donc une emphase sur la portée du consentement des personnes**. Alors même qu'il ne s'agit que d'une note de bas de page, attachée à un considérant, deux points sont ainsi spécialement développés.

* Le premier, qui n'a rien d'original, est l'hypothèse **de la réutilisation des données transférées pour un but de « recherche en santé »** (sans plus de précision [1098], mais elle doit être spécifiée en pratique). La personne est censée en être informée, et consentir, en amont : « *(...) Similarly, where an EU-U.S. DPF organisation receives personal data for health research purposes, it may only use it for a new research activity in accordance with the Notice and Choice principles. In this case, the notice to the individual* ***should in principle provide information about any future specific uses of the data (e.g. related studies)*** *».*

* Le second est l'hypothèse d'usages non déterminés à l'avance, notamment *« **Where it is not possible to include from the outset all future uses of the data** (because a new research use could arise from new insights or medical/research developments),* ***an explanation that the data may be used in future unanticipated medical and pharmaceutical research activities must be included.*** *If such further use* ***is not consistent with the general research purposes for which the data was collected*** *(i.e. if the new purposes are materially different,* ***but still compatible with*** *the original purpose, see recitals14-15), new consent (i.e. opt-in) needs to be obtained (...) ».*

Cette disposition aussi est classique. Mais, à nouveau, le point intéressant est qu'elle soit mise spécialement en exergue, de manière à ce que sa lecture ne nécessite pas l'analyse de la décision complète, particulièrement longue, ni de ses annexes.

Il restera à voir **le respect (et la sanction) en pratique, de l'obligation de recueil d'un consentement additionnel** pour une étude « en santé » (qu'est-ce que cela signifie, compte tenu de l'extension conceptuelle de la notion de « santé » ?) ; laquelle n'aurait, pas hypothèse, pas été spécifiée lors de la collecte pour le but initial, ni « anticipable », et ses conséquences.

[1097] Section II.1.b. Supplemental Principle 14 et Annex I, Section III.14

[1098] Ce qui remet en exergue, à nouveau, le champ de la « recherche » dans le domaine de la « santé ».

Rappelons que, si les « données de santé » peuvent être vendues aux Etats-Unis, tel n'est pas le cas en Europe. De fait, **elles en proviennent gratuitement pour stockage et traitement**…

2. Après l'arrêt « Shrems II », inquiétudes et frustrations quant aux données de santé

L'enjeu du transfert de ces données dans le cadre *Privacy Shield,* a donné lieu à d'abondantes réflexions du côté américain. Parmi les synthèses doctrinales, que l'on retiendra seules ici pour éviter une technicité excessive, on peut distinguer la visée rétrospective, ou prospective.

* Quelques articles se sont intéressés à la question d'un point de vue que **l'on pourrait qualifier de rétrospectif :** ils s'interrogent sur l'état du droit tel qu'applicable suite à l'arrêt « Schrems II », quant à l'avenir du transfert transatlantique des données personnelles de santé.

Le premier significatif appelle à « *démystifier* » l'impact de cette jurisprudence [1099] : il met en exergue des mesures contractuelles et techniques de contournement, dont la pseudonymisation des données, l'encryptage complet, le certificat de confidentialité, etc. Toutes ces techniques peuvent s'inscrire dans les « clauses types », qui n'ont pas été invalidées par l'arrêt Schrems II, *supra*. Pour autant, les auteurs notent que ces alternatives ne sont pas à l'abri de l'ingérence étatique sur le fondement du droit fédéral [1100]. Dès lors, la survivance ou l'adoption de ces clauses n'offre qu'une protection limitée.

Dans ce contexte, comme dans celui des clauses type [1101] qui, étant autonomes, demeurent applicables [1102], notons le **statut particulier de la pseudonymisation** des données.

Selon le Contrôleur européen des données, elle n'est concevable que « *if (i) the key to that data is 'held exclusively by the data exporter and kept separately in a Member State' or a third country with an adequacy decision and (ii) public authorities cannot use other information to re-identify the data* » [1103].

[1099] J. Liss, D. Peloquin, M. Barnes, B.E. Bierer préc., « Demystifying *Schrems II* for the cross-border transfer of clinical research data », *Journal of Law and the Biosciences*, Volume 8, Issue 2, July-December 2021, lsab032.
[1100] Ibid., page 11, « IV. Strategies facilitating data transfert ».
[1101] Dans la dernière version (actualisant celle de 2010), voir décision 2021/914 de la Commission du 4 juin 2021relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil.
[1102] L. Bradford, M. Aboy, K. Liddell préc., « Standard contractual clauses for cross-border transfers of health data after *Schrems II* », *Journal of Law and the Biosciences*, Volume 8, Issue 1, January-June 2021, lsab007.
[1103] EDPB, SCC Recommendations, Annex 2(80), at 23 (SCC dans la version 2021).

C'est pourquoi la question des codes est, nous l'avons vu, traitée dans tous les cadres successifs adoptés, dès la première décision d'adéquation *Safe Harbour* en 2000, **bien que le transfert de données pseudonymisées codées ne constitue pas un transfert de données personnelles soumis au *Safe Harbour*** [1104].

Or, cette position est depuis constante, alors que nous avons vu que, si la donnée « anonymisée » **n'était pas considérée comme une donnée personnelle dans le RGPD, tel n'était pas le cas de la donnée « pseudonymisée ».** Rappelons que le CEPD a souligné que « *in many situations, factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of a natural person (…) may allow the identification of that person' even without 'plain identifiers'* » [1105], pointant ainsi les risques de réidentification, *supra*.

***** Dans ce sillage, un article s'est intéressé **d'un point de vue prospectif, à la possibilité d'élaborer un droit qui serait plus pertinent en matière de santé** [1106]. En début 2020, avant donc que la CJUE rende son arrêt « Schrems II », ces auteurs (les mêmes que celui de l'article de 2021 sur les clauses contractuelles « après Schrems II » [1107]), considèrent que le cadre tracé par le *Privacy Shield* n'était pas adapté aux études de santé complexes, et que ses termes étaient trop restrictifs pour la variété d'échanges de données sous-tendant les activités de recherche, de traitement et de soin.
Nous n'entrerons pas dans le détail de cette intéressante étude, notamment quant à sa perception du *Privacy Shield* pour les organisations américaines.

De façon très entreprenante, ses auteurs proposent en conclusion que « *the USA seek an additional sector-based adequacy determination* ***based on the existing US health privacy law, the Health Insurance Portability and Accountability Act*** », c'est-à-dire selon le standard américain. Ils considèrent qu'une telle approche sectorielle spécifique à la santé, pourrait éviter « *many of the most contentious issues that divide the USA and EU on data protection* » [1108], et pourrait servir de modèle international pour faciliter l'harmonisation des pratiques de recherche en santé.

[1104] Réponse à Q7 sous la FAQ14 préc., voir JOCE 25 août 2000, page L. 215/25.
[1105] EDPB, SCC Recommendations, Annex 2(81), at 23–24 ; EDPB, « What is considered personal data under the EU GDPR ? », site EDPB, contrôlé juill. 2023.
[1106] L. Bradford, M. Aboy, K. Liddell, « International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection », *Journal of Law and the Biosciences*, Volume 7, Issue 1, January-June 2020, lsaa055.
[1107] Leur article a certes été publié en octobre 2020, mais a été disponible en ligne dès le premier semestre.
[1108] En fait, il y a pas vraiment de contentieux : nombre de contrats ne peuvent être conclu, les auteurs le rapportent eux-mêmes…

Ainsi, les auteurs proposent un « *HIPAA Shield* », dont ils examinent l'adéquation au regard du RGPD [1109]. Cette question sort de notre champ de recherche ; mais l'extension internationale d'une réglementation sectorielle restrictive, comme l'est l'HIPAA [1110], apparaît d'autant moins probable, que son extension nationale aux « entités non couvertes » **est précisément en cours d'examen par les institutions fédérales mêmes** [1111].

En outre et surtout, nous avons relevé que, non seulement le cadre DPF de 2023 **avait repris presque à l'identique les dispositions** du cadre *Privacy Shield* de 2016, qu'il avait même mises en exergue ; mais que, de surcroît, nombre d'acteurs (privés et publics) américains, et dès 2018 le *Council on Foreign relations*, **étaient désormais intéressés par une approche globale de type RGPD aux Etats-Unis**, plutôt que par une fragmentation sectorielle [1112].

B. DES QUESTIONS EN SUSPENS : DU BON USAGE DES DONNEES DE SANTE TRANSFEREES ?

S'il semble possible de considérer que le DPF approuvé en 2023 **constitue un cadre minimal pour le transfert de données de santé**, les auteurs précités n'en soulèvent pas moins une question intéressante : cet accord possède en effet un champ très général, et ne possède de dispositions spécifiques que sur les « *produits pharmaceutiques et médicaux* » (*supra*).

Mais il nous semble que ce champ est précisable par des clauses type dédiées, sur un support donc souple et adapté (sous réserve de la distinction validation requise / ou non par les autorités nationales de contrôle, *supra*). On ne peut alors exclure une approche plus spécifique des données de santé en économie globalisée.
Ainsi, **sur la base de cette recherche de garanties coordonnées,** semble pouvoir **émerger d'un droit international, sinon de la donnée de santé, du moins de son transfert**, mais qui ne saurait déroger au standard européen.

[1109] Sur la notion d'HIPAA, et sur les « entités couvertes », *supra* P1T1C1.
[1110] Lequel ne couvre que certaines entités, HIPAA § 262(a) « Any standard adopted under this part shall apply, in whole or in part, to the following persons: '(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction referred to in section 1173(a)(1) ».
[1111] U.S. Department of Health and Human Services, « Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA » (non daté, mais datable 2016).
[1112] CFR, « Reforming the U.S. Approach to Data Protection and Privacy », 30 janv. 2018, site du CFR ; dernièrement, S. Nayyar, « Is It Time For A U.S. Version Of GDPR ? » Forbes, 1er févr. 2022.

Nous proposons maintenant d'explorer les conséquences lorsque, sur une base juridique agréée (décision d'adéquation et/ou clauses contractuelles type), sont établis des flux de données de santé personnelles. **La légalité *a priori* de leur transfert international n'en pourrait pas moins donner lieu à des applications illicites à conséquences systémiques, que l'on ne fera ici qu'esquisser** (rappelons le but méthodologique de notre approche).

Le premier cas de figure est celui de la **domination technologique dans le traitement des données**. Sanctionné en droit de la concurrence, l'« *abus de position dominante* » consiste sur le marché en une exploitation délictueuse de sa position par le détenteur des données, ou en l'exclusion de ses compétiteurs (1).
L'**exploitation technologique de la porosité potentielle des catégories de données** met en cause, non en soi le droit de la concurrence, mais l'application du RGPD ; cette pratique relève d'une qualification en cours de réflexion (2).

1. Cas de la domination technologique dans le traitement des données de santé

Le droit européen comporte de vastes pans dédiés à la régulation de la concurrence, au gré de la transformation voire de l'apparition de nouveaux marchés. L'abus de position dominante y est visé par l'article 102 TFUE : « *est incompatible avec le marché intérieur et interdit, **dans la mesure où le commerce entre États membres est susceptible d'en être affecté,** le fait pour une ou plusieurs entreprises d'exploiter de façon abusive une position dominante sur le marché intérieur ou dans une partie substantielle de celui-ci (...)* » ; de même en droit français à son échelle (c'est-à-dire si même seul, le marché français était affecté), par l'article L. 420-2 du Code de commerce [1113].

La « position dominante » n'est définie que par la jurisprudence [1114], au regard d'un marché déterminé (« marché pertinent ») : ce dernier est caractérisé par l'absence d'alternative pour les produits ou services qui y sont en lice [1115].

[1113] D'une façon générale, voir C. Prieto, Abus de position dominante – Notion d'abus en droit communautaire, Fasc. 561 in JCl. Concurrence Consommation, 2018 ; N. Petit, L'abus, in Droit européen de la concurrence – Chapitre IV – Section III, Lextenso, 2020 ; P.L. Parcu, G. Monti, M. Botta, *Abuse of Dominance in EU Competition Law : Emerging Trends*, Edward Elgar Publishing, 2017 ; P. Akman, *The concept of abuse in EU competition law*, Hart Publishing, 2012.
[1114] CJUE Aff. 27/76 du 14 février 1978, United Brands et United Brands Continental BV/Commission, §65 : « *la position dominante concerne une position de puissance économique détenue par une entreprise **qui lui donne le pouvoir de faire obstacle au maintien d'une concurrence effective** sur le marché en cause, en lui fournissant la possibilité de comportements indépendants dans une mesure appréciable vis à vis de ses concurrents, de ses clients et, finalement, des consommateurs* ».

La position doit donner lieu à une exploitation « abusive », dans le but ou avec l'effet [1116], même potentiel, de restreindre la concurrence sur ce marché [1117]. **En matière d'information, est ainsi constitué l'abus de position dominante par rétention et utilisation d'information,** *« dans la mesure où la communication de ces informations par la société (X) à ses concurrents éventuels* ***était l'unique moyen d'ouvrir ce marché,*** *tout refus de sa part de les transmettre, fussent-elles couvertes par le secret des affaires, aurait constitué une exploitation abusive de sa position dominante »* [1118].

Très exposé aux risques de position dominante, et de leur abus du fait de ses caractéristiques de concentration et d'affinement continu de l'information qui y est capturée et valorisée [1119], le marché numérique vient de faire l'objet d'une réglementation dédiée en septembre 2022 (règlement 2022/1295 sur le marché numérique [1120]), et sa régulation spécifique est une priorité nationale [1121] ; à ces défis, s'ajoutent les possibilités élargies d'autant, de manipulation des comportements de marché [1122]. Mais seule la question de **l'abus de position dominante en matière de données de santé** nous intéresse ici. Nous proposons de distinguer selon que la position dominante est acquise par dessein, ou par défaut.

En matière de données de santé anonymisées, **la position dominante par dessein est improbable en Europe,** du fait nous l'avons vu, en matière de couverture des soins de base, de la prédominance de systèmes publics ou d'assurances obligatoires, donc de la vocation des données primaires à rejoindre des bases de données généralement soumises au droit public

---

[1115] CA Paris, 9 mars 2022, nº 19/19747, soit le « *lieu sur lequel se confrontent l'offre et la demande de produits ou de services qui sont considérés par les acheteurs comme substituables entre eux mais non substituables aux autres biens ou services offerts* ».

[1116] CJUE Aff. C-459/10 P du 19 avril 2012, Tomra, § 68 et 79 « *pour établir une violation de l'article 102 TFUE, il n'est pas nécessaire de démontrer que le comportement abusif de l'entreprise en position dominante a eu un effet anticoncurrentiel concret sur les marchés concernés, mais seulement qu'il tend à restreindre la concurrence ou qu'il est de nature à ou susceptible d'avoir un tel effet* ».

[1117] CJUE Aff. C-52/09 du 17 février 2011, TeliaSonera Sverige, Rec. 2011 p. I-527, § 64 *« Afin d'établir le caractère abusif d'une pratique d'éviction, l'effet anticoncurrentiel de celle-ci sur le marché doit exister, mais il ne doit pas être nécessairement concret, étant suffisante la démonstration d'un effet anticoncurrentiel potentiel de nature à évincer les concurrents au moins aussi efficaces que l'entreprise en position dominante ».*

[1118] CA Paris, 12 octobre 2017, n°15/14038.

[1119] Aux critères classiques de volume, vélocité et variété des données, la doctrine a adjoint les critères de valeur, véracité et variabilité, pour rendre compte de ce phénomène, voir N. Verlhiac, « Les six V du Big Data : exploitez pleinement votre base de données », blog 1er juin 2021, accessible sur Ostraca.fr.

[1120] Règlement (UE) 2022/1925 du Parlement et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques).

[1121] Le marché numérique est le premier abordé, in Feuille de route 2023-2024, Autorité de la concurrence.

[1122] N. de Macellis-Wartin, F. Marty, E. Thelisson, T. Warin, « Intelligence artificielle et manipulations des comportements de marché : l'évaluation *ex ante* dans l'arsenal du régulateur », Rev. Int. Dr. éco. 2020/2 (t. XXXIV), pp 203 - 245.

[1123]. Cela contraste avec des inquiétudes manifestées aux Etats-Unis, sur fond de compétition féroce entre des opérateurs mus par des paradigmes différents : certains s'inquiètent qu'Apple, au nom notamment de la protection de la vie privée, draine des données au sein de / au profit de son propre écosystème protégé de services, dont la performance ne cesse de croître [1124] ; en contraste de compétiteurs qui, ne revendiquant pas une telle protection (du fait d'un modèle économique différent), sont privés des avantages de son nouvel attrait [1125].

Sur le marché des données hors « santé », des procédures ont abouti, qui sanctionnent une telle infraction : ainsi en 2019 résultant du croisement de données à l'insu des utilisateurs des réseaux sociaux [1126], en 2022 résultant de l'utilisation de données de clients sur le marché de l'énergie [1127].
En matière de santé, une enquête est en 2021 en cours en France sur la « quasi hégémonie » de la société Doctolib sur le marché de la prise de rendez-vous médicaux [1128]. Dès ici, notons qu'il **peut découler d'une telle position, que des données de santé puissent être inférées** de la connaissance du champ, de la structure et fréquence des besoins des patients etc. Ainsi, une même situation pourrait **faire naître des infractions distinctes,** *infra*.

Il n'est pas lieu ici de passer en revue dans le règlement n° 2022/1295 sur le marché numérique, les pratiques de la part d'entreprises « contrôleurs d'accès » [1129] considérées comme déloyales (cf. le Chapitre III dédié), ce dont résulte pour eux l'obligation de les éviter.

[1123] Rappelons que ce contexte pourrait expliquer, dans le rapport du Conseil d'Etat de 2017, la notion de donnée publique de santé, par attraction sur les bases du SNDS, *supra* Partie I.
[1124] Nous avons vu *supra* que l' « application santé » drainait des données bien au-delà de la qualification organique des données de santé, Partie 1 titre 2.
[1125] O. Sadare, T. Melvin, H. Harvey *et al.* « Can Apple and Google continue as health app gatekeepers as well as distributors and developers? » *Nature Digit. Med.* 6, 8 (2023), publié en janvier 2023 ; N. Shah, « Thriving Apple Watch & Apple Health Ecosystem Advancing Digital Intelligent Healthcare », 21 juillet 2022, Blog, sur le site counterpoint, vérifié janv. 2023 ; Apple (communication d'entreprise), Health Report 2022, « Empowering people to live a healthier dayInnovation using Apple technology to support personal health, research, and care July 2022 (updated in September 2022).
[1126] Décision B6-22/16 du 15 fév 2022, « Bundeskartellamt prohibits Facebook from combining user data from different sources », accessible sur le site bundelskartellamt.de.
[1127] Décision 22-D-06 du 22 février 2022 « relative à des pratiques mises en oeuvre par la société EDF dans le secteur de l'électricité », accessible sur le site de l'Autorité.
[1128] Deux enquêtes sont en cours dont l'une suite à une plainte, mais aucune procédure n'est référencée en l'état (mai 2023) sur le site de l'Autorité de la concurrence. Voir « L'autorité de la concurrence enquête sur Doctolib », Le Figaro 7 juill. 2021.
[1129] Selon l'article 2 du règlement, « *une entreprise fournissant des services de plateforme essentiels, désignée conformément à l'article 3* », lequel désigne comme tel (article 3§1) une entreprise notamment quant « *a) elle a un poids important sur le marché intérieur ;b)elle fournit un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux; etc)elle jouit d'une position solide et durable, dans ses activités, ou jouira, selon toute probabilité, d'une telle position dans un avenir proche (...) ».*

Ces obligations peuvent néanmoins faire l'objet d'une « exemption pour raisons de santé publique et de sécurité publique » (article 10). Ainsi la Commission européenne peut-elle, à son initiative ou sur demande de l'entreprise concernée, adopter un acte d'exécution motivé qui exempte cette dernière de plusieurs obligations, à titre ou pourrait dire d'un « droit commun » (10§1), du fait qu'une situation d'urgence a été *a contrario* définie (10§4).

* L'exemption pour motif de santé publique peut nuancer l'obligation de l'article 5, selon lequel le contrôleur d'accès ne doit pas (à moins du consentement éclairé de l'utilisateur final des services essentiels) « *a) traiter, aux fins de la fourniture de services de publicité en ligne, les données à caractère personnel des utilisateurs finaux qui recourent à des services de tiers utilisant des services de plateforme essentiels fournis par le contrôleur d'accès; b)* ***combiner les données à caractère personnel provenant du service de plateforme essentiel concerné avec les données à caractère personnel provenant de tout autre service de plateforme essentiel ou de tout autre service fourni par le contrôleur d'accès, ni avec des données à caractère personnel provenant de services tiers*** *;c)utiliser de manière croisée les données à caractère personnel provenant du service de plateforme essentiel concerné dans le cadre d'autres services fournis séparément par le contrôleur d'accès, y compris d'autres services de plateforme essentiels, et inversement;* ***d)inscrire les utilisateurs finaux à d'autres services du contrôleur d'accès dans le but de combiner des données à caractère personnel*** ».

* En outre, l'exemption pour motif de santé publique peut nuancer l'obligation de l'article 6, dont le §2 dispose notamment que « *Le contrôleur d'accès n'utilise pas,* ***en concurrence avec les entreprises utilisatrices, les données, quelles qu'elles soient, qui ne sont pas accessibles au public, qui sont générées ou fournies par*** *ces entreprises utilisatrices dans le cadre de leur utilisation des services de plateforme essentiels concernés ou des services fournis conjointement aux services de plateforme essentiels concernés, ou à l'appui de ceux-ci, y compris les données générées ou fournies par les clients de ces entreprises utilisatrices (…) les données qui ne sont pas accessibles au public comprennent* ***toutes les données agrégées et non agrégées générées*** *par les entreprises utilisatrices* ***qui peuvent être déduites ou collectées au travers des activités commerciales de ces entreprises ou de leurs clients, y compris les données concernant les clics, les recherches, les vues et la voix,*** *dans le cadre des services de plateforme essentiels concernés ou de services fournis conjointement aux services de plateforme essentiels concernés du contrôleur d'accès, ou à leur appui.*

* Enfin, l'exemption pour motif de santé publique peut enfin l'article 7 « *Obligations incombant aux contrôleurs d'accès concernant l'interopérabilité des services de communications interpersonnelles non fondés sur la numérotation* ». Son contenu essentiellement technique invite le lecteur à s'y reporter directement, car nous ne le reproduirons pas ici : l'enjeu est en effet l'interopérabilité, entre fournisseurs de prestations, de services de communications interpersonnelles non fondés sur la numérotation.

Nous ne développerons pas plus allant : l'activation en urgence de ces systèmes d'exemption prévus par le règlement de 2022 postule un contexte de **crise forte appelant potentiellement la jonction de capacités publiques et privées.** Les « contrôleurs d'accès » pourraient y jouer un rôle fondamental, pour une gouvernance résiliente nationale, voire européenne [1130].

Ainsi la position dominante n'est pas nécessairement sanctionnée, si l'activation de l'article 10§1 rend judicieux (dans ce contexte précis) les combinaisons et usages croisés etc.

Curieusement, l'article 10 ne cite pas la condition d'absence d'alternative ; sans doute cela est-il implicite, l'article 10§2 prévoyant le réexamen de la décision « ***quand le motif de l'exemption n'existe plus*** *ou au minimum chaque année* ». On peut imaginer qu'une éventuelle mise en œuvre fera l'objet d'une forte surveillance.

L'anticipation de crises (qui n'est pas l'objet direct de notre recherche) **commande un développement suffisamment varié** des acteurs du numérique, pour qu'un tel scénario « par défaut » ne perdure pas. L'accumulation de données par ce biais est en effet source d'enrichissement continu des algorithmes, donc d'accumulation continue de capacité [1131] ; et, à l'ère de l'IA, on peut l'imaginer (sous les réserves précitées), une concentration exponentielle de puissance [1132], donc un **confortement continu de monopoles d'impact supranational**.

[1130] Sous réserve du chapitre II *infra*.
[1131] M. Mason, « Emergent Medical Data: Health Information Inferred by Artificial Intelligence » - 11 UC Irvine L. Rev. 995, mai 2021.
[1132] M. Mason, C.E. Haupt, « AI Chatbots, Health Privacy, and Challenges to HIPAA Compliance » JAMA 2023, 6 juill. doi:10.1001/jama.2023.9458. Auparavant, M. Mason, « Biosupremacy: Big Data, Antitrust, and Monopolistic Power Over Human Behavior », UC Davis Law Review 513, juin 2021.

Hors des situations d'exemption, notons seulement qu'une décision rendue en juillet 2023 par la CJUE vient de consacrer la compétence des autorités nationales au carrefour du droit de la concurrence et du RGPD. Le contentieux opposait l'autorité de la concurrence allemande à Meta (anciennement Facebook) et Facebook Deutschland GmbH [1133].

En l'occurrence, il s'agit d'un abus de position dominante, consistant en le traitement de données à caractère personnel des utilisateurs tel que prévu dans les conditions contractuelles générales du réseau social (infraction formalisée, donc) : **la CJUE juge que l'autorité de la concurrence d'un État membre est compétente pour constater la non conformité de ce traitement au règlement (UE) 2016/679** : il s'agit, pour le futur, d'un gain significatif d'efficience procédurale.

2. Cas de la porosité des catégories : le risque de ré-identification des données ?

Le sujet étant plus technique que juridique, nous développerons peu. Il est notoire que l'accumulation et le croisement des données non personnelles, outre qu'ils en accroissent la valeur par potentialisation affinée, peuvent conduire à une ré-identification de personnes dont les données étaient pseudonymisées, voire anonymisées. **Le processus d'anonymisation n'est donc pas nécessairement « irréversible »,** ce qui est censé le qualifier.

Nous avons souligné qu'en droit européen, il n'existait pas de définition de la donnée « anonyme ». Cette donnée échappe expressément au champ du RGPD, car elle n'est par définition pas « personnelle » ; pas plus, elle ne constitue une catégorie juridique : elle n'est évoquée que de façon incidente dans les considérants des règlements. Elle ne présente qu'un occurrence en 2016 dans le RGPD [1134] ; idem dans le règlement (UE) 2022/1295 sur le marché numérique, lequel seul **la définit par l'irréversibilité** [1135]. Or, dès 2014, le « groupe de travail de l'article 29 » (CEPD) avait formulé des mises en garde à ce sujet [1136].

[1133] CJUE 4 juillet 2023, Metaplatform vs. Bundeskartellamt, affaire C-252/21, sur demande préjudicielle, ECLI:EU:C:2023:537

[1134] La notion n'est présente que dans son seul considérant n°26, lequel en contraste des définitions qui suivront, **ne met pas en exergue le caractère irréversible :** « (…) *il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable.* »

[1135] Son considérant n° 61 dispose que « ***Les données concernées sont anonymisées si les données à caractères personnel sont irréversiblement modifiées de façon à ce que*** *les informations ne soient plus liées à une personne physique identifiée ou identifiable, ou si les données à caractère personnel sont rendues anonymes de telle manière que la personne concernée n'est pas ou n'est plus identifiable* ».

[1136] Avis 05/2014 sur les Techniques d'anonymisation, 0829/14/FR/WP216.

En revanche, la notion de « pseudonymisation », processus qui aboutit à ce qu'une donnée reste personnelle, quoique la personne concernée **cesse en théorie d'être identifiable et donc échappe au DPF de 2023, nous l'avons vu,** y est définie. Elle y présente de nombreuses occurrences [1137], et l'adoption du RGPD a aussitôt soulevé des questionnements.

***** Il est ainsi **difficile en matière d'anonymisation, de définir une obligation juridique de résultat technique,** laquelle doit être balancée, pour le « contrôleur d'accès », avec la sauvegarde de l'utilité des données qu'il communique [1138] : on peut imaginer comment, malgré l'obligation de l'article 6 du règlement n° 2022/1925, il serait possible à une entreprise en situation de position dominante (*supra*), de ne communiquer **que des informations de valeur résiduelle à ses compétiteurs**, **sous prétexte de protection des données personnelles qu'elle détient** : en théorie, il suffirait de créer une entité juridiquement distincte bénéficiant de contrats privilégiés (car à moindre dégradation des données sous couvert de protection), ce qui n'est pas moins exposé à une requalification jurisprudentielle de l'unité de groupe.
Mais ce problème d'application du droit de la concurrence sort de notre champ de recherche.

Dans le champ biomédical (emblématique, du fait de sa sensibilité), des auteurs ont relevé la difficulté à définir le terme « identification » : **cette définition présuppose l'existence de caractéristiques identifiantes, et conduit donc à un raisonnement circulaire.** L'examen des notions montre ainsi qu'un chemin reste à parcourir pour une bonne compréhension entre techniciens et juristes [1139]… Qu'en est-il en attendant, en droit ?

[1137] Pour rappel, l'article 4§5 entend par ce terme, « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* »;
[1138] Ibid. : « *un contrôleur d'accès* ***devrait garantir la protection des données*** *à caractère personnel des utilisateurs finaux, notamment contre les risques de réidentification,* ***par des moyens adéquats,*** *par exemple l'anonymisation des données à caractère personnel,* ***sans altérer considérablement la qualité ou l'utilité des données*** », également *supra*.
[1139] M. Sariyar, I. Schlünder, « Reconsidering Anonymization-Related Concepts and the Term "Identification" Against the Backdrop of the European Legal Framework », Biopreserv Biobank 2016 oct. ; 14(5): 367–374.

Les tentatives illicites de réidentification de données protégées sont immémoriales, mais d'une acuité contemporaine particulière du fait de leur production et des progrès de leur traitement. Elles sont devenues de plus en plus fréquentes pour les données de santé [1140], leur développement commercial dans certains pays ouvrant aussi des opportunités croissantes [1141].

Dès lors, les risques correspondant donnent lieu à une recherche continue sur les méthodes de prévention en cas de partage de données issues des dossiers de patients notamment [1142], et sur les méthodes visant l'évaluation de tels risques, **pour proportionner les besoins de modification des données,** notamment dans l'hypothèse dans laquelle l'attaquant connaîtrait des caractéristiques « identifiantes » [1143].

* En matière biomédicale, il en résulte une science en développement continu : celle des méthodes de désidentification des données [1144] qui ne permettrait pas moins d'en conserver la valeur, laquelle ne pouvant se concevoir que **selon les champs disciplinaires et usages** [1145].

Cela recoupe le problème précité, soulevé par le considérant n° 61 du règlement (UE) 2022/1925 : « *(...) un contrôleur d'accès devrait garantir la protection des données à caractère personnel des utilisateurs finaux,* ***notamment contre les risques de réidentification,*** *par des moyens adéquats, par exemple l'anonymisation des* données à caractère personnel, sans altérer considérablement la qualité ou l'utilité des données ».

[1140] Déjà, voir K . El Emam, E. Jonker, L. Arbuckle, B. Malin, « A systematic review of re-identification attacks on health data » PlusOne, 2011;6(12):e28071 ; avec erratum : « Correction: a systematic review of re-identification attacks on health data » PlosOne 2015 Apr 16;10(4):e0126772. ; auparavant, B. Malin, « A computational model to protect patient data from location-based re-identification », Artif Intell Med 2007 Jul;40(3):223-39, doi: 10.1016/j.artmed.2007.04.002.

[1141] I.R. Alberto, N.R. Alberto, A.L. Ghosh, B. Jain et al. « The impact of commercial health datasets on medical research and health-care algorithms ». Lancet Digit Health. 2023 May;5(5):e288-e294 ;

[1142] G.E. Simon, S.M. Shortreed, R.Y. Cloey et al. « Assessing and Minimizing Re-identification Risk in Research Data Derived from Health Care »n, EGMS (Wash.DC) 2019 Mar 29;7(1):6.

[1143] W. Xia, Y. Liu, Z. Wan, Y. Vorobeychic et al., « Enabling realistic health data re-identification risk assessment through adversarial modeling », J Am Med Inform Assoc 2021, Mar 18;28(4):744-752.

[1144] R.N. Cardinal, A. Moore, M. Burchell, J.R. Lewis, « De-identified Bayesian personal identity matching for privacy-preserving record linkage despite errors: development and validation », BMC Med Inform Decis Mak. 2023 May 5;23(1):85. R. Chevrier, V. Foufi, C. Gaudet-Blavignac, A. Robert, C. Lovis, « Use and Understanding of Anonymization and De-Identification in the Biomedical Literature: Scoping Review ». J Med Internet Res. 2019 May 31;21(5):e13484 ; non encore agréé par comité de lecture (à la date de notre rédaction), J.A. Seibert, J. Perry, J.W. Gichoya, J. Kirby et al. « Report of the Medical Image De-Identification (MIDI) Task Group -- Best Practices and Recommendations ». ArXiv [Preprint]. 2023 Apr 1:arXiv:2303.10473v2. PMID: 37033463; PMCID: PMC10081345 ; Y.U. Jeong, S. Yoo, Y.H. Kim, W.H. Shim, « De-Identification of Facial Features in Magnetic Resonance Images: Software Development Using Deep Learning Technology », J Med Internet Res. 2020 Dec 10;22(12):e22739.

[1145] S.M. Moore, D.R. Maffitt, K.E. Smith et al. « De-identification of Medical Images with Retention of Scientific Research Value ». Radiographics. 2015 May-Jun;35(3):727-35.

Or, **là aussi le raisonnement devient circulaire,** car le problème posé est la ré-identification d'une personne à partir de ses données qui auront été « anonymisées », ce qui jusqu'alors était réputé une opération de caractère non réversible. En conséquence, le débat sur les obligations en la matière, **qui nous semble un parent pauvre du RGPD**, ne fait sans doute que s'ouvrir.

Rappelons ici les publications de l'European Union Agency for Cybersecurity (ENISA) [1146], sur notamment le « partage de données » : après son document d'étude de 2022 sur le partage des données non personnelles [1147], l'ENISA énonce dans son document d'étude 2023 sur l'ingénierie du partage des données personnelles [1148], que le « *Data sharing can be considered as* ***disclosing data to third parties outside the organisation*** *in order to achieve a specific purpose. Such sharing can be performed either as part of a processing operation or while attempting to provide additional utility to existing data* » [1149].

Dans le champ d'application du RGPD, on pourrait s'étonner de cette approche (« *peut être considéré comme* ») [1150], mais le « *partage des données* » n'est pas défini en soi dans les textes de droit européen. Enfin, la notion de « *partage des données* » est ici entendu dans un sens très différent de celui, strict, que nous avons relevé en droit français de la santé.

Ainsi l'évolution des technologies et des puissances de calcul conduit parfois à se demander à quel point, alors que **les données santé / non santé sont de plus en plus susceptibles d'être croisées,** il pourra être garanti que celles réputées « non personnelles » le restent ; et à quel point cette éventualité peut être raisonnablement décrite / anticipée par les normes [1151].

[1146] Instituée en 2004, renforcée depuis par le EU Cybersecurity Act

[1147] ENISA (2022), « Data protection engineering – From Thory to Practive », janv. 2022, ISBN 978-92-9204-556-2, Doi 10.2824/09079.

[1148] ENISA (2023), « Engineering Personal Data Sharing - Emerging Use Cases and Technologies », janv. 2023, ISBN 978-92-9204-602-6, Doi 10.2824/36813

[1149] Ibid., page 5.

[1150] L'ENISA n'avait pas pour prétention d'établir une doctrine du partage de données, et devait chercher un concept englobant sans reconvoquer toutes les catégories, ce qui explique cela.

[1151] Les textes européens notamment, invoquent fréquemment les capacités technologiques requises et délais raisonnables, qui ne cessent de se réduire.

SYNTHESE P2T2C1

Dans ce titre 2 dynamique des garanties coordonnées contre l'accès illicite aux données de sante, nous examinons dans un premier chapitre, les garanties coordonnées face aux ingérences d'Etats tiers par voie du droit. Comme dans d'autres domaines, la capacité individuelle des Etats à négocier des garanties dans le cadre de transferts de l'Union est limitée. Si cette dernière a pu convenir d'un droit commun très innovant qui était l'objet du Titre I, l'enjeu est ici de déterminer les conditions d'un dialogue caractérisé par le transfert massif de données outre Atlantique, l'analyse porte donc sur l'interaction droit européen / droit fédéral américain.

* dans une première section, nous relevons les voies juridiques par lesquelles les Etats partageant des valeurs quant aux droits fondamentaux, ont décidé de mutualiser leurs positions et centraliser la négociation. Nous analysons ainsi l'action exécutive européenne en la matière, dévolue à la Commission européenne, et consistant en le contrôle d'adéquation des ordres juridiques tiers de destination, et la validation de clauses type de transfert de données, ces outils étant trans-sectoriels donc non spécifiques aux données de santé. Nous relevons ensuite la sanction juridictionnelle, par la Cour européen de justice de l'Union, du potentiel d'ingérence étatique tierce par voie de droit, d'abord du fait de sa portée non formellement précisée, puis du fait d'une porté certes précisée, mais insuffisamment circonscrite.

* ce panorama brossé, nous analysons la façon dont la recherche coordonnée de garanties par l'Union aboutit à la modification du droit fédéral américain. Nous relevons d'abord les conditions d'élaboration et d'adoption du nouveau cadre juridique approuvé en juillet 2023, avant d'examiner ses conséquences pour les « données de santé » : elles marquent le primat heureux de la conception européenne. Enfin nous esquissons la conséquence de l'approbation, quoique conditionnelle, du transfert des données de santé, si l'Europe ne développe pas rapidement de capacités propres en intelligence artificielle. Le nouveau droit dédié de la concurrence (2022) vise certes à prémunir l'Europe d'abus de position dominante numérique, mais constate la nécessité potentielle d'une jonction des forces publiques et privées dans les scénarios de crise. L'accroissement du volume des données transférées, et des puissances de calcul, met enfin en exergue le risque croissant de réidentification. Il nous conduit à nous demander à quel point une donnée anonymisée même « de santé » pourra longtemps rester anonyme.

CHAPITRE II. GARANTIES COORDONNEES CONTRE LES INGERENCES ETATIQUES TIERCES PAR VOIE DE FAIT

Dans le précédent chapitre, nous avons examiné la recherche coordonnée par les Etats, sous l'égide de l'Union européenne puis à son initiative, de garanties contre les ingérences par voie de droit. L'attribution de l'ingérence ne fait alors pas de doute : **l'Etat tiers revendique formellement un cadre d'ingérence**, que les données aient été transférées sur son territoire ou pas [1152], même s'il se garde généralement de revendiquer des actions précises.

La question de l'accès non attribuable *a priori,* engage une **dimension distincte : celle de la cybersécurité** [1153]. Elle doit répondre à deux défis, parfois mixés : la criminalité de droit commun, que son échelle et impact font depuis des années envisager à une échelle supranationale ; et le dessein d'une **atteinte calculée aux intérêts fondamentaux** d'une communauté politique, pour un but stratégique selon une géopolitique de puissance.

Ce chapitre est justifié par le fait que **données et systèmes de santé sont devenus des cibles fréquentes et massives, voire préférentielles, de telles actions [1154]**. Ceci du fait de la sensibilité de l'opinion publique (au-delà des patients), de l'impact sur la confiance en les décideurs, les institutions publiques et privées et naturellement leur fonctionnement. Cela participe du concept et des stratégies de « cybersécurité », que l'on ne considérera que sous l'angle des données et systèmes de traitement automatisé des données (STAD) en santé.

Le **mélange fréquent des objectifs et des modes d'action (parfois de la mixité même des acteurs de l'illicite)** met en exergue la qualification des actions et leurs conséquences juridiques (section I). Quelle qu'en soient les motivations, elles appellent de plus en plus une réponse coordonnée : celle-ci est désormais également source au plan européen d'une dynamique intégrative, dans un champ historique de souveraineté nationale (section II).

[1152] Nous avons vu que le CLOUD Act de 2018, d'application extraterritoriale, n'était censé concerner que les citoyens ou résidents américains.

[1153] Ce concept et ses applications seront définis au gré de nos développements.

[1154] Réf. citées *infra*, et tout dernièrement, Cartwright AJ. « The elephant in the room: cybersecurity in healthcare ». J Clin Monit Comput. 2023 Apr 24:1–10. doi: 10.1007/s10877-023-01013-5 (impression à venir).

SECTION 1. DYNAMIQUE DES INGERENCES *A PRIORI* NON ATTRIBUABLES DANS LES DONNEES DE SANTE

La dynamique des accès illicites n'est véritablement perceptible que grâce à la recension et qualification des attaques par les spécialistes de cybersécurité. Depuis des décennies, elle est l'objet d'une abondante littérature qu'il n'est pas lieu de développer ici [1155]. Le cyberespace est devenu un espace de déploiement voire de confrontation de puissances, où la distinction public/privé est difficile et parfois artificielle.

Dès lors, en sus de l'adaptation des composantes judiciaires et militaires, le risque / la menace cyber, croissants, sont à l'origine d'institutions nouvelles. Le but est centraliser la vision et orchestrer les réponses, en vue d'une approche systémique dans l'aide à la décision publique : au plan national, avec depuis 2009 l'Agence nationale de sécurité des systèmes d'information (ANSSI), rattachée au secrétaire général de la défense et de la sécurité nationale [1156] ; au plan européen, avec depuis 2004 l'European Union Agency for Cybersecurity (ENISA), laquelle « *vise à* ***garantir un niveau élevé commun de cybersécurité dans toute l'Europe*** **»** [1157].

En juillet 2021, le gouvernement français a créé auprès du Secrétaire général de la défense et de la sécurité nationale (SGDSN) un **service à compétence nationale** dénommé « *service de vigilance et de protection contre les ingérences numériques étrangères* » [1158] ; et en décembre 2021, a autorisé un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères [1159]. Nous ne développerons pas ces points, qui mettent suffisamment **en exergue l'importance, la visée et l'impact du phénomène**.

Dans cette section, nous relevons l'ampleur et la dynamique du phénomène des ingérences par voie de fait [1160] dans le traitement des données de santé (§1). Puis la difficulté de sa qualification, lié à la cause des phénomènes et leurs conséquences (§2).

[1155] N. Arpagian, *La cybersécurité*, PUF 2018.
[1156] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».
[1157] Introduite par règlement (CE) no 460/2004 du 10 mars 2004, puis pérennisée par Règlement (UE) no 526/2013 du Parlement européen et du Conseil du 21 mai 2013.
[1158] Décret n° 2021-922 du 13 juillet 2021.
[1159] Décret n° 2021-1587 du 7 décembre 2021.
[1160] Rappelons que nous utilisons ce terme non au sens du droit public, pénal ni civil français, mais en miroir de l'ingérence par voie de droit, laquelle est formellement revendiquée par son auteur selon ses propres règles.

§1. L'OBSERVATION DES INGERENCES : UNE DYNAMIQUE PERCEPTIBLE DANS LE CHAMP DE LA SANTE

A l'instar d'ingérences relevant de la criminalité de droit commun, ces ingérences sont multiformes. Elles peuvent consister (nous regroupons ici les infractions citées aux articles 323-1 à 323-3 du Code pénal français, détaillées *infra*) : en l'accès ou le maintien frauduleux dans tout ou partie d'un système de traitement automatisé des données ; en le fait d'entraver ou de fausser son fonctionnement ; d'y introduire ou d'en extraire, d'y détériorer, d'en reproduire, transmettre, supprimer ou modifier frauduleusement des données, qu'elles soient personnelles ou non.

En l'état, ces infractions apparaissent définies de façon exhaustive ; l'imagination peine à concevoir de nouvelles possibilités qui s'en détacheraient : l'irruption de l'intelligence artificielle comme moyen technique ne modifie pas ces **concepts de base**.
Certes, ces infractions, dont en 2013 le droit européen a voulu l'harmonisation [1161], **ne sont par nature pas propres aux « données de santé » et aux systèmes de santé** ; mais nous limiterons notre propos à ce terrain emblématique, qui est notre clef d'investigation.

Le fait que la santé soit devenue un champ privilégié et croissant de cyberattaques, a conduit en 2021 à la mise en place en France d'un **observatoire de signalement national pour le secteur santé et médico-social** en la matière [1162], à la publication de rapports dédiés au plan national, et leur pendant au plan européen (*infra*). Ces rapports visent à partager les expériences, sensibiliser les parties, éclairer les politiques et aider à la décision. En santé, le signalement des attaques relève depuis peu en France d'une obligation à la charge des organismes, au-delà de leurs obligations de droit commun à l'égard des personnes concernées.

Pour cette mise en perspective, nous rapporterons ici des pratiques connues d'attaques (A), dont l'analyse met en exergue des méthodes de plus en plus ciblées et sophistiquées (B).

[1161] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information, remplaçant la décision-cadre 2005/222/JAI du Conseil.
[1162] https://esante.gouv.fr/actualites/lobservatoire-des-signalements-dincidents-de-securite-des-systemes-dinformation-pour-le-secteur-sante-et-medico-social-est-en-ligne

A. LES STAD ET LES « DONNEES DE SANTE », DEVENUS CIBLES PRIVILEGIEES DES ATTAQUES

En 2022, le Conseil des ministres de l'Union a invité les Etats membres à intensifier les efforts nationaux en matière de cyber sécurité, qu'il a qualifiée de « priorité de politique de l'Union », ce qui s'exprime tant sur le plan industriel que normatif [1163], *infra*. L'acceptabilité de normes dans l'opinion publique est d'autant plus forte, que cette dernière est sensibilisée à grande échelle sur un terrain d'effet immédiat : les systèmes et données de santé.

Dès 1988, les « systèmes de traitement automatisé des données » (STAD) ont fait l'objet d'une protection pénale [1164], que nous examinerons avec les infractions qui s'y rattachent. Lors de la préparation de la loi, qui ne le définit pas, un STAD est considéré comme « *tout ensemble composé d'une ou plusieurs unité de traitement, de mémoires, de logiciels, de données, d'organes d'entrée sortie et de liaisons, qui concourent à un résultat déterminé,* ***cet ensemble étant protégé par des dispositifs déterminés*** » [1165].

La jurisprudence **n'a pas retenu que cette protection était un critère de définition du STAD** (ce qui, par défaut, eût compromis la caractérisation de l'infraction) : les dispositions permettant de restreindre l'accès ou d'empêcher le fonctionnement du système, de coder ou non les données, n'intéressent ainsi pas la qualification en droit pénal [1166]. En revanche, ils intéressent la couverture assurancielle du dommage ; en outre, la sécurisation du STAD, **qui n'est pas un élément de sa définition, est devenue une obligation légale** [1167], *infra*.

Peu importe l'ingéniosité du mode de pénétration (la jurisprudence sanctionne tant l'utilisation d'un code d'accès [1168], que l'emploi d'un logiciel d'attaque ou d'espionnage [1169] etc.). Nous proposons ici une esquisse de typologie des ingérences dans les STAD **spécialement dans le domaine de la santé** (1) ; ceci avant de relever comment l'appréciation du risque y détermine de toutes récentes obligations graduées de notification (2).

[1163] Conseil des Ministres, 23 mai 2022, Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne, Document 9364/22.
[1164] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite « Godefrain ».
[1165] Doc. Assemblée Nationale 1987-1988, n'1009 – préparation de la loi n°88-19 préc.
[1166] Dreyer E, *Droit pénal spécial*, LGDJ 2020.
[1167] En droit européen, articles 24 et 32 du RGPD (*comp*. article 17§1 de la directive 95/46) ; en droit français, article 4 alinéa 6 de la loi informatique et libertés modifiée par la loi d'adaptation au RGPD du 20 juin 2018, puis par l'ordonnance n° 2018-1125 du 12 décembre 2018.
[1168] CA Paris, chambre correctionnelle, 27 mars 2002, n°01/03421 : Jurisdata n° 2002-180229
[1169] Cass.Crim, 16 janvier 2018, n°16-87.168.

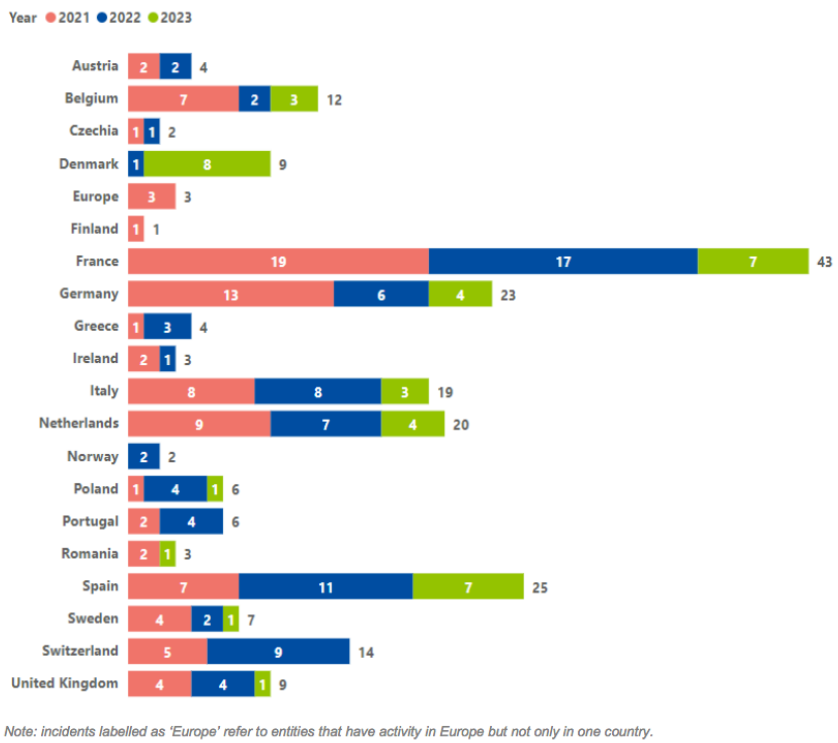
1. Ingérences spéciales dans le domaine de la santé : esquisse de typologie

La mesure du phénomène justifiant la recherche coordonnée de garanties contre ces ingérences, **par les Etats et à rebours de leur tradition régalienne**, appelle une vision consolidée, à l'échelle européenne, des incidents signalés au plan national (nous reviendrons sur l'action de l'ANSSI), et pouvant par ailleurs toucher les institutions de l'Union. Nous ne considérerons ici que l'inventaire le plus récent, publié en juillet 2023 par l'Agence Européenne pour la Cybersécurité (ENISA) [1170].

La particularité de ce rapport est d'être le premier de l'ENISA **qui porte spécifiquement sur atteintes aux STAD dans le domaine de la santé,** de 2021 à début 2023. Il est documenté sur la base de 215 incidents répertoriés dans l'Union élargie à trois pays voisins.

Notons ici que les pays baltes (Estonie, Lettonie, Lituanie), pourtant membres de l'Union, et l'Ukraine, certes non membre de l'Union (mais tout comme la Norvège, la Suisse et le Royaume-Uni), n'apparaissent pas dans ce panorama, **alors qu'ils ont été parmi les premiers théâtres d'action**, *infra*. Nous ne rapportons ici que les tableaux de synthèse.

Les incidents par pays et par année se répartissent comme suit [1171] :



Note: incidents labelled as 'Europe' refer to entities that have activity in Europe but not only in one country.

[1170] ENISA *Threat landscape: Health Sector* (January 2021 to March 2023), July 2023, ISBN 978-92-9204-638-5. https://www.enisa.europa.eu/publications/health-threat-landscape

[1171] Rapport ENISA, juillet 2023, page 9.

Il ne s'agit ici que de la collecte de faits publiés, nous n'y reviendrons pas. **La France est particulièrement concernée, car elle a la réputation de payer les rançons,** *infra*. Il n'existe pas de périmètre d'observation *a priori* pour relater les attaques (naturellement, des ères de surveillance spécifique sont mises en place et élargies au gré des expériences, il n'est pas lieu ici d'entrer dans ces développements) : ce périmètre est celui tracé par les signalements et publications, **la liste n'est donc pas exhaustive**.

Dans ce contexte, on entend par attaques « dans le domaine de la santé » les attaques qui ont ciblé :

* les prestataires de soins largement entendus (directive 2011/24 préc.), ainsi le secteur ambulatoire, hospitalier et médico-social, les services d'urgences, établissements psychiatriques etc. également les prestataires à domicile ;

* les laboratoires de référence de l'Union européenne, évoqués *supra* (règlement 2022/237 préc.), les sites de R&D en matière de produits de santé (Directive 2001/83, en cours de refonte en 2023) et entités publiques ou privées se livrant à la recherche biomédicale ;

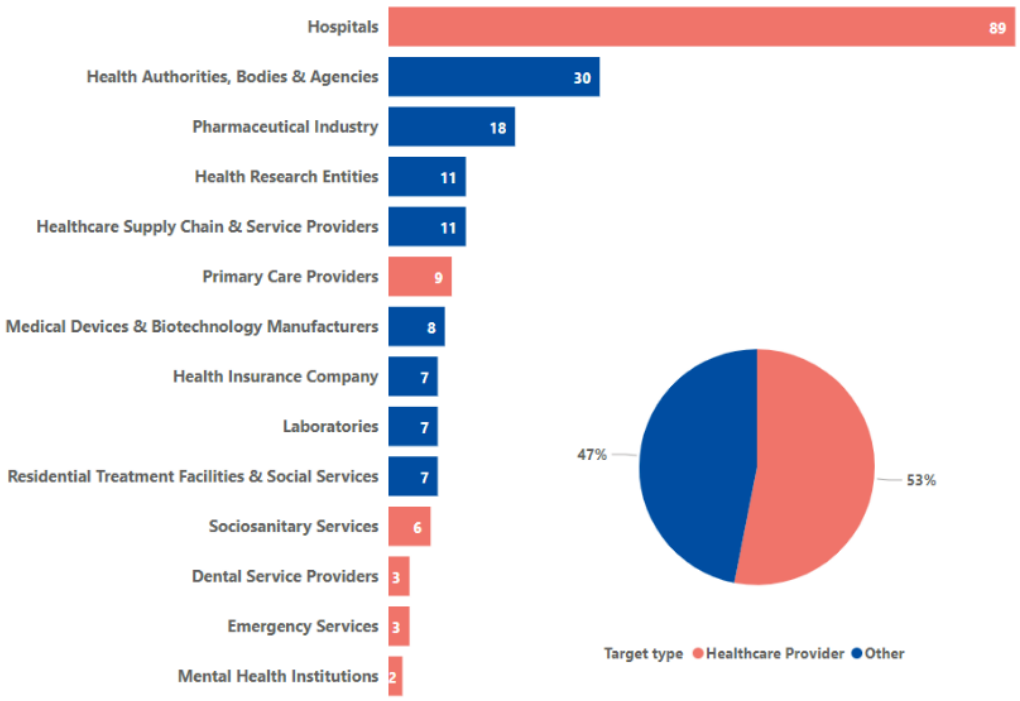
* les industries pharmaceutiques au sens large, entendant des fabricants de principes actifs et intermédiaires de synthèse, jusqu'aux préparations pharmaceutiques en passant par les opérations de façonnage ;

* les industries des technologies médicales (règlement 2022/123 préc.) et des produits biotechnologiques ;

* les organisations assurant la prise en charge des soins, que ce soit le paiement direct ou le remboursement aux patients (secteur public, assurances, mutuelles etc.) ;

* les autorités et agences nationales et européennes en charge de la conception des politiques, de leur pilotage et de la régulation.

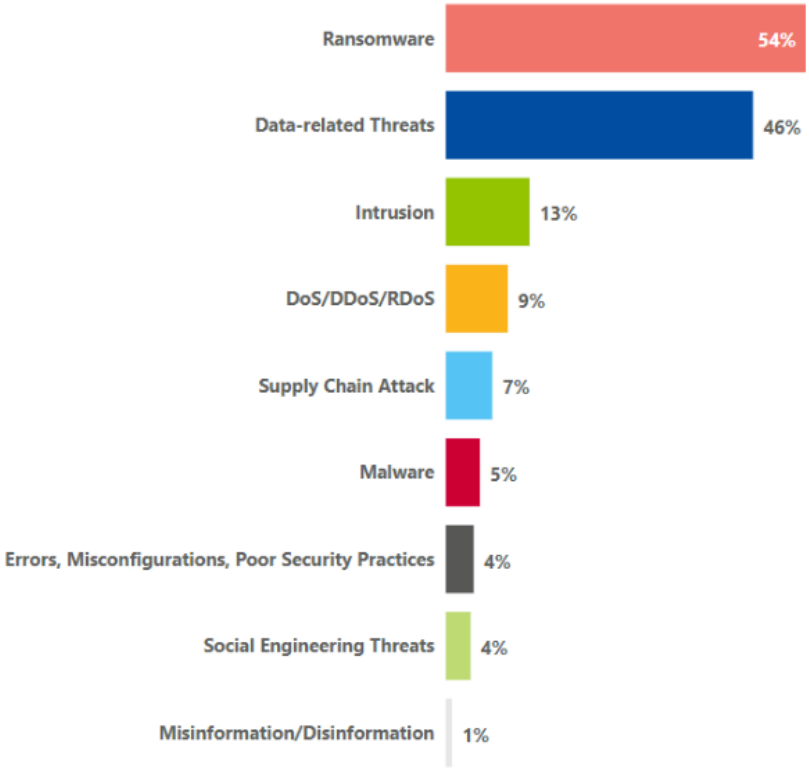
La répartition des entités attaques en santé sur la période est la suivante [1172] :



Les attaques ont été classifiées selon la méthodologie ENISA [1173], qui rapport **des techniques et des buts apparents d'attaques.** L'ENISA distingue spécialement dans son rapport attaques par logiciels de rançonnage ; attaque des données ; attaques par déni de service ; attaques par logiciels malveillants ; menaces par ingénierie sociale [1174] ; attaques de fournisseurs (*supply chain*) ; actions de désinformation et manipulations [1175], etc. **Ces *items* sont parfois connexes** : leur distinction ne sert qu'à la restitution dans ce tableau :

[1172] *Ibid*., page 10.
[1173] Sur la méthodologie en général, ENISA Cybersecurity Threat Landscape Methodology, July 2022.
[1174] Recouvre en anglais « *phishing, spear-phishing, whaling, smishing, vishing, business email compromise, fraud, impersonation or counterfeiting* », rapport ENISA, p. 14.
[1175] Objet d'un rapport général dédié, ENISA, *Foreign Information Manipulation and Interfrence (FIMI) and Cybersecurity – Threat Landscape*, déc. 2022, ISBN: 978-92-9204-606-4. Voir par ailleurs, distinctement sur l plan méthodologique mais pas de finalité stratégique : Suarez-Lledo V, Alvarez-Galvez J. « Prevalence of health misinformation on social media: systematic review », J Med Internet Res. 2021;23(1):e17187.

La typologie des attaques répertoriées sur la période est la suivante [1176] :



A ces éléments directement répertoriés par l'ENISA sur la base des expériences signalées, il faut **ajouter des menaces non rapportées, quant au piratage de dispositifs médicaux individuels** (qui peuvent servir tant de cibles, que de portes d'entrée dans les systèmes) [1177].

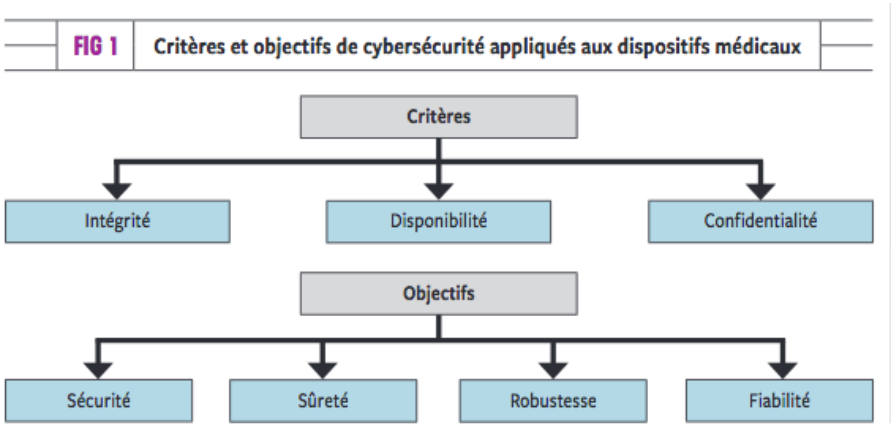
Ainsi, des vulnérabilités ont été découvertes sur des pompes à perfusion, qui visent à l'administration de médicaments comme les antibiothérapies, antidouleurs (pompe à morphine), l'équilibrage de l'insuline, les antinéoplasiques (traitements contre les cancers) [1178] ; sur des stimulateurs cardiaques (Dick Cheney, ancien vice-président des Etats-Unis, a fait désactiver la fonction wi-fi de son défibrillateur par sécurité contre une éventuelle attaque ciblée) [1179] ; on pourrait ajouter les implants connectés de stimulation neurologique profonde.

[1176] Rapport ENISA 2023 préc., p. 12.
[1177] Wellington K. « Cyberattacks on medical devices and hospital networks : legal gaps and regulatory solutions ». Santa Clara High Tech 2013;lJ30:139.
[1178] Voir le très intéressant Healthcare Industry Cybersecurity Task Force, « Ressource Catalog», mai 2017 (https://www.phe.gov/Preparedness/planning/CyberTF/Documents/hccs-tf-resource-catalog.pdf) ; Armstrong DG, Kleidermacher DN, Klonoff DCet al. « Cybersecurity regulation of wireless devices for performance and assurance in the age of « medjacking ». J Diabetes Sci Technol 2015;10:435-8 ; FDA, « Cybersecurity vulnerabilities of hospira symbiq infusion system » : FDA safety communication, 2015.
[1179] Gupta S (CNN Chief Medical Correspondent), « Three things I learned about Dick Cheney », CNN, 19 octobre 2013 ; auparavant, Gupta S. « Implantable medical devices-cyber risks and mitigation approaches ». Cybersecurity in Cyber- Physical Systems workshop, 2012.

Des vulnérabilités existent sur des dispositifs de santé portables (de portes d'entrée vers les STAD), lesquels recouvrent tant les dispositifs médicaux, que les applications de « bien être », *supra*. Plus généralement, tous les objets connectés (dit « IoT », pour *Internet of Things*) entreront dans le champ des textes sur la cybersécurité que nous analyserons ; mais ils ne couvriront pas les dispositifs médicaux, lesquels relèvent de leur propre droit, *infra*.

Ces considérations et parfois expériences, justifient aussi en droit fédéral américain l'adoption **du critère de la vulnérabilité cyber comme élément de définition du « *cyber medical device* »,** *supra* ; et la proposition en mai 2023 par la Federal Trade Commission d'une modification du statut des déclarations d'incidents en la matière : pour rappel, la FTC propose que, en cas de divulgation de données non autorisées, les « *breaches by health apps and other technologies* » **deviennent des « *health breaches* »** [1180], nous l'avions vu en introduction.

En septembre 2022, le FBI a encore lancé une alerte en ce sens, assortie de nombreuses recommandations techniques [1181]. Rappelons ici qu'en 2017, l'ANSM avait créé en France le premier comité scientifique spécialisé temporaire (CSST) sur la cybersécurité des dispositifs médicaux [1182] ; la question était formalisée en 2013 aux Etats-Unis [1183], et une étude suisse en 2016 résume bien plusieurs points d'attention que nous ne développerons donc pas ici :



[1180] FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule, 18 mai 2023.
[1181] FBI, Cyber Division, Notification Private Industry, 12 sept. 2022, n° 20220912-001 (TJP :WHITE).
[1182] http://ansm.sante.fr/L-ANSM/Comites-scientifiques-specialises-temporaires/Comites-scientifiques-specialises-temporaires/Comites-scientifiques-specialises-temporaires/CSST-Cyber-securite-des-logiciels-dispositifs-médicaux. Voir Pezzali g, Espesson-Vergeat B, « Cyberattaque des objets connectés dans le secteur de la santé : quelle protection des fabricants et des utilisateurs ? »20 nov. 2017, FIDAL.
[1183] Wellington K. « Cyberattacks on medical devices and hospital networks : legal gaps and regulatory solutions ». santa clara High tech 2013;lJ30:139 ; Aker SD, Knudsen J, Ahmadi DM. « The Wireless challenge : security and safety for medical devices and Hospitals », Biomed Instrum technol 2013;47:208-11.

2. L'appréciation du risque détermine des obligations graduées de notification en santé

Quelles conséquences en France ? Si toutes les hypothèses précitées **entrent dans le champ du signalement obligatoire**, tel n'est pas le cas de toute atteinte à un STAD, même dans le domaine de la santé. On esquisse ici ce qu'il en est en matière d'obligations, tant à l'égard des institutions que des personnes.

*** Depuis octobre 2017, le droit de la santé impose** en effet aux « *établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins* » [1184], et depuis 2018, aux hôpitaux des armées (sous réserve du respect des règles relatives à la protection du secret de la défense nationale), de déclarer les incidents de sécurité relatifs à leurs systèmes d'information (L. 1111-8-2 CSP).

Depuis novembre 2020, cette obligation a été étendue par ordonnance aux établissements médico-sociaux [1185]. Mais le droit a ensuite défini les établissements concernés : l'article D. 1111-16-4 CSP précise qu'il s'agit des établissements de santé ; hôpitaux des armées ; laboratoires de biologie médicale ; centres de radiothérapie ; établissements médico-sociaux, et cela (quels que soient leur statut, public ou privé). **Or, cela écarte** les maisons de santé, équipes pluridisciplinaires de soins et autres formes d'activité libérale ou sociale qui peuvent interconnecter des STAD également convoités ou infectables [1186].

Le but est, au niveau national, l'information continue des autorités compétentes de l'Etat (not. l'ANSSI) tant pour décider de mesures de prévention en matière de sécurité, que visant à la continuation des soins (D. 1111-16-4, 1°) ; au niveau local, d'aider à la prise de mesures pour prévenir la survenue d'incidents qualifiés (*infra*), ou en limiter les effets (D. 1111-16-4, 2°).

Les catégories d'incidents concernés, les modalités de leur signalement et traitement ont été précisés dans une sous-section 4 dédiée du Code de la santé publique (D.1111-16-2 à D. 1111-16-4), créée en 2017 [1187] et modifiée en 2022 [1188]. A **l'obligation de signalement de**

[1184] Loi n° 2016-41 du 26 janvier 2016.
[1185] Ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé.
[1186] MASCF, « Les cybercriminels s'attaquent aux professionnels de santé », 15 juin 2020, site MASCF. Nous le citons, car il s'agit du volet d'information d'un site d'assurances pour les professionnels de santé libéraux.
[1187] Décret n°2016-1214 du 12 sept. 2016.
[1188] Décret n°2022-715 du 27 avril 2022.

l'incident « grave », le décret de 2022 ajoute l'obligation de signalement de l'incident « significatif ».

Ainsi dans la typologie réglementaire, existent depuis 2022 des incidents **« graves ou significatifs »** définis dans le CSP [1189] ; mais aussi des incidents **significatifs « parmi les incidents graves »,** du fait de leur potentiel d'extension dans les systèmes [1190]. Quoiqu'il en soit, il n'est pas lieu ici d'examiner la procédure et les conséquences de la déclaration, sinon pour relever la jonction avec l'ANSSI. Elle s'impose « *notamment en cas d'incident concernant un opérateur de service essentiel* (OSE) *ou qui pourrait avoir un impact de portée nationale* » (D. 1111-16-3), la déclaration de cet OSE à l'ANSSI étant obligatoire [1191].

Sur cette base, l'ANSSI a en 2020 contribué au développement dans le cadre du programme France Relance, d'un **volet de cybersécurité dédié aux établissements de santé** [1192]. Il consiste en des prestations financées pour renforcer au plan local la sécurité des établissements de santé grâce aux « *parcours de cybersécurité* », selon leur maturité en la matière ; et au plan national, notamment en le soutien de la cellule « *Accompagnement cybersécurité des structures de santé* » (ACSS) du ministère des Solidarités et de la Santé.

* A ces obligations spécifiques entre établissements et institutions relevant du droit de la santé, s'ajoutent en droit commun, **en cas de risque pour la vie privée d'individus dont les données personnelles seraient compromises, l'obligation d'informer la CNIL** d'un tel risque, et d'informer individuellement les personnes concernées en cas de « risque élevé » [1193].

[1189] Sont qualifiés tels, « *les événements générateurs d'une situation exceptionnelle au sein d'un établissement, organisme ou service, et notamment : - les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins ; - les incidents ayant des conséquences sur la confidentialité ou l'intégrité des données de santé ; - les incidents portant atteinte au fonctionnement normal de l'établissement, de l'organisme ou du service ; - les incidents ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé ; - les incidents susceptibles de toucher d'autres établissements, organismes ou services* » (D. 1111-16-2-II CSP).

[1190] « *Incidents ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé et les incidents susceptibles de toucher d'autres établissements, organismes ou services* » (D.1111-16-2-III CSP).

[1191] Sur le plan pratique, voir la mise en œuvre des procédures éclairée par (vérifié juillet 2023) https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/

[1192] ANSSI 2020 (publié avril 2021), Cybersécurité : protéger les établissements de santé avec France Relance.

[1193] RGPD, article 34 : « *La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d)* ».

En cas de doute quant à la graduation de ce risque, la CNIL indique la procédure à suivre au responsable qui l'a saisi. L'obligation d'informer la personne ne s'applique pas dans certaines conditions, qu'il n'est pas lieu de développer ici (RGPD, article 34§3, a,b,c).

Notons qu'aux Etats-Unis, des règles de notification ont été posées dès 2009, pour informer les patients [1194]. En 2021, l'agence fédérale américaine FTC a appelé les opérateurs à respecter les règles de notification d'atteinte aux données en santé [1195], sachant que sa position de « clarification », contenant une extension du champ d'application, n'a pas fait l'unanimité, nous l'avons vu en introduction : depuis 2023, les détenteurs des données ne doivent **pas seulement déclarer les incidents de violation, mais aussi les cas d'accès non autorisés** [1196].

En outre, la FTC vient de proposer (mai 2023) un renforcement des règles, **afin de l'étendre aux « applications de santé » et les autres technologies** [1197] : cela témoigne aussi de la porosité des champs technologies médicales / non médicales [1198].

B. LES MODES D'INGERENCE AU CARREFOUR DES ORGANISATIONS CRIMINELLES ET ETATIQUES

L'analyse des modes d'action a fait l'objet de recherche approfondies et de rapports de synthèse réguliers. En 2022, l'ANSSI a publié son panorama de la menace informatique 2021, et en 2023, le rapport 2022 (on a vu *supra* le rapport ENISA sur la santé au niveau européen). Dans son rapport 2021, elle relève la constante progression des capacités d'« *acteurs offensifs* », avec, distinctement de la classique criminalité de droit commun, des intentions peu visibles d'espionnage et de sabotage ; elles exploitent les opportunités technologiques et nouveaux usages du numérique [1199], confirmé en 2023 dans un contexte qui a changé, *infra*.

[1194] Code of Federal regulation, Article 318, « Health breach notification rule », Public Law 111-5, 123 Stat. 115 (2009) 74 FR 42980, 25 août 2009.

[1195] (Federal Trade Commision) FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule, 15 sept. 2021 site www.ftc.gov.

[1196] (Federal Trade Commission) FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising, 1er fév. 2023.

[1197] (Federal Trade Commision), FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule, 18 mai 2023, site www.ftc.gov

[1198] Levine S, Directeur du bureau de la protection des consommateurs de la FTC, en mai 2023 : "*We are witnessing an explosion of health apps and connected devices, many of which aren't covered by HIPAA, collecting vast amounts of sensitive consumer health information. When this information is breached, it is more vital than ever that mobile health app developers and others covered by the Health Breach Notification Rule provide consumers and the FTC* ***with timely notice about what happened*** ".

[1199] ANSSI, Panorama de la menace informatique 2021, 1.9.1. du 9 mars 2022, TLP :White.

L'ANSSI note que la « *porosité entre différents profils d'attaquants complique la caractérisation des activités malveillantes* » [1200], et *a fortiori* leur attribution. Un considérant de la proposition en avril 2023 du règlement « Cybersolidarité » pointe de façon explicite et contextualisée, la menace de cyberattaques majeures sur des infrastructures critiques : *« Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister* ***au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles*** » (Consid. 2) [1201].

Le rapport de l'ANSSI en 2022 invite à distinguer des cas d'emprunts d'outils cybercriminels par des acteurs étatiques (2), après des cas d'emprunts d'outils de niveau étatique par des cybercriminels (1) ; nous rapporterons rapidement cette distinction dont les propos précédents constatent les limites, du fait de l'ambigüité des acteurs et des modes opératoires.

1. Emprunts d'outils de niveau étatique par des cybercriminels

La notion de « niveau étatique » n'a rien de juridique : elle exprime seulement que des acteurs privés non étatiques (mais pouvant travailleur pour le compte d'Etats) développent des **capacités technologiques d'impact stratégique, ce qui était autrefois l'apanage des Etats.**

Il n'est pas nécessaire ici de nombreux développements. Depuis plus de 10 ans, des prestataires spécialisés développent des outils proposés sur le marché pour des finalité d'ingérence, et cela à des **clients multiples qui ne sont plus seulement des clients étatiques.** Le marché propose des outils techniques, de l'expertise humaine, des méthodes d'exploitation de différents types de vulnérabilités, qui seront présentés comme des outils défensifs (marché légal sous licence d'exportation de matériels classés, *infra*), ou offensifs (marché illégal notamment sur le *DarkWeb*). Ainsi en est-il de, l'exploitation de

*** vulnérabilités dites « *0-Day* » :** ce terme exprime le fait que l'entité attaquée ne dispose d'aucun délai (zéro jour, *zero day*) pour programmer un correctif. La découverte de la vulnérabilité est généralement liée à l'objectivation du dommage. Cette vulnérabilité naît de la programmation initiale d'un logiciel, dans lequel surnage une faille qui par définition n'aura pas été perçue par son développeur. Un « *hacker* » qui la découvre, écrit un code qui

[1200] *Ibid*., page 3.
[1201] Proposition présentée le 18 avril 2023, de Règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, COM(2023) 209 final 2023/0109(COD).

permet de l'exploiter. Le *hacker* peut alors l'exploiter lui-même, vendre son code d'attaque sur le marché noir (ou le vendre au développeur du logiciel pour prémunir ses propres produits de l'attaque), à moins de travailler pour le compte d'autrui.

Seule son exploitation révélera la faille, dont le colmatage rapide sera le but de développeurs internes à l'entité, ou agissant pour elle. Seule l'installation du correctif permettra le retour de la sécurité. Mais **en attendant, les informations sont compromises sur une période et pour une ampleur non connue,** sans que les logiciels dits « antivirus » puissent détecter le code d'attaque 0-Day : n'étant pas connu donc reconnu, **il peut donc agir longtemps** (comme en biologie un virus qui muterait pour leurrer le système immunitaire dont la vitesse d'apprentissage est moindre). En réponse, des outils sont développés pour la détection précoce d'anomalies dans les accès aux données et leurs mouvements [1202], afin de limiter les dégâts par une action précoce.

Il n'est pas nécessaire ici de rappeler que de nos jours, des personnes « *hackers* » de tous âges, de tous pays, pour tous motifs (pas seulement par cupidité ou malveillance), peuvent s'adonner à la traque et à la valorisation des failles, ou plus honorablement à leur signalement. Cela n'est plus un sport **que l'on pouvait historiquement imaginer de monopole étatique**. Mais certains pays motivent et « industrialisent » spécialement ces modes d'action, *infra*.

*** vulnérabilités dites « *0-Click* » :** ce terme exprime le fait qu'aucune interaction n'est nécessaire avec la cible (0-Click). Cela rend ce type d'attaque particulièrement redoutable, pour le **vol de données ou la prise de contrôle à distance d'un système**, car son *utilisateur légitime,* victime de l'action, peut ignorer qu'il a été ciblé et pénétré : aucune action de sa part *n'est requise,* qui pourrait le faire douter avant, ou l'alerter rétrospectivement.

Cela différencie l'attaque « *0-Click* » de modes d'action moins sophistiqués que sont le *phishing (hameçonnage* [1203]*) ou le smishing (hameçonnage par SMS, en plein essor) etc.,* lesquels s'appuient sur l' « ingénierie sociale » précitée : elle vise à faire qu'un utilisateur abusé, active un code malveillant en cliquant sur un fichier (message écrits, vocaux, images etc.). Ces techniques peuvent être qualifiées de rustiques, quoique très efficaces, du fait de la faible attention souvent des utilisateurs non avertis ou non disciplinés, notamment dans les

[1202] Systèmes de détection d'intrusion (IDS) et systèmes de prévention des intrusions (IPS).
[1203] Récupérer par tromperie, des données personnelles en vue d'un usage malveillant.

organisations civiles. En contraste, un utilisateur **même méfiant et discipliné**, peut être circonvenu par un outil 0-Click, apanage, pour l'instant, d'acteurs sophistiqués.

Dès lors, on voit des opérateurs **privés utiliser des systèmes de plus en plus sophistiqués pour la capture de données, l'interception de communications, la prise de contrôle de systèmes,** alors que ces systèmes sont en droit sous haute surveillance pour la protection des libertés publiques et des droits fondamentaux, nous l'avons vu.

Certains de ces savoir-faire et ressources technologiques sont vendus sur le marché officiel, **régulé par des licences d'exportation, quand les matériels sont déclarés** et que leur fabricant/distributeur cherche une autorisation administrative, au titre par ex. en France de leur classement « guerre et assimilé », sous le contrôle de la Commission interministérielle pour l'étude des exportations de matériels de guerre (CIEMG) [1204].

Hors de la compétence française, la vente par la société israélienne NSO Group, du système dit « *Pegasus* », est à l'origine d'une affaire particulièrement connue. Après installation dans un téléphone mobile, ce système permet de suivre toutes activités de son utilisateur, et l'actionner à distance pour la capture de son et d'images. L'affaire a été révélée en 2021 par un consortium de 17 médias internationaux, après la découverte d'un usage extensif attentatoire aux droits fondamentaux et libertés politiques [1205], comme à la souveraineté [1206].

Or, la société *NSO Group* le présentait « *comme sans égal pour permettre aux gouvernements de lutter contre les réseaux criminels et les groupes terroristes* » ; mais il a manifestement été utilisé aussi pour d'autres finalités. De même, la société italienne *Hacking Team* vend des prestations avec le même slogan « *nous pensons que combattre le crime doit être facile : nous fournissons dans le monde entier une* ***technologie offensive****, efficace et simple d'utilisation, à destination des organismes chargés d'appliquer la loi et des services de renseignements* » [1207]. Ainsi, **les Etats sont devenu les clients des opérateurs marchands, et leur achètent dans le privé une capacité technologique pour assumer leurs responsabilités d'Etats.**

[1204] Articles L. 2335-2, L. 2335-3, L. 2335-9 et L. 2335-10 du Code de la Défense ; voir la directive 2012/10/UE du 22 mars 2012 portant modification de la directive 2009/43/CE du Parlement européen et du Conseil en ce qui concerne la liste des produits liés à la défense. Voir le Rapport d'information n°3581 déposé le 18 nov. 2020 à l'Assemblée nationale, sur le contrôle des exportations d'armement.

[1205] Journalistes, parlementaires, militants, chefs d'entreprise, familles, etc.

[1206] Coll. « Comment les services de renseignement français ont traqué Pegasus après les révélations du « Monde», Le Monde, 19 novembre 2021.

[1207] Signalé par Reporters sans frontières, Rapport « Les ennemis d'Internet », 2013.

Ce qui nous intéresse ici, sont les questions posées **sur les clients effectifs** de sociétés et sur leurs buts : Comme d'autres, NSO Group fait savoir « *nous fournissons le logiciel, nous n'exploitons pas le système* », déclare officiellement avoir « *lancé une enquête interne* » suite à la révélation d'usage extensif, puis invoque opportunément le besoin d'un cadre légal international « *pour mieux déterminer les utilisateurs finaux légitimes de ces systèmes* » [1208].

Des sociétés spécialisées dans le développement de tels produits et prestations, soumises à licence d'exportation, et ayant pour client prioritaire ou revendiqué des Etats dans leurs missions régaliennes, ont été notoirement *hackées* [1209] : une opportunité de récupérer leurs données et savoir-faire, conçus pour un marché en théorie hautement surveillé (aussi de connaître des clients non toujours bien identifiés ?). **Cela justifie leur surveillance étatique** par les licences d'exportation tant qu'un prestataire s'y soumet [1210], et leur assujettissement aux exigences spécifiques de la réglementation sur la cybersécurité (Dir. 2022/2555, *infra*).

Il ne semble pas nécessaire ici de citer d'autres exemples, pour expliquer que **sophistication et puissance exponentielle d'ingérence ne sont plus l'apanage de puissances étatiques**. Ceci sans compter le potentiel ouvert par l'intelligence artificielle, au regard des enjeux de compétence humaines, qui déjà l'emportaient sur les besoins en capitaux et infrastructures.

2. Emprunts d'outils cybercriminels par des acteurs étatiques

La question de l'« acteur » ou du « commanditaire étatique » devient complexe, car elle suppose une attribution, sur laquelle on reviendra. Dans son rapport publié en 2022, l'ANSSI a en ce sens, dans son champ de compétence, relevé l'emploi croissant d'outils et/ou de méthodes relevant de la cybercriminalité, par de tels « acteurs étatiques » [1211].

Dans le rapport 2023 de l'ANSSI, ces *items* sont développés, mais avec une autre présentation, sans qu'une évolution majeure soit constatée après une année marquée par le conflit russo-ukrainien [1212] ; en revanche, « *si une chute de l'activité liée aux rançongiciels a bien été observée par l'(ANSSI) sur les opérateurs régulés publics et privés* ***à l'exception des hôpitaux,*** *elle n'illustre pas l'évolution générale de cette menace cyber qui se maintient à un*

[1208] Saget J, « Affaire Pegasus ; NSO appelle à une régulation internationale », Le Figaro, 5 oct. 2021.
[1209] Reynaud F, « Le vendeur de logiciels espions Hacking Team victime d'un piratage massif », Le Monde, 6 juillet 2015 ;
[1210] Untersinger M., « Logiciels espions : Hacking Team privé de licence d'exportation », Le Monde, 11 avril 2016.
[1211] Rapport ANSSI « Panorama de la menace informatique 2021 », mars 2022 préc., spéc. pages 8 à 10.
[1212] Rapport ANSSI publié le 24 janvier 2023, « Panorama de la menace informatique 2022 ».

niveau élevé ***en se déportant sur des entités moins bien protégées*** » [1213], et parfois vulnérables sur le terrain de l'ingénierie sociale, ainsi dans le domaine de l'Assurance Maladie [1214].

Il n'est pas lieu de développer ces points ici, mais la (présomption d') attribution est liée aux types de cibles (une demande de rançon peut habiller un dessein plus profond, et distraire quand à l'attribution) ; aux modes opératoires révélant l'implication directe ou indirecte de services de renseignement ; le recours à des « *modes opératoires réputés liés à des Etats* » ; le soin particulier mis à la combinaison de modes opératoires, qui rend difficile de caractériser l'action et floute son attribution, alors que cette action est menée sur une cible de façon durable, par des entités que l'on peut supposer structurées et professionnalisées [1215] . **Cette dimension sophistiquée et persistante qualifie les APT,** bien distinctes de ce qui précède.

Les acteurs et attaques dites APT (*Advanced Persistant Threat*) sont particulièrement difficiles à identifier et contrer : pour maintenir ses accès à long terme dans le système, l'attaquant adapte en effet de façon continue les outils qu'il y déploie. Dès lors, il est difficile pour ses défenseurs et les enquêteurs d'établir l'historique et la durée d'implantation (donc l'ampleur de la compromission du système/ des données), sachant certaine la motivation de l'attaquant à s'y maintenir (que la cible soit un organisme gouvernemental, une entreprise d'intérêt stratégique, ou autre). **Pour autant, il devient possible par l'expérience partagée d'établir des modes opératoires récurrents,** y compris dans leur évolutivité (Techniques, Tactiques et Procédures - TTP).

Depuis les années 1990, ce travail a aboutit à l'établissement progressif d'une typologie publique dont des *Advanced Persistant Threat*, et leur identification selon une nomenclature conventionnelle, le n° identifiant l'initiateur de l'attaque de façon non nécessairement chronologique pour les raisons précitées (les APT1, APT2 et APT3 etc. sont chinoises ; les APT28 dite « *Fancy Bear* », APT29 dite « *Cozy Bear* » etc. russes ; les APT 34 dite « *Hellix Kitten* » et APT35 dite « *Charming Kitten* » etc. iraniennes ; l'APT38 dite « *Lazarus Group* »

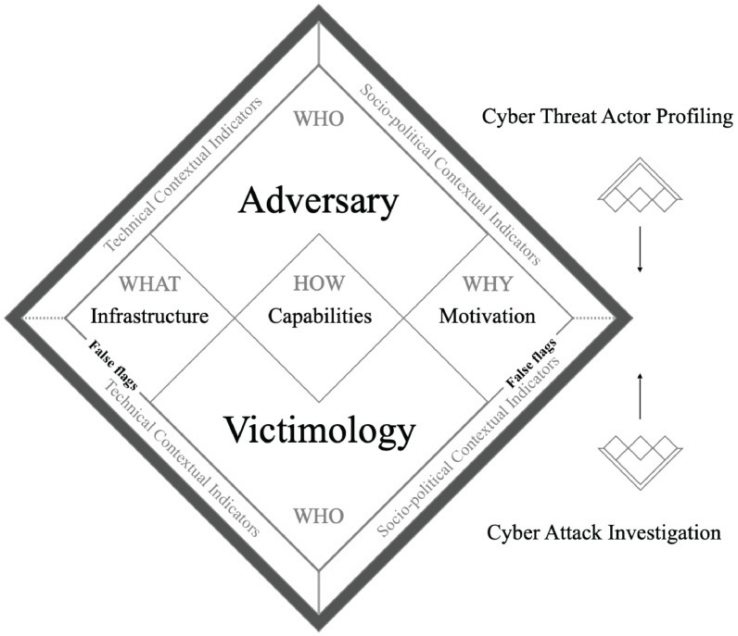
[1213] *Ibid*., p. 4.
[1214] *Ibid*., p. 19 (exploitation exponentielle du thème « Assurance Maladie » dans les courriels l'hameçonnage).
[1215] Rapport ANSSI 2021 publié 2022 préc. « 1.2. Des acteurs étatiques de moins en moins identifiables », p. 8.

de Corée du Nord etc.). Cela permet de caractériser les objectifs stratégiques (extorsion, espionnage, sabotage), les activités, modes opératoires, et liens éventuels avec des Etats [1216].

Ainsi en 2021, une APT31 (également identifié sous les appellations « *BARIUM* » et « *Winnti* ») contre la France par un groupe de hackers soupçonné d'être affilié à l'Etat chinois [1217] ; en 2020 une APT41 sans cible particulière par des hackers chinois, etc. actions qui relèvent d'une finalité considérée duale (dont la société *FireEye* relève l'alignement des cibles avec le plan quinquennal de développement chinois [1218]) ; auparavant le groupe APT20 depuis 2011, selon le rapport de la société *Fox-IT*, etc. Il n'est pas lieu de développer : **l'atteinte à la souveraineté est suffisamment caractérisée au-delà de la criminalité de droit commun**.

La particularité est que les APT sont des outils **qui participent de guerres parfois dites « hybrides »** *infra*, car elles procèdent de modes d'actions non conventionnels dans des conflits non déclarés : en l'absence de déclaration de conflit et/ou d'emploi parallèle de moyens conventionnels, les APT permettent, par leur nature, aux commanditaires publics, de conduire des **actions stratégiques sous couvert de groupes criminels** ; de dénier des ingérences dont l'attribution certaine est difficile (infra) ; d'arguer de leur respect du droit international, et… de la souveraineté de leurs interlocuteurs. Une matrice de raisonnement spécialement explicite [1219], permet de comprendre la base du raisonnement :

[1216] Guiffard J, « Menace dans le cyberespace : qu'est-ce qu'une APT et pourquoi s'en soucier ? », 7 juin 2023, plateforme *Expressions*, Institut Montaigne.
[1217] Cimino V, « APT31 : le groupe de hackers affilié à l'État chinois s'attaque à la France » in Le Siècle Digital, 23 juill. 2021 ; CERT-FR : Campagne d'attaque Du Mode Opératoire APT31 : Description, Contre-Mesures et Code. 15 décembre 2021, disponible sur https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/.
[1218] Fraser N, Plan F, O'Leary J, Cannon V, Leong R, Perez D, Shen C.E Rapport Fire Eye, « APT41: A Dual Espionage and Cyber Crime Operation », 7 août 2019, disponible sur https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf
[1219] Kim K, Shin Y, Lee J, Lee K. « Automatically Attributing Mobile Threat Actors by Vectorized ATT&CK Matrix and Paired Indicator ». Sensors (Basel) 2021 Sep 29;21(19):6522.



En santé, les APT ont vocation à concerner les centres de recherche, les industries pharmaceutique et de technologie médicale, les agences et organismes de régulation, pour **l'acquisition discrète à long terme d'avantages compétitifs** : des informations à caractère scientifique, technique, clinique (résultats d'essais) ; des éléments de positionnement doctrinal (préparation de décisions, projets de réglementation, etc.).

L'APT dans un hôpital aurait peu de sens, à moins de convoiter des données de recherche scientifique et clinique, des données personnelles de santé [1220], et potentiellement des données génétiques. Mais dans l'affaire « *NotPetya* » (qui n'est pas une APT, mais dont le vecteur était une APT), on verra le déploiement d'outils cybercriminels **à dessein terroriste** : après paiement de la rançon, le programme malveillant insinué dans un logiciel de comptabilité **activait non la restitution, mais la destruction des données,** de portée mondiale (attaque initiée en Ukraine en 2017), avec un effet dramatique sur les hôpitaux notamment, *infra*.

[1220] Ainsi de dirigeants politiques.

§2. L'ATTRIBUTION DES INGERENCES : UNE COMPLEXITE POLITIQUE AUTANT QUE TECHNIQUE

Rappelons qu'en juillet 2021, a été créé auprès du Secrétaire général de la défense et de la sécurité nationale (SGDSN) un **service à compétence nationale** dénommé « *service de vigilance et de protection contre les ingérences numériques étrangères* » [1221] ; et en décembre 2021, l'autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères [1222]. Nous ne développons pas ce point.

Nous venons de relever l'observation des ingérences « de fait » dans les STAD en santé notamment. Cette observation est documentée par le signalement obligatoire des risques selon leur nature et gravité, et analysée par les experts de la sécurité de systèmes d'information et des stratégies de prévention d'ingérences. Dans son prolongement, la question de **l'attribution à un auteur** relève d'une démarche qui mêle technique, judiciaire et politique.

Le préalable est l'existence des infractions commises à l'égard des « STAD ». Cette notion qui n'avait pas été définie en droit (*supra*), est **en cours d'élargissement,** on va le voir : en 2022, un règlement européen vient d'être proposé qui vise à étendre aux produits *à composante numérique* (sauf les dispositifs médicaux qui relèvent d'un droit propre) l'obligation de sécurité faite à leurs producteurs face au risque cyber, *infra*. Cette extension annoncée du périmètre n'a pas ici d'incidence, le problème étant constant pour deux raisons.

En premier lieu, sauf à ne pouvoir immédiatement **connaître et mesurer les conséquences à terme** d'une ingérence dans un STAD (en cas notamment d'APT), sa qualification en droit commun ne soulève pas de difficultés particulières (A).
En revanche, il est complexe d'**établir techniquement, puis assumer politiquement l'attribution en cas d'ingérence étatique,** dans le but de la dénonciation d'action, de la réparation (B), et/ou de mesures de rétorsion.

A. L'ABSENCE DE DIFFICULTE EN DROIT COMMUN DE QUALIFICATION DES PRATIQUES D'INGERENCE

Les systèmes de traitement automatisé des données (STAD) combinent à des degrés et pour des finalités variables, des unités de stockage et/ou traitement de données (à caractère personnel ou non), douées d'interfaces pour la communication et la liaison. **Ces systèmes ont**

[1221] Décret n° 2021-922 du 13 juillet 2021.
[1222] Décret n° 2021-1587 du 7 décembre 2021.

en commun de devoir être obligatoirement sécurisés par leurs responsables légaux [1223], sous peine de sanctions administratives [1224] comme pénales [1225]. La défaillance humaine s'avère souvent critique dans des systèmes même bien protégés *a priori*, d'où l'importance de l'ingénierie sociale par les *hackers*, et leurs facilités à l'égard des patients et assurés sociaux.

Mais au-delà des « systèmes » au sens classique, quoique non définis dans le RGPD [1226], la notion de STAD tend à recouvrir les objets connectés, en développement exponentiel [1227]. Pour rappel, on entend habituellement par là « *un objet physique dans lequel sont intégrés des moyens techniques lui permettant de collecter, stocker, traiter et émettre des données grâce à des technologies sans fil* » [1228], qu'ils soient connectés à un réseau, un logiciel, ou entre eux.

Or, **l'obligation légale de cybersécurité en la matière est en cours d'extension européenne. En septembre 2022,** un règlement européen dédié aux produits « *comportant des éléments numériques* » a en effet été proposé en ce sens [1229]. Il s'appliquera à tous ces produits car aucun n'étant anodin, du fait des conséquences des interconnexions [1230]. Jusqu'alors, ces produits n'étaient pas couverts par les textes européens sur la cybersécurité, qui traitaient d'autres aspects de certification de produits, processus et services TIC [1231], *infra*.

De ce fait, nous voyons rapidement les incriminations existantes en droit pénal (1), avant de relever la difficulté de d'appliquer ce droit en cas d'ingérences sophistiquées (2).

[1223] En droit européen, articles 24 et 32 du RGPD (*comp*. article 17§1 de la directive 95/46) ; en droit français, article 4 alinéa 6 de la loi informatique et libertés modifiée par la loi d'adaptation au RGPD du 20 juin 2018, puis par l'ordonnance n° 2018-1125 du 12 décembre 2018.

[1224]Amende administrative d'un maximum de 10 millions d'euros ou de 2% du chiffre d'affaires annuel mondial total de l'exercice précédent (le montant retenu étant le plus élevé).

[1225] Articles 226-16 et s. du Code pénal.

[1226] Dans son article 1, le RGPD traite des opérations, non des systèmes, il n'invoque que le recours à des « *procédés automatisés* » sans précision ; non plus l'article 32, lequel ne traite que des opérations et procédures.

[1227] On l'a vu en matière de santé, bien-être et performance, que même sans être des « dispositifs médicaux » abondent désormais les bases avec des données qualifiées « de santé, *supra*.

[1228] Bernheim-Desvaux S., « L'objet connecté sous l'angle du droit des contrats et de la consommation », Contrats, conc., consomm. 2017, étude n° 1).

[1229] Proposition de Règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE)2019/1020, COM(2022) 454 final.

[1230] Du fait que (Consid. 7) « *tous les produits comportant des éléments numériques intégrés ou connectés à un système d'information électronique plus vaste* ***peuvent servir de vecteur d'attaque*** *pour des acteurs malveillants. En conséquence, même le matériel et les logiciels considérés comme moins critiques peuvent faciliter une première compromission d'un appareil ou d'un réseau, permettant à des acteurs malveillants* ***d'obtenir un accès privilégié à un système ou de se déplacer latéralement entre différents systèmes*** **».**

[1231] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº526/2013 (règlement sur la cybersécurité).

1. Les incriminations existantes en droit pénal en cas d'atteintes aux STAD

Les cyberattaques qui nous intéressent ici relèvent des **infractions à portée systémique** : celles qui visent les STAD, au sens virtuellement élargi donc par la proposition de règlement de 2022.
Les autres attaques, qui consistent en l'atteinte aux biens ou en l'usurpation d'identité etc. [1232], et qui peuvent s'appliquer aux personnes tant morales que physiques, ne sont certes pas moins délétère [1233]. Mais en l'état des techniques, elles sont encore à portée collective limitée (une portée sélective parfois suffit), bien que des outils d'intelligence artificielle pourraient permettre le **déploiement massif d'actions sélectives**… ce qui n'est plus un oxymore : la distinction sélectif vs. massif est donc provisoire. Nous concentrons ici l'attention sur les **infractions visant les STAD, et leur dynamique**.

Les infractions d'atteinte aux STAD ont été créées en 1988, par la loi dite « Godfrain » [1234]. Depuis, les attaques contre les systèmes d'information ont fait l'objet en 2013 d'une directive européenne [1235] : elle visait notamment **à rapprocher le droit pénal des Etats membres, en ce qui concerne la définition et la sanction des infractions** : accès illégal à des systèmes d'information (article 3), atteinte illégale à l'intégrité d'un système (article 4), atteinte illégale à l'intégrité des données (article 5), interception illégale (article 6).

Ainsi, dans le titre II du livre III de sa partie législative « *Des crimes et délits contre les biens* », le Code pénal français comprend un chapitre III dédié aux « *atteintes aux systèmes de traitement automatisé de données* » (articles 321-1 à 323-8 CP). Il est inutile de le paraphraser ; pour partie modifiées en 2023, ses dispositions peuvent être présentées en tableau : on y constatera que les infractions au delà de l'accès initial **relèvent de peines cumulatives, car ces délits sont subséquents** au délit d'accès ou de maintien dans le STAD.

[1232] Cas de fraude à la sécurité sociale, par obtention de prestations indues sur base d'états de santé falsifiées ; cas de détournement de remboursements après capture d'identités réelles, auxquelles sont associés des états de santé non fictifs ; cas d'induction de décisions privées ou publique biaisées (crédit, travail, logement etc.) sur la base d'états frauduleusement modifiés.
[1233] Rappelons aussi les cas précités, certes marginaux, d'attaques individuelles de dispositifs médicaux à fin de piratage de données ou de préjudice physique.
[1234] Loi nº 88-19 du 5 janvier 1988 relative à la fraude informatique ; sur l'état d'alors du droit, voir P.A. Weil, « État de la législation et tendances de la jurisprudence relatives à la protection des données personnelles en droit pénal français », Rev. Int. Dr. comp.1987, 39-3, pp. 655-675.
[1235] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

Infraction	Peine encourue depuis janvier 2023 [1236]	Peine encourue avant 2023	Fondement CP
Accès ou maintien frauduleux dans tout ou partie d'un STAD	Trois ans d'emprisonnement et amende de 100 000 €. Lorsqu'il en est résulté **soit la suppression ou la modification de données contenues dans le système, soit une altération de son fonctionnement,** cinq ans d'emprisonnement et amende de 150 000 €. Si à l'encontre d'un STAD à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende.	**Deux ans et 60 000** € Trois ans et 100 000 € Cinq ans et 150 000 €	**article 323-1**
Entraver ou fausser le fonctionnement d'un STAD	Cinq ans et 150 000 € Si à l'encontre d'un STAD à caractère personnel mis en œuvre par l'Etat, sept ans et 300 000 €		**article 323-2**
Introduire frauduleusement des données dans un STAD	Cinq ans et 150 000 € Si à l'encontre d'un STAD à caractère personnel mis en œuvre par l'Etat, sept ans et 300 000 €		**article 323-3**
Extraire, détenir, reproduire, transmettre frauduleusement les données que contient un STAD	Cinq ans et 150 000 € Si à l'encontre d'un STAD à caractère personnel mis en œuvre par l'Etat, sept ans et 300 000 €		
Détériorer, supprimer ou modifier frauduleusement les données que contient un STAD	Cinq ans et 150 000 € Si à l'encontre d'un STAD à caractère personnel mis en œuvre par l'Etat, sept ans et 300 000 €		**article 323-3**

Par ailleurs, la loi a introduit **la sanction du fait, «** ***sans motif légitime, notamment de recherche ou de sécurité informatique,*** *d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée* ***conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions*** » (article

[1236] Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur.

323-3-1, inchangé depuis 2013) [1237]. Cette infraction a été contestée, ayant parfois servi à la poursuite judiciaire de publications sur des failles de sécurité : c'est pourquoi a été ajouté l'exception du « motif légitime » (mais ce motif ne s'y réduit naturellement pas) [1238].

Outre ces infractions, **leur préparation collective est incriminée** : ainsi « *la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels (etc)* » (article 323-4, inchangé depuis 2004). Mais **depuis 2023 seulement, leur commission « en bande organisée »** donne lieu à une majoration à dix ans d'emprisonnement et 300 000 € d'amendes (article 323-4-2) [1239].

De même, lorsque cette commission des infractions a « *pour effet d'exposer autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente ou de faire obstacle aux secours destinés à faire échapper une personne à un péril imminent ou à combattre un sinistre présentant un danger pour la sécurité des personnes* » (323-4-2). **Mais cette circonstance aggravante ne vise pas spécifiquement les STAD de santé**, et ne s'appliquerait pas à toutes leurs attaques.

Enfin, relevons que depuis 2015, ces dispositions « ***ne sont pas applicables aux mesures mises en œuvre, par les agents habilités des services de l'Etat*** *désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement (…) pour assurer* ***hors du territoire national*** *la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code* » (article 323-8, créé en 2015, non modifié).

Cela implique **que ce mode d'action peut appeler des actions de contre-ingérence de la part de tels services,** mais que celles-ci ne devraient pas être appliquées sur le « territoire national », *infra*.

2. Le défi de l'attribution des ingérences relevées dans les STAD

« *Qui* » se cache derrière la cyberattaque ? La question est justifiée dans une double perspective : judiciaire (punition de comportements, réparation de dommages), et d'éventuelles contre-mesures, hors de la compétence juridictionnelle de droit commun.

[1237] Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[1238] En revanche, selon la Cour de cassation, « *les atteintes aux systèmes de traitement automatisé de données prévues aux articles 323-1 à 323-3 du code pénal ne sauraient être reprochées à la personne qui, bénéficiant des droits d'accès et de modification des données, procède à des suppressions de données, sans les dissimuler à d'éventuels autres utilisateurs du système* » Crim. 7 janvier 2020, n° 18-84.755, publié au Bulletin.
[1239] Loi n° 2023-22 du 24 janvier 2023 préc.

* On écartera rapidement la dimension organique, policière et judiciaire [1240]. Au plan national, ces aspects ont, entre autres, appelé la spécialisation de services d'enquête : ainsi, au sein de la direction centrale de la police judiciaire, la sous-direction de lutte contre la cybercriminalité (SLDC) ; l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), et des brigades spécialisées [1241].

En matière de procédure pénale, le législateur a créé dans le code un titre XXIV : « *De la procédure applicable aux atteintes aux* (STAD) », et a centralisé à Paris en 2016 une **compétence concurrente nationale en matière d'atteintes aux STAD** [1242]. Les magistrats spécialisés sont formés et interagissent avec en amont notamment l'ANSSI, pour caractériser et cerner l'ampleur des dommages créés par une ingérence, identifier et retracer ses modalités, localiser son origine.

Au plan européen et au-delà, nous avons relevé la directive de 2013. Outre l'harmonisation de la définition et de la sanction des infraction, cette directive vise à **renforcer la coopération entre autorités compétentes**, il n'est pas lieu ici de développer ce point [1243]. Notons seulement que l'ENISA est aussi une structure sollicitée en ce sens (depuis sa création, *a fortiori* depuis son renforcement en 2019), sachant la forte implication pour la coopération internationale, des services dédiés à la cybercriminalité d'EUROPOL et d'INTERPOL. On reviendra sur cette articulation, *infra*.

* Or, les mêmes questions d'attribution se posent en amont des **actions étatiques de cyber contre-ingérence, non nécessairement reliées à une procédure judiciaire [1244]**. Elles ne se posent pas moins dans l'hypothèse d'éventuelles actions privées dites *hack-back* (qui ne bénéficient pas d'une telle exonération en droit pénal). Ces dernières consistent en ce que qu'« *un acteur privé (mène) des actions cyber offensives en réponse à une attaque dont il*

[1240] V. Bensoussan-Brulé, « Focus : le traitement juridique et judiciaire des cyberattaques », mai 2021 et les réf citées ; Club des juristes, « Le droit pénal à l'épreuve des cyber attaques », avr. 2021, et bibliographie.
[1241] Brigade de lutte contre la cybercriminalité (BLCC), anciennement Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) – elle a absorbé le groupe de La Brigade des fraudes aux moyens de paiement (BFMP) ; Brigade de répression de la délinquance astucieuse (BRDA) pour certaines pratiques en ligne ; Brigade de protection des mineurs ; Brigade de répression de la délinquance envers la personne (BRDP) ; Centre de lutte contre les criminalités numériques (C3N) ; et, auprès de la direction nationale du renseignement et des enquêtes douanières (DNRED), le Service des cyberdouanes (dit « cellule Cyberdouane ») etc.
[1242] Au profit du procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris (article 706-72-1 du Code de procédure pénale).
[1243]Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.
[1244] Exonérées de l'application du droit pénal pour leur conduite **hors territoire national** (art. 323-8 préc.).

serait victime » [1245], ou pour le compte de la victime. Promues dans d'autres pays [1246], considérées illégales en France [1247], ces actions **supposent partout l'attribution certaine à un tiers « ingérant »,** et une réaction qui l'affecte de façon effective.

Dans ce contexte, qu'il soit judiciarisé ou non, le problème commun est d'ordre technique : la caractérisation, traçabilité, localisation et imputation des actes etc. [1248] et leur preuve légalement recevable sachant les obstacles juridiques dressés par la subtilité parfois des APT. Les « groupes » parfois identifiés peuvent être déférés devant la justice pénale nationale, mais sans actions en l'état devant une juridiction de compétence internationale [1249].

B. LA DIFFICULTE EN DROIT COMMUN DE « L'ATTRIBUTION » DE L'INGERENCE HORS CONFLIT DECLARE

A la supposer distinguable d'une criminalité de droit commun, sous laquelle elle peut (aisément et volontiers, si rémunératrice) se dissimuler [1250], l'ingérence étatique dans les STAD soulève parfois d'importants problèmes pour l'application du droit / pour des mesures de rétorsion. Cela même si l'attribution était certaine.

Observée depuis quelques années, la pratique massive parfois à haute intensité de telles ingérences, appliquées à un pays comme cible, permet d'affirmer qu'elles **sont rattachables « *désormais au répertoire d'action des Etats* »** [1251], distinctement d'autres pratiques historiquement identifiées et formellement interdites [1252].

[1245] SGDSN, Revue stratégique de cyberdéfense, 12 février, 2018, p. 88.

[1246] Pour les arguments en présence, voir K. Bannelier et T. Christakis, *Cyberattaques – Prévention-Réactions : Rôles des États et des acteurs privés*, *Les Cahiers de la Revue Défense Nationale*, Paris, 2017 ; W. Hoffman, A.E. Levite « Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace ? », 14 juin 2017, Rapport pour Carnegie Endwment for international Peace.

[1247] Position du SGDSN, in *Revue stratégique de cyberdéfense*, 12 février, 2018 préc. ; K. Bannelier, T. Christakis, « Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la Revue Stratégique de cyberdéfense de la France et le projet de loi ACDC aux Etats-Unis », Rev. Stratégique 2017/4 n°117, pp 99-118.

[1248] Signalons entre autres les difficultés naissant de la pratique du *spoofing* (usurpation de l'adresse IP source) : un serveur a pu faire l'objet d'une compromission et être soupçonné ; de la pratique du « rebond » de serveur en serveur, laquelle ne permet pas de localiser l'origine de l'attaque, etc. Voir les podcasts didactiques proposés sur https://technique-et-droit-du-numerique.fr/attribution-des-cyber-attaques-podcast/

[1249] Sur ces questions d'impact en droit international et sur les relations internationales, spéc. Buzatu AM, « 15 - Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace », Cambridge Press en ligne (21 avril 2022).

[1250] Par demandes de rançon, revendications déceptives, leurres techniques divers etc. On verra dans l'affaire NotPetya en 2017 que sous couvert de *ransomware*, le but était la destruction des données, même rançon payée.

[1251] S. Taillat, « Un mode de guerre hybride dissymétrique ? Le cyberespace», éditions Institut de Stratégie Comparée, 2016/1 (n°111), p. 89-106.

[1252] Ainsi les éventualités d'« intervention indirecte » : les Etats doivent de **s'abstenir de favoriser, d'encourager ou d'appuyer tout désordre ou trouble dans un autre Etat** ; une conséquence formelle est que

Or, il en découle une **extension potentielle de la notion juridique « d'agression » au sens du droit international public** [1253]. Jusqu'alors, cette notion était cantonnée aux conflits armés caractérisés par la violence physique provoquées par des moyens physiques, sur un ou des territoires circonscrits. L'hybridation des conflits a ainsi complexifié leur nature, et rend leur qualification parfois complexe (mais la pudeur n'est plus de mise dans la dénonciation [1254]).

Mais massive ou sélective, la **pratique de telles cyber ingérences ne se limite pas aux situations de conflits armés territoriaux**, et parfois même ne les suppose pas. Cela rend notamment le droit de la guerre inopérant, sachant sa portée souvent limitée à la dénonciation d'une infraction (en attendant que le sort des armes parfois détermine la compétence juridictionnelle). Dès lors, certains auteurs invoquent le droit international humanitaire en complément ou substitut de ce droit, quand les conditions d'application de ce dernier ne sont pas réunies [1255] : le DIH interdit les attaques indiscriminées touchant notamment les civils [1256]. Pour une approche plus large, on se référera à l'étude approfondie et autrement référencée (lien APT / droit international), de madame Buzatu, qu'il n'est pas lieu de paraphraser [1257].

Or, à supposer une improbable autolimitation de l'attaquant des données, STAD et réseaux, cela ne règle pas la question de l'attribution. **Le défaut de réunion des conditions formelles et/ou matérielles de qualification de l'attaque** quand elle s'exprime essentiellement en champ cyber (1), **conduit à considérer un autre fondement de l'action** (2).

---

les activités des agents diplomatiques ne doivent pas constituer une intervention indirecte dans les affaires internes de l'Etat accréditaire (art. 41 §1 *in fine*, Convention de Vienne sur les relations diplomatiques, 1961).

[1253] Skoze-Pellet V., *Les cyberattaques étatiques et la notion d'agression en droit international*, Mémoire de Master 2, U. Aix Marseille, Droit. 2018. dumas-02089316 (2019).

[1254] Voir les visas de la Résolution du Parlement européen du 18 janvier 2023 sur la mise en œuvre de la politique de sécurité et de défense commune – rapport annuel 2022 (2022/2050 (INI)).

[1255] C. Bories, « Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point », Rev. dr. homme 2014, n°5 ; *comp*. L. Gisel, « Le droit de la guerre impose des limites mêmes aux cyberattaques », 17 janv. 2013, site CICR.

[1256] CICR, (article) « Appel pour mettre fin aux cyberattaques contre le secteur de la santé », 27 mai 2020 ; (article) « Le droit international peut-il limiter la cyberguerre ? », 25 fév. 2021 ; (déclaration) « Pirater les données des personnes les plus vulnérables est un affront à l'humanité », 29 janv. 2022 ; (communiqué) Le CICR ouvre au Luxembourg un bureau dédié au cyberespace », 17 nov. 2022.

[1257] Buzatu A-M, « 15 - Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace », in *Cyber Pease, Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge U Press, 2022.

1. L'élision de la qualification « risque de guerre » pour l'ingérence : la jurisprudence américaine NotPetya de 2021

En 2017, est survenue l'attaque informatique « *NotPetya* ». Cette attaque n'était pas une *Advanced Persistant Threat (supra)*, mais une attaque de logiciel malveillant de type rançonnage (*ransomware)*. Initiée en Ukraine, où elle a infecté un logiciel de comptabilité largement utilisé, elle a eu un impact mondial, du fait de sa propagation aux réseaux d'entreprises, selon une technique similaire à celle du programme *WannaCry* porté par le « *Lazarus Group* » préc. associé à l'APT38 liée à la Corée du Nord [1258].

Les experts en sécurité informatique ont établi des liens entre *NotPetya* et un groupe de pirates informatiques connu sous le nom *Sandworm Team*, qui aurait des liens avec les services de renseignement militaire russes, sachant que le gouvernement russe nie toute implication [1259]. Des recherches ont également suggéré que l'attaque avait pour objectif de perturber les infrastructures et de saboter l'économie ukrainienne. Cependant, l'attaque s'est rapidement propagée à l'échelle mondiale, ce qui en fait l'une des attaques informatiques les plus destructrices de l'histoire.

Chiffrant les données des systèmes qu'il avait infectés, *NotPetya* exigeait le paiement d'une rançon pour les récupérer. Mais contrairement à d'autres logiciels de rançonnage, *NotPetya* **était conçu pour détruire les données, non simplement les chiffrer** : la récupération des fichiers était impossible, même après le paiement de la rançon.

En conséquence, *NotPetya* a causé plusieurs milliards de dollars de dommages, et affecté de nombreuses organisations et entreprises dans des secteurs comme la finance, les transports, l'énergie, **et spécialement la santé : hôpitaux, cliniques et entreprises pharmaceutiques**. En Ukraine, premier pays infecté, puis aux Etats-Unis etc., les hôpitaux ont ainsi été

[1258] BBC, « WannaCry ransomware cyber-attacks traced to North Korea », (https://www.bbc.com/news/technology-42193009) ; Wired, « The WannaCry Ransomware Has a Link to Suspected North Korean Hackers » (https://www.wired.com/story/wannacry-ransomware-north-korea-lazarus-group/) ; Forbes, « WannaCry Hackers Linked To North Korea In New Report » (https://www.forbes.com/sites/thomasbrewster/2017/06/14/wannacry-hackers-linked-to-north-korea-in-new-report/) ; Rapport du National Cyber Security Centre britannique : « WannaCry ransomware outbreak » (https://www.ncsc.gov.uk/report/wannacry-ransomware-outbreak).

[1259] The Guardian, « NotPetya: how Ukraine's most devastating cyberattack unfolded », The Guardian, 2017, https://www.theguardian.com/world/2017/jun/28/notpetya-cyber-attack-ukraine-russia-what-is-wannacry ; ZDNet, « NotPetya ransomware attack: What is it, how it started, who is responsible and more », ZDNet, 2017, https://www.zdnet.com/article/notpetya-ransomware-outbreak-chaos-reigns-supreme-in-ukraine/; TWP, « Russian hackers are accused of a massive, devastating cyberattack », The Washington Post, 2018, https://www.washingtonpost.com/world/national-security/russian-hackers-are-accused-of-a-massive-devastating-cyberattack-heres-what-you-need-to-know/2018/02/15/9c2d2934-11f0-11e8-8ea1-c1d91fcec3fe_story.html

particulièrement affectés, imposant interruption de services, report d'opérations, déplacement de patients, destruction de données des dossiers médicaux électroniques, destruction des dossiers de paiement, etc [1260] avec notamment des conséquences humaine dramatiques.

Mais c'est des Etats-Unis, que vient la jurisprudence emblématique du problème de la qualification. Fortement touché par NotPetya, le groupe pharmaceutique Merck a vu son système hors services durant des jours, avec des **effets systémiques sur la production et la mise à disposition des médicaments notamment**.

* Merck a réclamé à ses assureurs la couverture des pertes financières et frais de restauration de ses systèmes informatiques. **Les assureurs ont refusé de couvrir le dommage, affirmant que l'attaque était une « *opération hostile ou un acte de guerre* » ; que, par conséquent,** ses conséquences ne pouvaient bénéficier de la couverture par la police d'assurance de Merck. En 2019, Merck a saisi la juridiction américaines compétente.

* En mars 2021, la justice américaine a statué en faveur de Merck : au fond et en appel, les juges ont considéré que l'attaque NotPetya **n'était pas une « *opération hostile ou un acte de guerre* »** au sens de la police d'assurance de Merck ; que, par conséquent, les assureurs étaient tenus de couvrir les pertes subies et frais supportés par Merck [1261].

Dans cette affaire, le tribunal a décidé que les assureurs ne peuvent se prévaloir de la « *clause d'exclusion de guerre* », pour refuser leur couverture suite à une cyberattaque. **Outre son impact potentiel sur la rédaction des clauses des police d'assurance**, la généralisation d'une telle solution jurisprudentielle a elle-même des conséquences systémiques sur la responsabilité contractuelle, la responsabilité extracontractuelle, le marché de l'assurance et naturellement la protection des données, outre le débat sur les relations internationales et le droit international public on l'a vu.

[1260] Barrett B, « Petya Ransomware: What You Need to Know », Wired, 27 juin 2017, https://www.wired.com/story/petya-ransomware-what-you-need-to-know/ ; Sanger D.E et Perlroth N, « Hospitals Wrestle With Unprecedented Cyber Assault », The New York Times, 28 juin 2017, https://www.nytimes.com/2017/06/28/technology/ransomware-hospitals-wanna-cry-attack.html ; Sutner S, « Cyberattack on Medical Devices Shows Healthcare Industry's Vulnerability », TechTarget, 11 juillet 2017, https://searchhealthit.techtarget.com/news/450422835/Cyberattack-on-medical-devices-shows-healthcare-industrys-vulnerability ; Bowen C, « WannaCry, Petya and MEDoc: lessons for healthcare », SC Media, 9 août 2017, https://www.scmagazine.com/home/security-news/cybercrime/wannacry-petya-and-medoc-lessons-for-healthcare/

[1261] Merck & Co. Inc. et al. v. Insurers of Merck & Co. Inc., United States District Court for the District of New Jersey, Case No. 2:19-cv-01913 (WJM) (MAH), déposé le 20 mai 2019 ; Opinion du tribunal dans l'affaire Merck & Co. Inc. et al. v. Insurers of Merck & Co. Inc., 2021 WL 1054337 (D.N.J. Mar. 19, 2021).

Depuis 2020, le contexte n'est pas celui de 2017 : il est marqué par un agression de l'Ukraine par la Russie. Mais

* aucun équivalent de l'attaque NotPetya (destruction plutôt que restitution des données, après paiement de rançon) n'a depuis été répertorié à cette échelle [1262] : lorsque le but final de destruction est avéré, un tel mode opératoire ne peut qu'enrayer le paiement des rançons, donc tarir la source de revenu (voire d'informations [1263]) des acteurs cybercriminels et de leurs commanditaires.

* bien qu'aucune juridiction n'ait été saisie, à notre connaissance, d'un contentieux équivalent à celui généré par l'attaque NotPetya, l'élision (action d'éluder) soigneuse, dans la guerre Ukraine - Russie, de co-belligérance formelle, **conduit ici à nouveau à écarter la « clause d'exclusion de guerre »**. Mais un élément a changé, du fait de la nature des parties impliquées, et de leur possible qualification sur un fondement nouveau.

2. Les conséquences de la qualification « terroriste » pour l'ingérence : quel droit applicable ?

Si l'on écarte l'hypothèse NotPetya pour les motifs précités, et l'actions d'APT dont le but n'est pas la rançon, il reste ici à traiter du régime du paiement éventuel de rançons aux acteurs de l'ingérence, sachant le **secteur de la santé spécialement vulnérable et visé**, *supra* : cette question est essentielle, car selon que la rançon est payée ou non, assurable ou pas, le « signal » envoyé à l'écosystème criminel est clair.

En outre, **la propagation transnationale rapide** par des vecteurs de type WannaCry (*supra*) **invite à une réflexion conjointe des Etats** dans la recherche de garanties coordonnées, contre une tradition de susceptibilité ombrageuse dans un champ typiquement souverain.

Dans ce contexte, il existe des contrats d'assurance proposant de protéger les entreprises et organisations [1264] contre les risques cyber (dont les frais de gestion de crise, notification et surveillance, enquête, reconstitution de systèmes et de données, pertes d'exploitation, conséquences de recours de tiers victimes pour réparation des préjudices, les frais procéduraux, etc.). *Quid* des rançons demandées par les cybercriminels (éventuellement pour leurs commanditaires) ?

1262 Voir les rapports ANSSI et ENISA préc**.**

1263 La corruption des fichiers et systèmes infectés par les *ransomware* reste fortement probable.

1264 Lorsque l'Etat n'est pas son propre assureur.

En 2021, la proposition dans les contrats du paiement de rançon a été dénoncée par le Parquet de Paris et par l'ANSSI devant le Sénat français, comme stimulant les cyberattaques. Cette analyse a été relayée par le Sénat [1265] et à l'Assemblée nationale, où un rapport a proposé d'*« inscrire dans la loi l'interdiction pour les assureurs de garantir, couvrir ou (indemniser) la rançon »* [1266]. Le détail des arguments en présence a été l'objet en 2022 d'un panorama approfondi sous l'égide du HCJP [1267], qui en développe de nombreux aspects.

Dans le sillage de nos commentaires de l'affaire NotPetya *supra*, ce qui nous intéresse ici est le **rapport entre le paiement et le financement du terrorisme**, car le contrat d'assurance doit respecter l'ordre public et les « bonnes mœurs » [1268], comme tout autre contrat [1269]. Si ce défi n'a pas donné lieu à jurisprudence en matière de paiement de rançons, il est considéré acquis que l'*« assurance d'un risque purement pénal est illicite en tant que telle et* ***que celles des autres risques est illicite à deux conditions alternatives :*** *qu'un texte spécial le prévoie ou que la garantie ait directement pour objet une activité elle-même illicite »* [1270].

Or, tant qu'aucun texte ne prévoit l'interdiction du paiement de la rançon (et le paiement au *hacker* ne constituant pas en soi une activité illicite), le paiement ne tombe pas sous le coup de la loi. D'autre part, à moins d'une collusion frauduleuse avec le *hacker*, l'assuré est une victime : on ne saurait reprocher une faute intentionnelle ou dolosive (laquelle faute ne serait pas un aléa, article L. 113 Code Ass.). Enfin, on ne saurait lui reprocher un paiement sous contrainte, dont l'exigence correspond au délit d'« extorsion » (article 312-1 Code Pénal).

Dans ce contexte, quel impact de la question de l'attribution de l'ingérence ?

* En droit français, la connaissance du fait que les fonds fournis sont « *destinés à être utilisés en tout ou partie, en vue de commettre un (acte de terrorisme)* » est constitutif de l'infraction de financement de terrorisme (article 421-2-2 du Code pénal). Une telle poursuite suppose que l'organisation victime savait qui a demandé le paiement ; mais, même cette connaissance

[1265] Rapport d'information du Sénat du 10 juin 2021, n°678 « La cybersécurité des entreprises – Prévenir et guérir : quels remèdes contre les cyber virus ? ».
[1266] Mme Faure-Mutian V (groupe d'études Assurance), Rapport à l'Assemblée octobre 2021 dédié à la Cyber assurance, non autrement référencé.
[1267] Haut Comité Juridique de la Place financière de Paris, 28 janvier 2022, « Rapport sur l'assurabilité des risques cyber ».
[1268] Régi par l'article L. 113-1 du Code des assurances, mais aussi par le droit commun des articles 6 (pas de dérogation à l'ordre public), article 1102 (*idem*) et 1162 du Code civil (*idem*, que le but soit connu ou non).
[1269] CA Paris, 14 février 2012, n° 09/06711.
[1270] Mayaux L, « Assurance et ordre public : à la recherche d'un critère », RGD Ass 2008, n°3.

n'exclut pas l'invocation d'une contrainte exonératoire de la responsabilité pénale (article 122-2 du Code pénal) : le caractère irrésistible de cette contrainte **peut être soutenu par les opérateurs de services d'importance vitale ou essentielle, dont notamment les hôpitaux**.

Pas plus, le paiement de la rançon ne saurait être en soi reproché à un assureur (à l'instar de la couverture assurantielle du risque de vol ou de destruction), d'autant qu'il verse la somme **non à l'agresseur, mais à la victime** qui verse à l'agresseur. Mais la question peut être posée, **selon la connaissance détenue sur l'attaquant** après enquête, en amont du paiement.

Or, le Code monétaire et financier enjoint aux secteur financier (banque et assurance) de ne procéder à aucune opération sur des sommes « *dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou sont liées au financement du terrorisme* » (article L. 561-15 CMF) ; la réalisation est subordonnée à l'absence d'opposition [1271].
Si cette obligation de vigilance renforcée a été conçue hors de l'optique de l'ingérence ici étudiée, celle-ci (dont le vol de données personnelles) entre *de facto* dans les critères issus de la typologie des financements du terrorisme [1272], **et a déjà été mise en œuvre en cas de cyber attaque (prétendue)** [1273].

De même, les acteurs du secteur financier doivent respecter les sanctions prononcées au plan national, européen et international contre des personnes morales ou physiques dont les avoirs peuvent avoir être gelés par mesures judiciaires voire exécutives [1274]. En 2020, le dispositif a été renforcé [1275]. **Il en résulte une obligation de résultat, qui remet en exergue l'attribution des cyber attaques comme fondement de l'application de ces règles**.

D'autres Etats, comme notamment les Etats-Unis, ont adopté des dispositions similaires, avec des règles de portée extraterritoriale, **qui fixent leur propre liste nationale des entités sanctionnées** (incluant des personnes physiques et des gouvernements dont certains associés

[1271] Opposition notifiée par Tracfin, ou au terme du délai de cette notification, décidée par le président du tribunal judiciaire de Paris.
[1272] Lignes directrices (5 nov. 2018) TRACFIN / ACPR sur les obligations de déclaration et d'information à TRACFIN.
[1273] Rapport d'activité TRACFIN 2019 ; suite au signalement par un prestataire de services sur actifs numériques (PSAN), de l'acquisition par un dirigeant d'entreprise pour le paiement face à un logiciel de rançonnage, de 5,35 bitcoins (équiv. alors de 50000 euros).
[1274] Registre des entités concernées accessible sur : https://gels-avoirs.dgtresor.gouv.fr/
[1275] Ord. n°2020-1342 du 4 nov. 2020 renforçant le dispositif de gel des avoirs et d'interdiction de mise à disposition.

à des APT, dont l'APT38) vers lesquelles des versements sont susceptibles de poursuite judiciaire [1276]. Cette liste a été fortement élargie depuis l'agression russe en Ukraine, sans changer la qualification géopolitique, laquelle ne relève pas de la guerre au sens des clauses d'exclusion de couverture assurantielle [1277]. **Cela confirme le renouvellement profond des procédés d'ingérences et des réponses souveraines dans le champ géopolitique.**

* En matière de souveraineté justement, se pose la question de l'opportunité d'un texte européen sur la question [1278]. L'approche dispersée de législations nationales (autorisant ou interdisant le paiement de rançon, **indépendamment du raisonnement qui précède et qui suppose une attribution à des acteurs « listés »**), pourrait induire des distorsions de concurrence dans le marché intérieur.

Or, il n'apparaît pas impossible en droit européen, qu'un Etat membre **puisse édicter une interdiction plus large**, que celle de posture commune (mais alors au « détriment compétitif » des organisations / entreprises relevant de sa compétence) [1279] ; **ni que l'Union puisse elle-même légiférer**, pour une approche unifiée : l'« *exercice par l'UE de sa compétence vis-à-vis d'un texte européen visant à interdire l'assurabilité des rançons en cas de cyber attaque »* fait l'objet d'une réflexion approfondie [1280], pour l'instant sans suites européennes.

D'éventuelles suites pourraient cristalliser les questions de qualification.

Compte tenu de cette complexité surajoutée, la priorité est la prévention, laquelle suppose à nouveau que dans des **matières hautement régaliennes de sécurité**, les Etats procèdent sous l'égide de l'Union à la recherche de nouvelles garanties coordonnées contre l'ingérence. Nous allons maintenant en constater l'accélération.

[1276] Aux Etats-Unis, le paiement d'une rançon est illicite s'il viole la réglementation de *l'Office of Foreign Assets Control* (OFAC). L'OFAC a en 2020 signalé le risque de sanction encourue par des entreprises qui pourraient envisager un paiement, du fait notamment qu'il serait couvert par leur assurance (voir la jurisprudence NotPetya), vers des entités sanctionnées**.** Voir OFAC, Département du trésor, « The treasury 2021 sanctions review ».

[1277] Gonzalez R, Thompson J, « Sanctions Recent Developments in U.S. Sanctions: Russia Sanctions, OFAC Enforcement Trends, and Compliance Lessons Learned 2023 », ICLG, publié 30 sept. 2022.

[1278] HCJP, Rapport sur l'assurabilité des risques cyber » 28 janvier 2022.

[1279] Rapport HCJP préc. 2022, page 34.

[1280] Rapport HCJP 2022 préc., voir annexe VII, pages 83 à 89, spéc. page 87.

SECTION 2. RECHERCHE DES GARANTIES COORDONNEES FACE AUX INGERENCES : QUELLE ACCELERATION ?

Nous venons de relever des ingérences croissantes dans les STAD notamment de données de santé, et quelques-uns des problèmes de qualification posés, que le champ soit judiciarisé ou non. Ces questions d'attribution, durablement problématiques, postulent la réalisation de l'ingérence ; son évitement est œuvre à la fois d'éducation et d'organisation, et d'anticipation **pour l'harmonisation voire l'unification normative qui seules nous intéressent ici**.

Dès 1995, des bases communes d'une protection ont été invoquées au niveau européen par la directive 95/46/CE [1281], selon laquelle les « ***États membres doivent veiller à ce que le responsable du traitement mette en œuvre*** *les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés (...) »* (article 17§1 de la directive 95/46).

En 2002, la directive 2002/21/CE relève alors que la **garantie de l'intégrité et de la sécurité des réseaux, comme la protection des données personnelles, relèvent essentiellement des autorités nationales**, qui doivent « *coopérer entre elles et avec la Commission* » [1282]. Cette obligation faite aux Etats est devenue une obligation faite aux responsables des traitements (articles 5§1,f et 24 du RGPD), pénalement et administrativement sanctionnée en droit français, nous l'avons vu *supra*.

Ainsi énoncé en matière de données personnelles (le point de départ était jusqu'alors les droits fondamentaux), le souci s'est étendu : sécurité, intégrité structurale et fonctionnelle des STAD, organismes de services essentiels (OSE), puis réseaux de tous secteurs dont commerce, communication, services etc., selon alors une dynamique en « mille-feuilles » [1283].

1281 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

1282 Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre")

1283 Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ; Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») ; Directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive "accès") ;

Accélérons : en 2004, l'**Agence européenne chargée de la sécurité des réseaux et de l'information** (ENISA) est crée par règlement [1284], de façon alors provisoire, *infra*. En 2013, la Commission publie sa « *stratégie sur la cybersécurité* » [1285], saluée comme « *la première déclaration d'une cyberstratégie européenne autonome* », dans un domaine où l'Union était jusqu'alors en retrait [1286]. Elle a été récemment renouvelée[1287].

Or, de façon emblématique, elle est alors **placée sous le signe de l'article 222 TFUE qui porte « *clause de solidarité* » pour prévenir, protéger et assister face aux risques terroriste,** de catastrophe naturelle ou d'origine humaine [1288], à distinguer du focus de la « cyberdéfense » [1289]. Bien que le contexte géopolitique se soit crispé, et les modes d'action illicite précités développés (sans toujours être attribuables), cet article sera peu invoqué. Il s'agit en effet d'un **fondement d'action circonstancielle, non en soi d'un fondement d'action normative** (à la différence des articles 114 et 173 TFUE).

Directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive "autorisation").
Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre") ; Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive "service universel") ; Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ; Résolution du Parlement européen sur la communication de la Commission "eEurope 2005: une société de l'information pour tous" (Plan d'action à présenter en vue du Conseil européen de Séville des 21 et 22 juin 2002) 2022/2242 (INI) ; Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information ; Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.

[1284] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information ; pérennisée par Règlement (UE) no 526/2013.

[1285] **C**ommunication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, 7 février 2013, JOIN/2013/01 final.

[1286] O. Kempf, « La cyberstratégie de l'Union européenne », Sécurité Globale 2013/2 n°24, 25-40.

[1287] Communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité du 16 décembre 2020 intitulée «La stratégie de cybersécurité de l'UE pour la décennie numérique » (JOIN(2020)0018).

[1288] Introduit par le Traité de Lisbonne, TFUE, article 222§1 : « *L'Union et ses États membres agissent conjointement dans un esprit de solidarité si un État membre est l'objet d'une attaque terroriste ou la victime d'une catastrophe naturelle ou d'origine humaine. L'Union mobilise tous les instruments à sa disposition, y compris les moyens militaires mis à sa disposition par les États membres, pour (…) ».*

[1289] D. Deschaux-Dutard, « L'Union européenne, une cyberpuissance en devenir ? Réflexion sur la cyberdéfense européenne », Rev. Int. et Strat. 2020/1 n°117, 18-29 ;

Nous en resterons à notre fil rouge des « *données de santé* ». Dans ce contexte, avivé par l'agression en 2022 de la Russie contre l'Ukraine [1290], mais lancinant bien avant nous l'avons vu, relevons ici des points emblématiques d'une **double accélération sous l'égide de l'Union.** Nous l'esquisserons en matière de règles de fond avec un focus sur les conséquences en santé (§1) ; puis, ouvrant le champ au-delà, en matière de règles de compétence (§2).

§1. DYNAMIQUE DES REGLES COMMUNES DE FOND POUR LA CYBERSECURITE EN SANTE

Ce qui nous intéresse ici, est **l'élargissement du champ dans le domaine typiquement régalien et l'accélération de l'adoption de ces règles**. Ils sont motivés, tant par la diversification et la diffusion exponentielle des technologies du traitement automatisé de l'information, que par le développement corrélatif d'une menace par des outils nouveaux d'une géopolitique sous tension (l'apparition de nouveaux outils pouvant contribuer à la tension, laquelle était relativement contenue sans eux).

Tout comme le partage des données de santé était un but préexistant à la pandémie, laquelle en a accéléré la réalisation, nous allons voir que **l'objectif de sécurisation cyber des infrastructures n'est qu'accéléré par l'urgence géopolitique**. Toutefois, sur le terrain de la méthode, une approche globale (infrastructures, produits, services, processus) se substitue à l'approche ciblée, du fait du caractère systémique de la vulnérabilité ; et du fait que peut-être aussi, les règles communes sont **politiquement moins difficiles à négocier, quand l'urgence en est brutalement perçue** notamment par l'opinion publique ?
Nous limiterons notre propos en distinguant dans l'actualité récente, l'extension des normes de protection en matière **d'infrastructures (A) puis de produits connectés (B) en santé.**

A. L'EXTENSION DES NORMES COMMUNES DE PROTECTION EN MATIERE D'INFRASTRUCTURES

L'extension des garanties coordonnées pour la protection contre les cyber-ingérences dans les infrastructures d'exprime dans plusieurs champs. **A chaque fois s'y expriment des problématiques propres au secteur de la santé,** si ce n'est directement quant aux données

[1290] Si cette agression n'est pas rapportée dans les considérants mêmes, elle est développée dans les contextes et motifs, en préalable de plusieurs textes. Mais les textes eux-mêmes ne sont pas le lieu d'une « attribution ».

de santé. Ainsi sont notamment concernés les prestataires de soins et laboratoires de référence (qui génèrent et utilisent des données de santé au titre de la prise en charge des patients), comme les fabricants de médicaments et de technologies médicales (qui génèrent et utilisent les données de santé pour la R&D et pour la surveillance de leurs produits commercialisés).

Nous relevons ici le prolongement en 2022, de la première directive de 2016 dite SRI (« *sécurité des réseaux et des systèmes d'information* »), souvent appelée « NIS » (« *Network and Information Security* ». Elle a été adoptée sur le fondement de l'article 114 TFUE, lequel a pour objet la réalisation et le fonctionnement du marché intérieur. En contraste de la directive « NIS 1 » (2016), et à la lumière des expériences précitées, la directive « NIS 2 » **retient un champ plus large de criticité des infrastructures en santé** (1).

En outre, dans la même dynamique de fond, la proposition en 2023 d'un règlement de cyber-solidarité marque une approche trans-sectorielle, certes sans évocation normative de la santé. Mais il **met en exergue l'exercice du droit fondamental d'accès à celle-ci** (2).

1. L'élargissement par NIS2 en 2022 des infrastructures « hautement critiques » en santé

La directive sur la sécurité des réseaux et systèmes d'information dite « NIS 1 » a été adoptée en 2016 **sur le fondement de l'article 114 TFUE** [1291]. Son but est d'« *assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* » [1292]. A cette fin, elle a visé a créer des capacités dans toute l'Union (par l'élaboration de cadres nationaux et stratégies nationales), à atténuer des menaces sur les réseaux et systèmes d'information sous-tendant des services essentiels dans des secteurs critiques (identification des infrastructures et entités essentielles et mesures réglementaires), et à assurer leur continuité le cas échéant.

Elle a aussi montré des limites. Son réexamen a révélé **des divergences importantes dans la mise en œuvre par les Etats, notamment quant à son champ d'application :** il leur laissait une large marge d'appréciation (cf. notamment article 5 « *Identification des opérateurs*

[1291] Pour rappel, l'article 114 TFUE (ex 95 TCE) a pour objet l'établissement et le fonctionnement du marché intérieur, à distinguer de la base juridique de la stratégie de cybersécurité en 2013 (article 222 TFUE).
[1292] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

essentiels », article 7 « *Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information* » et article 16, « *Exigences de sécurité et notification d'incidents* »).
Or, **du fait des écarts nationaux entre les mesures appliquées**, il en a résulté une relative dispersion des postures dans le marché intérieur, impactant la fourniture transfrontière des services (dont de santé, *infra)*, **et la cohérence globale du dispositif de sécurisation**.

En outre et surtout ici, la directive NIS 1 ne citait, dans son annexe II (« *types d'entités aux fins de l'article 4 point 4* ») **qu'un seul « sous-secteur » pour la santé.** Il s'agit alors des « *établissements de soins de santé (y compris les hôpitaux et les cliniques privées)* », qui y sont définis comme les « *Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil* » [1293]. **Certes, cela n'empêchait pas les Etats membres d'appliquer chacun ces mesures à d'autres entités.**

Mais l'élargissement des ingérences depuis « NIS 1 », le choc systémique de la pandémie de Covid-19, et l'amplification des tensions géopolitiques (*supra*), ont conduit à **reconsidérer au plan européen les infrastructures** devant être couvertes de façon homogène par la cybersécurité.

En conséquence, une nouvelle directive « *sécurité des réseaux et systèmes d'information* » dite « NIS 2 » a été adoptée en décembre 2022, et abroge donc la précédente [1294]. Entrée en vigueur en janvier 2023, elle doit être transposée avec des dispositions nationales applicables dès le 18 octobre 2024, **ce qui montre l'urgence du sujet.**

Cette directive NIS 2 vise à améliorer la cybersécurité dans l'Union par différentes mesures, dont notamment la création d'une structure de management des crises cyber (CyCLONe [1295]), l'harmonisation supérieure des exigences de sécurité et de notification, etc. Surtout, pour ce qui nous intéresse ici, elle vise **l'inclusion expresse de nouveaux secteurs critiques dès lors tenus d'accroître leur niveau de cybersécurité** : énergie, transports, banque, infrastructures numériques, administration publique [1296], espace, **et naturellement santé.**

[1293] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers.
[1294] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.
[1295] EU-CyCLONe (*EUropean Cyber Crisis Liaison Organisation Network*), en français « *réseau européen pour la préparation et la gestion des crises cyber* », institué par la Directive 2022/2555 dite « NIS 2 » (article 16).
[1296] Les champs de compétence régalienne comme la sécurité publique, défense, judiciaire, parlements et banques centrales ne sont pas couverts.

En ce qui concerne la santé, relevons ici que « NIS 2 » développe substantiellement les dispositions de « NIS 1 » : d'une part, elle **élargit les entités attirées dans son champ** ; d'autre part, elle les répartit en deux annexes, **selon la criticité perçue en application de critères unifiés** : ces critères ne relèvent plus de la seule appréciation nationale.

*** L'Annexe I détaille les secteurs « hautement critiques ».** Son contenu appelle peu de commentaires à ce stade. L'annexe I comprend ainsi :

- les « *Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil* » [1297], lequel *item* recouvre mot pour mot, le périmètre initialement visé par la directive NIS 1 ;
- les « *Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil* [1298], particulièrement sollicités durant la pandémie de Covid 19, et en première ligne face au risque biologique dont bioterroriste ;
- les « *Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil* » [1299], sachant la directive de 2001 en cours de refonte en 2023 ;
- les « *Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21* », soit notamment des matières premières, excipients et précurseurs de synthèse ;
- les « *Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil* » [1300], qui recouvrent notamment les moyens diagnostiques (DMDIV) mais aussi thérapeutiques.

Le développement de cette liste par « NIS 2 » **met en exergue l'enjeu exacerbé de la protection des données et réseaux en santé**. En contraste d'autres secteurs, on pouvait les

[1297] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers.
[1298] Règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision no 1082/2013/UE.
[1299] Directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain.
[1300] Règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux.

imaginer protégés par le droit international humanitaire contre les ingérences étatiques ; mais l'expérience dénie ce point.

*** L'annexe II de la directive NIS 2 détaille les « autres secteurs critiques ».** Cette fois le secteur « santé » n'y apparaît plus en soi, car il a été traité comme secteur en annexe I. En revanche, dans le secteur 5 titré « fabrication », on retrouve un unique sous-secteur : « *a) fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic* in vitro » (les médicaments figurent en Annexe I). Ce sous secteur recouvre plusieurs entités, dont :
- les « *entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE) 2017/745 du Parlement européen et du Conseil* » [1301];
- les « *entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746 du Parlement européen et du Conseil* » [1302] ;
Mais la définition en droit de ce sous-secteur « fabrication » de technologies de santé est résiduelle : les fabricants de DM et DMDIV concernés par le réhaussement uniforme exigé des mesures de sécurité au titre de l'annexe II, **sont tous ceux non mentionnés à l'annexe I**.

Après avoir vu l'élargissement significatif en santé, des entités **devant impérativement adapter leur sécurité selon les critères communs face à la menace cyber**, voyons maintenant ce qu'il en est du règlement proposant une « cybersolidarité » au sein de l'Union.

2. La santé, premier objectif concret de la proposition en 2023 du règlement « cybersolidarité »

En complément de ce qui précède, la Commission européenne vient en avril 2023 de proposer à l'instigation du Conseil [1303], un règlement « *établissant des mesures destinées à **renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir*** » [1304].

[1301] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) no 178/2002 et le règlement (CE) no 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.
[1302] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission.
[1303] Conclusions du Conseil sur la mise en place d'une posture cyber de l'Union européenne approuvées par le Conseil lors de sa session du 23 mai 2022 (9364/22).
[1304] Proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, COM(2023) 209 final, 2023/0109(COD).

* Cette proposition est essentiellement formulée sur le fondement de l'article 173§3 TFUE (conditions de la compétitivité de l'Union) : **la cybersécurité étant considérée comme le corollaire nécessaire du marché unique numérique**. La proposition s'appuie sur les textes précédents, dont le réseau européen mis en place à compter de 2022 par la directive « NIS 2 », pour la préparation et gestion des crises (EU-CyCLONe) [1305] et, issus de la directive « NIS 1 », pour la réponse aux incidents de sécurité informatique (CSIRT) [1306].

L'article 222 TFUE (clause de solidarité face aux attaques terroristes, catastrophes naturelles ou d'origine humaine), qui, on l'a vu, a fondé l'exposé de la première « *stratégie sur la cybersécurité* » de l'Union [1307], **n'est à nouveau pas invoqué ici comme fondement juridique**. Le texte de présentation **n'y fait référence, que pour constater la cohérence** [1308].

Pourtant, dès le second § de cette présentation, il est souligné que « *les cyberopérations sont de plus en plus* ***intégrées dans les stratégies de guerre hybrides****, avec des effets significatifs sur la cible. En particulier, l'agression militaire de la Russie contre l'Ukraine a été précédée et s'accompagne d'une stratégie de cyberopérations hostiles,* ***ce qui change la donne en ce qui concerne la perception et l'évaluation de la préparation collective de l'Union à la gestion des crises de cybersécurité et nécessite une action urgente.*** *La menace d'un éventuel incident de cybersécurité majeur provoquant de graves perturbations et dommages à des infrastructures critiques exige une préparation accrue à tous les niveaux de l'écosystème de cybersécurité de l'Union* » [1309]. Cela est un écho direct de la résolution du Parlement de janvier 2023 sur la mise en œuvre **de la politique de sécurité et de défense commune** [1310].

[1305] EU-CyCLONe (*EUropean Cyber Crisis Liaison Organisation Network*), en français « *réseau européen pour la préparation et la gestion des crises cyber* », institué par la Directive 2022/2555 dite « NIS 2 » (article 16).

[1306] CSIRT (également sous l'appellation CERT), *Centre de réponse aux incidents de sécurité informatique*, créés et institués en réseau par la directive 2016/1148 dite « NIS 1 » (not. article 1§2c, articles 9 et 12). L'ENISA assure le secrétariat de ce réseau.

[1307] Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé, 7 février 2013, JOIN/2013/01 final.

[1308] Il y est précisé que celle-ci « *complètera les actions mises en œuvre dans le cadre de l'article 42, paragraphe 7, du traité sur l'Union européenne ou dans les situations définies à l'article 222* » TFUE, en section « Cohérence avec les autres politiques de l'Union », distinguée de la section qui la précède « Cohérence avec les dispositions existantes dans le domaine d'action ». Les éléments sont donc présentés, certes comme connexes, mais hétérogènes, ibid. page 2.

[1309] Ibid., page 1 (« Contexte de la proposition »).

[1310] Pour des développements circonstanciés permettant le relevé de tous les visas invocables dans cette situation, Résolution du Parlement européen du 18 janvier 2023 sur la mise en œuvre de la politique de sécurité et de défense commune – rapport annuel 2022 (2022/2050 (INI)).

Cet élément circonstancié d'explication sera développé dans le consid. n°2 de la proposition, sans qu'y soit appliqué la qualification de « *terrorisme* » au sens de l'article 222 TFUE [1311], **alors que l'attaque peut ne pas être « *hybride* »** : une attaque peut en effet n'être « que » cyber, non combinée à des moyens conventionnels. Cela laisse volontairement dans l'indétermination, complexifiant d'autant l'attribution et les mesures de rétorsion, on l'a vu, mais facilite l'invocation de l'article 222, le cas échéant.

Si le contenu de cette « *cybersolidarité* » sort de notre axe de recherche, notons que la proposition vise notamment : « a*) le déploiement d'une infrastructure paneuropéenne de centres d'opérations de sécurité (« cyberbouclier européen ») dans le but de mettre en place et de développer des* ***capacités communes de détection et d'appréciation de la situation****; b) la création d'un mécanisme d'urgence dans le domaine de la cybersécurité pour aider les États membres à se préparer aux incidents de cybersécurité importants et majeurs, à y* ***réagir et à s'en rétablir immédiatement****; c) la mise en place d'un mécanisme européen* ***d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents importants ou majeurs*** » (*ibid*.). Ce point suscite la circonspection sur le terrain de la confidentialité [1312].

*** Quelle place pour la santé ?** Si aucun secteur spécifique n'est identifié, un *item* attire l'attention dans la 3ème section des motifs dont l'exposé précède la proposition (il ne s'agit pas encore des considérants) : il évoque les « *droits fondamentaux* » [1313].

En effet, c'est au regard de ces droits fondamentaux des individus, non d'un concept de souveraineté des Etats membres ou de l'Union, que l'ensemble est justifié : ainsi, le projet invoque l'article 6 de la Charte des droits fondamentaux de l'Union pour le droit à la protection de la liberté et de la sécurité ; l'article 7, pour le droit au respect de la vie privée et familiale ; 16, pour la liberté d'entreprendre ; 17, pour le droit de propriété. Curieusement, pas l'article 8 (droit à la protection des données à caractère personnel) notamment : peut-être son

---

[1311] « Compte tenu de l'évolution rapide du panorama des menaces, le risque que d'éventuels incidents majeurs provoquent des perturbations ou des dommages importants à des infrastructures critiques nécessite que la préparation soit renforcée à tous les niveaux du cadre de cybersécurité de l'Union. Ce risque va au-delà de l'agression militaire de la Russie contre l'Ukraine et il est susceptible de persister au vu de la multiplicité des acteurs de niveau étatique, criminels et hacktivistes qui sont impliqués dans les tensions géopolitiques actuelles. De tels incidents peuvent entraver les services publics et nuire à la poursuite des activités économiques, notamment dans les secteurs critiques ou hautement critiques, entraîner de lourdes pertes financières, entamer la confiance des utilisateurs, causer un préjudice majeur à l'économie de l'Union, voire mettre en danger la santé ou la vie des personnes ».

[1312] Sénat français, voir le Rapport du GT sur la subsidiarité (déposé le 26/05/2023), textes européens sur les Menaces et incidents de cybersécurité.

[1313] Ibid., pages 6 et 7.

évidence a-t-elle pu conduire à juger inutile de ce rappeler.

Or, **la santé, seul secteur concrètement évoqué,** y donne lieu à une mise en exergue (consid. n°2) : ainsi « *Finally, by protecting the integrity of critical infrastructure in the face of cyberattacks,* ***the proposal will contribute to the right to healthcare in accordance with Article 35*** *of the EU Charter of Fundamental Rights* (…) » [1314], et le droit d'accès aux services d'intérêt général visés à l'article 36. Ces considérations ne réapparaissent pas dans les considérants : ils ne pointeront aucun secteur particulier.

Mais **la proposition invoque une collection des droits individuels fondamentaux**, **non un principe de souveraineté de communauté politique.**

B. L'EXTENSION PREVUE DES NORMES DE PROTECTION EN MATIERE DE PRODUITS CONNECTES

Poursuivons le relevé systématique de la place des données de santé (étendue aux systèmes d'information qui les génèrent, stockent et émettent, voire les traitent) dans la dynamique. Distinctement de la question des infrastructures, dont nous avons vu la qualification de criticité approfondie pour élargir les obligations des parties, nous relevons ici la question des **produits susceptibles d'être corrompus par des attaques cyber, voire de relayer de telles attaques.** Or, cela concerne même les produits *a priori* les moins critiques [1315].

La compétence européenne est ici à nouveau justifiée du fait de la **dimension transfrontière de la cybersécurité**, à double titre : les produits sont souvent commercialisés et utilisés dans l'ensemble du marché intérieur ; les attaques cyber qui n'affectent à l'origine qu'une entité ou un Etat peuvent s'y propager très rapidement, et de façon intersectorielle.

Or, la directive « NIS 2 » que nous venons d'évoquer, **ne traite pas d'exigences en la matière :** son objet est les infrastructures. Mais d'un point de vue méthodologique en droit, le

---

[1314] *« Toute personne a le droit d'accéder à la prévention en matière de santé et de bénéficier de soins médicaux dans les conditions établies par les législations et pratiques nationales. Un niveau élevé de protection de la santé humaine est assuré dans la définition et la mise en oeuvre de toutes les politiques et actions de l'Union* ».

[1315] car la « *première compromission d'un appareil ou d'un réseau,* (permet) *à des acteurs malveillants d'obtenir un accès privilégié à un système ou de se déplacer latéralement entre différents systèmes* », consid 7.

défi identifié [1316] est similaire : la dispersion des obligations nationales place fabricants et utilisateurs des objets connectés dans une situation d'incertitude juridique, et renchérit les coûts de production par accumulation des standards exigibles. Cela permet d'invoquer l'article 114 TFUE au profit des entreprises, citoyens et collectivités.

En septembre 2022, il en résulte la proposition d'un règlement « cyber-résilience » (*cyber-resilience Act*) [1317]. Nous esquissons son apport pour les objets connectés en général (1), avant de relever **l'autonomie des « dispositifs médicaux » connectés** (2).

1. De nouvelles obligations pour la cybersécurité des dispositifs connectés en général

La proposition **s'applique aux « produits comportant des éléments numériques »**, entendu comme « *tout produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels destinés à être mis sur le marché séparément* » (article 3), **qui doivent être « connectés »** : c'est-à-dire que leur « *utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau* » (article 2).

La proposition énonce des exigences essentielles relatives à la conception, au développement et à la production et les obligations des opérateurs économiques (article 1-a) ; celles relatives aux processus devant être introduits par les fabricants en vue de la gestion des vulnérabilités, durant le cycle de vie du produit (1-b), et les règles relatives à la surveillance du marché et au contrôle des obligations précitées (1-c).

Mais dès l'article 2 de la proposition de règlement de septembre 2022, il est expressément spécifié que celui-ci **ne s'applique ni aux dispositifs médicaux en général** [1318], **ni aux dispositifs médicaux de diagnostic *in vitro*** [1319].

[1316] Communication conjointe (2020) au Parlement européen et au Conseil : La stratégie de cybersécurité de l'UE pour la décennie numérique JOIN/2020/18 final ; Résolution du Parlement européen du 10 juin 2021 sur la stratégie de cybersécurité de l'Union pour la décennie numérique (2021/2568 (RSP)).

[1317] Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE)2019/1020.

[1318] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE.

[1319] Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro, abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission.

* Or, ces définitions étant strictes, les exigences essentielles en matière de cybersécurité des dispositifs connectés parfois bardés de métrologie, ne revendiquant qu'une finalité de « bien-être », récréative, de mesure de performance sportive etc. mais produisant des données de santé « par destination », **relèvent du champ de la proposition de règlement cyberrésilience de 2022**. Rappelons que, bien qu'ils ne soient pas des dispositifs médicaux, les données qu'ils génèrent **pourraient abonder l'espace numérique de santé personnel**.

* **L'implication d'une « donnée de santé » n'est pas, en soi,** un critère de qualification de la technologie, donc du droit applicable. On le voit avec une réserve dans le considérant n°31 de la proposition de règlement de 2022, lequel évoque **les systèmes de « dossiers médicaux électroniques » (DME),** qui ont vocation à être généralisés par la proposition de règlement de mai 2022 sur l'Espace européen des données de santé.
Or, le considérant relève que ces DME sont **essentiellement régis par la proposition de règlement EEDS** (non, donc, par le droit général des dispositifs médicaux qui couvre les logiciels médicaux) ; ceci à l'exception des DME conçus et utilisés « en interne » par les établissements de santé, car ils n'ont pas vocation à être commercialisés (consid. 31).

En outre, le règlement cyberrésilience ne couvrant pas les SaaS (*Software as a Service*) en tant que tels [1320], « *les systèmes DME proposés par l'intermédiaire du modèle de licence et de livraison du SaaS* ***ne relèvent pas du champ d'application du présent règlement*** » (*ibid*.). Notons que, tout comme les DME conçus et utilisés « en interne » par les établissements de santé, les SaaS pourraient entrer à terme (quand ?) dans le champ **d'actes d'exécution de la Commission en application de la directive NIS 2.** Cette précision ne figure toutefois pas dans les considérants du règlement, mais dans l'exposé des motifs de sa proposition [1321].

En revanche, si les DME sont des « *produits comportant des éléments numériques* » au sens de l'article 3, **ils sont également soumis aux dispositions du règlement cyberrésilience mais** (selon son article 24) suivant la procédure du règlement EEDS… sachant que « *pour faciliter la mise en conformité, les fabricants peuvent établir une documentation technique unique contenant les éléments requis par les deux actes législatifs* » (consid 31)... Ouf !

[1320] Seulement les « ***produits comportant*** *des éléments numériques* », i.e. des entités matérielles combinées.
[1321] Proposition, page 3 : *« Pour toutes les autres entités, la Commission peut adopter un acte d'exécution établissant les exigences techniques et méthodologiques ainsi que les exigences sectorielles (…) Par exemple, cela pourrait être un moyen d'assurer un niveau élevé de cybersécurité dans des cas tels que celui des systèmes médicaux électroniques (DME), y compris lorsque ceux-ci sont fournis sous la forme de logiciel en tant que service (SaaS) ou développés au sein des établissements de santé (en interne)* ».

* Enfin, les dispositifs relevant de la définition légale de DM ou de DMDIV, sont régis de façon autonome. Dès lors, s'impose **une certification de conformité aux exigences essentielles propres, lesquelles doivent intégrer ces paramètres** [1322]. Mais qu'en est-il ?

2. L'attente d'obligations en matière de cybersécurité des « DMIL » : jusqu'à quand ?

S'il existe un droit spécifique dans les règlements 2017/745 (DM) et 2017/746 (DMDIV) et leurs annexes respectives, **la question de la cybersécurité des dispositifs médicaux n'y est que peu développée,** alors que le consid. 12 de la proposition de 2022 dispose que « *ces deux règlements traitent des risques de cybersécurité et suivent des approches particulières qui sont également abordées dans le présent règlement* ». La connectivité des DM est exponentielle (par wifi, radiofréquence, Bluetooth etc.) et renouvelle pour partie la réflexion.

Certes, les règlements (UE)2017/745 et (UE)2017/746 établissent des exigences essentielles pour les DM qui « *fonctionnent au moyen d'un système électronique ou sont eux-mêmes des logiciels* » (ibid.). **Mais la singularité est ici l'interconnexion, qui fait entrer dans une dimension différente**.

Le but est de générer des données de santé, de notifier des activités, parfois d'automatiser des décisions (d'administration de médicaments, d'activation ou modulation de stimulateurs implantés ou non etc., au profit de processus thérapeutiques, d'actions de compensation), d'automatiser la maintenance des systèmes etc. ; **et de s'assurer de l'absence de leur violation pour une corruption de ces finalités** [1323], ou leur usage comme vecteur, pour pénétrer un réseau (de santé ou non) au-delà de la personne concernée.

En l'état, la question précise est donc **appréhendée en premier lieu au niveau national**. En matière de DM, il n'existe en effet pas dans l'Union, d'instance centralisée de régulation et mécanisme centralisé d'autorisation comme pour les médicaments [1324]. Il en résulte une mosaïque de positionnements nationaux, dont on peut sans doute prédire la résorption proche (mais quand ?) par un texte unifiant sur le fondement de l'article 114 TFUE ...

[1322] Cette certification étant opérée par les fabricants ou les « organismes notifiés » ; selon la criticité du dispositif médical du point de vue de la réglementation applicable, les critères étant différents selon qu'il s'agit de dispositifs non DMDIV (classe I, spéciale IIa, IIb, III) ou de DMDIV.
[1323] Sur les risques spécifiques d'attaque individualisée sur ces systèmes, voir la section précédente.
[1324] A la différence du droit applicable aux médicaments issus de la directive 2001/83 CE, en refonte en 2023.

Ainsi, **l'Agence française (ANSM)** s'est en 2017 dotée d'un Comité Scientifique Spécialisé nommé « *Cyber sécurité des logiciels dispositifs médicaux »* [1325], et joue depuis un rôle moteur important, au-delà du plan français. Elle a lancé une consultation publique sur un projet de recommandations pour la cybersécurité des dispositifs médicaux, sur la base d'un projet diffusé en juillet 2019 [1326]. Un document final **vient d'être publié en septembre 2022** [1327] .

Or, ce sont les premières recommandations publiées sur le sujet dans l'Union (des homologues d'autres Etats membres s'y affairent également), **partagées avec la Commission européenne en vue d'adapter** la réglementation spécifiquement applicable, puisque tel n'est pas l'objet de la proposition de règlement « cyberrésilience » [1328]. Mais ce rapport français de préciser qu'il ne consiste par nature qu'en un ensemble de **recommandations de bonnes pratiques, non un texte normatif [1329]**. Il n'est pas lieu ici d'entrer dans le contenu technique.

En revanche, il nous intéresse de relever la dynamique parallèle **aux Etats-Unis, qui ont pour particularité une approche normative centralisée en matière également de DM**.

Ainsi en décembre 2022, la section 3305 de la loi « omnibus » (*Consolidated Appropriations Act* [1330]) a modifié le droit fédéral en introduisant dans le FDC Act une section 524B, titrée « *Ensuring Cybersecurity of devices* ». Ce nouveau droit ne s'appliquera pas aux DM présentés avant mars 2023, et ne régira ceux présentés auparavant, qu'en cas de leur modification si elle appelle un examen pré-commercialisation[1331]. Il n'est pas non plus utile

---

[1325] Décision DG n° 2017-243 du 08/06/2017 - Création CSST Cyber sécurité des logiciels dispositifs médicaux, Décision DG n° 2018-160 du 22/06/2018 - Prorogation CSST Cyber sécurité des logiciels dispositifs médicaux, Décision DG n° 2019 –385 du 29/11/2019 -Création CST Cyber sécurité des dispositifs médicaux et nouveaux enjeux des technologies de l'information - Poursuite des travaux.

[1326] ANSM, (projet) recommandations, « Cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie », juill. 2019, sur le site ANSM (disponible en français et en anglais).

[1327] ANSM, (final), recommandations, « Cybersécurité des dispositifs médicaux intégrant du logiciel au cours de leur cycle de vie », sept. 2022, site ANSM.

[1328] « *The ANSM French Competent Authority published in July 2019 a draft guideline on cybersecurity for medical devices. The European medical device sector should greatly applaud this initiative.* ***This is the first and only guideline on cybersecurity with regard to the European medical device regulations.*** » https://blog.cm-dm.com/post/2019/07/26/Guideline-on-Cybersecurity-from-ANSM-French-Competent-Authority (juillet 2019). Ce n'était alors qu'un projet encore ; il a donné lieu à publication en anglais, suite au reproche de n'avoir été publié qu'en français.

[1329] Cela peut sembler évident en droit français, mais la signification est ainsi claire au plan international.

[1330] En droit fédéral américain, une loi « *omnibus* » désigne une loi de fin d'année qui regroupe des thématiques trans-sectorielles, dont le nom ne saurait donc être significatif. En droit français, on la nommerait un collectif (*omnibus* signifie « pour tous »), si n'était le risque de confusion avec la qualification de « collectif budgétaire », qui y désigne une loi de finance rectificative en cours d'année.

[1331] Site de la FDA, FAQ3 sur l'onglet dédié : https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

ici d'entrer dans le détail technique ; le lecteur intéressé par le droit des dispositifs médicaux connectés pourra se livrer à un utile exercice comparatif. Ce qui nous intéresse ici, est que :

* le droit européen a défini les DM et les DMDIV, mais pas encore les « DM connectés ». On peut imaginer que la définition résultera du croisement avec la définition de « *produit comportant des éléments numériques* ». Du fait que la « connectivité » transcende les classes technico-réglementaires [1332], **ils appelleront un texte transverse.** Ils sont définis par l'ANSM comme des « *dispositifs médicaux intégrant du logiciel* » ou DMIL (ibid., p 7), avec dans son glossaire pour équivalent anglais, MDIS (*Medical device integrating software*).

* en contraste, **le droit fédéral américain est le premier à donner une définition normative d'un « cyber device »** : « *Section 524B(c) of the FD&C Act **defines "cyber device"** as a device that (1) includes software validated, installed, or authorized by the sponsor as a device or in a device, (2) has the ability to connect to the internet, and (3) contains **any such technological characteristics** validated, installed, or authorized by the sponsor **that could be vulnerable to the cybersecurity threats.** If manufacturers are unsure as to whether their device is a cyber device, they may contact the FDA*. ».

Or, il est significatif qu'en 2023, **la vulnérabilité à une menace cyber soit un élément de définition même du « *cyber device* » médical,** dans le but de son agrément spécifique. On peut imaginer que le droit européen s'en inspirera dans l'élaboration d'un texte transverse.

§2. LA DYNAMIQUE DES COMPETENCES EN MATIERE DE PROTECTION CONTRE LES CYBER-INGERENCES

Avant d'examiner la dynamique des compétence des opérateurs et procédures, notons une dynamique emblématique : **celle de la compétence normative**. Depuis 1995, les textes visant à sécuriser les systèmes et réseaux ont essentiellement été adoptés par voie de directives en mode « millefeuille » nous l'avons relevé, du fait de la nécessité d'actes sectoriels [1333]. Ceci

[1332] Etablies selon la criticité intrinsèque du dispositif : ainsi en matière de DM, les classe I, I « fonction spéciale », IIa, IIb, III etc. cette dernière recouvrant notamment les dispositifs médicaux implantables actifs (stimulateurs cardiaques, neurologiques etc).

[1333] Pour rappel : Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ; Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») ; Directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de

en l'absence longtemps d'une approche systémique, incarnée depuis par les stratégies précitées.

Mais la directive « NIS2 » adoptée en 2022, et portant sur la sécurisation des infrastructures et réseaux, **propose une accélération dans l'élaboration des règles** visant à garantir un niveau élevé de cybersécurité dans l'Union. Eu égard à la technicité de dispositions dont le principe est désormais acquis, il y est en effet souligné (considérant 22), que la Commission « *devrait évaluer si de telles dispositions supplémentaires pourraient être prévues par un acte d'exécution* ». **De fait, les actes juridiques sectoriels sont considérés par défaut.**

* Or, la proposition en 2022 de règlement « *cyberrésilience* » envisage elle-même dans l'exposé de ses motifs (non dans les considérants, ni dans le corps du texte), la possibilité que des **actes d'exécution pris en application de la directive NIS 2 (d'objet pourtant différent)** puissent couvrir des entités non couvertes. Ainsi, hors des exclusions de l'article 3, des dispositifs qui pourraient constituer des DME : ceux on l'a vu, « *fournis sous la forme de logiciels en tant que services (SaaS) ou développés au sein des établissements de santé* ».

* De même, la proposition en 2023 de règlement « *services de sécurité gérés* » [1334], a pour but essentiel de permettre, **par actes d'exécution de la Commission,** l'adoption de schémas européens de certification de cybersécurité. **La technicité de la matière certes le justifie – mais c'est aussi un champ hautement régalien !** On reviendra d'ailleurs *infra* sur la perception ombrageuse, au plan national, de cette dynamique.

---

communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive "accès") ; Directive 2002/20/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'autorisation de réseaux et de services de communications électroniques (directive "autorisation") ; Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive "cadre") ; Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive "service universel") ; Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ; Résolution du Parlement européen sur la communication de la Commission "eEurope 2005: une société de l'information pour tous" (Plan d'action à présenter en vue du Conseil européen de Séville des 21 et 22 juin 2002) 2022/2242 (INI) ; Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information **;** Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148.

[1334] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés, COM(2023) 208 final2023/0108 (COD).

Ces évolutions sont emblématiques de la dynamique en cours. Elle est certes **stimulée par la transformation numérique rapide dans une économie globalisée compétitive, mais aussi aiguillonnée par la menace pandémique, géopolitique et cybercriminelle**. Dans ce contexte de hautes pressions et d'imprévisibilité tous azimuts, nous évoquons la dynamique d'extension nécessaire des opérateurs de sécurité reconnus (A). Puis nous invitons à s'interroger sur une dynamique incertaine : celle des régimes procéduraux (B).

A. DYNAMIQUE D'EXTENSION DES COMPETENCES DES OPERATEURS FACE AUX CYBERINGERENCES

Les textes précités qui qualifient les infrastructures « *hautement critiques* » et « *critiques* », les « *produits, services et processus TIC* » et les « *produits à composante numérique* », **sont pour leurs destinataires publics et privés la source d'obligations nouvelles et unifiées.** Elles visent à un niveau élevé et homogène de « cybersécurité » dans l'Union européenne.

Or, si la définition conceptuelle de la cybersécurité, son atteinte pratique et son maintien adaptatif dépendent des référentiels et de l'action continue des organismes publics tant au niveau européen qu'étatique ; **ils dépendent aussi de l'interaction avec des fournisseurs, dans le cadre de prestations de service en secteur marchand.** Ces prestations sont définies comme visant à « *prévenir et détecter les incidents* », et aider à « *y réagir ou se rétablir* » [1335].

En conséquence, l'enjeu, pour la performance et pour la confiance, de l'encadrement de tels **« fournisseurs de services de sécurité gérés »** est critique, mais était **absent des textes précédents**. Il est donc l'objet en 2023 d'une proposition de règlement qui vise à leur certification intrinsèque (2).
Nous verrons ce point après avoir relevé l'élargissement, depuis 2019, des compétences de l'ENISA, en tant qu'organisation faîtière devenue *leader* dans la stratégie européenne de cybersécurité. Elle devra en effet concourir à la fiabilité du marché compétitif ainsi ouvert (1).

[1335] Consid. 86, Directive 2022/2555 dite « NIS 2 ».

1. L'élargissement des compétences de l'ENISA dans la stratégie de cybersécurité

La transformation numérique, son exploitation opportuniste par les acteurs cybercriminels voire géopolitiques, expliquent la dynamique depuis 2004 des compétences de **l'Agence européenne chargée de la sécurité des réseaux et de l'information** (ENISA) [1336]. En 2008, son mandat a été prorogé jusqu'en 2012 [1337] ; en 2011, jusqu'en 2013 [1338] ; en 2013, élargi et prorogé jusqu'en 2020 [1339]. Mais en 2019, le règlement 2019/881 ne se limite pas à une prorogation du mandat : **il étend fortement les compétences de l'ENISA, au vu du contexte de menace systémique transfrontière croissante.** Il en fait **un acteur central** de la stratégie européenne de cybersécurité, **et institue des obligations de fond** pour réaliser celle-ci [1340].

Mais seules les dimensions de compétence nous intéressent ici :

*** Le règlement 2019/881 étend substantiellement les compétences de l'ENISA.** Son article 4 définit sept objectifs [1341], avant que le Chapitre II énonce les tâches correspondantes :

[1336] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information.

[1337] Règlement (CE) n°1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) n°460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée.

[1338] Règlement (UE) n°580/2011 du Parlement européen et du Conseil du 8 juin 2011 modifiant le règlement (CE) n°460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée.

[1339] Règlement (UE) n°526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n°460/2004.

[1340] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013.

[1341] *« 1. L'ENISA est un centre de compétences en matière de cybersécurité du fait de son indépendance, de la qualité scientifique et technique des conseils et de l'assistance qu'elle dispense, des informations qu'elle fournit, de la transparence de ses procédures de fonctionnement, des modes de fonctionnement et de sa diligence à exécuter ses tâches ; 2. L'ENISA assiste les institutions, organes et organismes de l'Union, ainsi que les États membres, dans l'élaboration et la mise en œuvre des politiques de l'Union liées à la cybersécurité, y compris les politiques sectorielles concernant la cybersécurité ; 3. L'ENISA soutient le renforcement des capacités et contribue à l'état de préparation au sein de l'Union en aidant les institutions, organes et organismes de l'Union, ainsi que les États membres et les parties prenantes des secteurs public et privé, à accroître la protection de leurs réseaux et systèmes d'information, à développer et à améliorer les capacités de cyber-résilience et de cyber-réaction, et à développer des aptitudes et des compétences dans le domaine de la cybersécurité ; 4. L'ENISA favorise la coopération, notamment le partage d'informations et la coordination au niveau de l'Union, entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes concernées des secteurs public et privé en ce qui concerne les questions liées à la cybersécurité ; 5. L'ENISA contribue à renforcer les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de soutenir les actions des États membres pour prévenir les cybermenaces et réagir à celles-ci, notamment en cas d'incidents transfrontières ; 6. L'ENISA favorise le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur. L'ENISA contribue à l'établissement et au maintien d'un cadre européen de certification de cybersécurité, conformément au titre III du présent règlement, en vue de rendre plus transparente la cybersécurité des produits TIC, services TIC et processus TIC et, partant, de rehausser la*

élaboration et la mise en œuvre de la politique et du droit de l'Union (*article 5, comprenant 6 alinéas dont 6 subdivisions*) ; assistance au renforcement des capacités (*article 6, comprenant 2 alinéas dont 10 subdivisions*) ; le soutien à la coopération opérationnelle au niveau de l'Union (*article 7, comprenant 7 alinéas, dont 12 subdivisions*), l'activité en matière de marché, certification de cybersécurité et de normalisation (*article 8, comprenant 7 alinéas, dont 5 subdivisions*), l'activité en matière d'analyse, expertise, avis et diffusion (*article 9, comprenant 5 subdivisions*), sensibilisation et éducation (*article 10, comprenant 4 subdivisions*), recherche et innovation (*article 11, comprenant 3 subdivisions*) et coopération internationale (*article 12, comprenant 4 subdivisions*).
Ces **très copieux développements réglementaires** [1342] déterminent les nouvelles modalités d'organisation (Chap. III) et de financement (Chap. IV) de l'ENISA.

Parmi les productions au titre de l'article 9 notamment, rappelons la publication en juillet 2023, du **premier rapport de l'ENISA sur les cybermenaces relatives au secteur de la santé** [1343] : nous l'avons exploité *infra* pour l'observation du développement des ingérences.

***** Mais **ce périmètre pourtant élargi de compétence de l'ENISA va être mis en cause,** par des limites rapidement constatées quant aux règles de fond en matière de certification de cybersécurité des produits, services et processus, adoptées en 2019 (ibid., *Titre III, cadre de certification de cybersécurité*, articles 46 à 62). Il n'est pas lieu de les développer ici, car cela échappe à notre axe de recherche, et nous avons vu que **les dispositifs médicaux étaient à leur égard autonomes**. **Quel lien donc avec la question de compétence ?**

Le règlement 2019/881 avait introduit des « *schémas européens de certification* » des « *produits TIC* » [1344], « *services TIC* » [1345], et « *processus TIC* » [1346], qui impliquent largement l'ENISA (article 8). Ces règles communes ont été adoptées par l'Union, pour y palier la dispersion des exigences nationales quant à la cybersécurité en la matière. Certes, il y existait

---

confiance dans le marché intérieur numérique et la compétitivité de ce dernier ; 7. L'ENISA promeut un niveau élevé de sensibilisation des citoyens, des organisations et des entreprises aux questions liées à la cybersécurité, y compris en matière d'hygiène informatique et d'habileté numérique ».
[1342] Pour mesurer l'accroissement des tâches de l'ENISA au regard de ses compétences antérieures, il suffit de relever dans les considérants du règlement, le nombre d'occurrence du verbe « devrait » attaché à l'ENISA. Sur un plan purement fonctionnel, cela fait 52 occurrences ! Il n'est pas lieu d'établir ici un tel inventaire comparatif.
[1343] ENISA, « Threat Landscape : Health Sector (January 2021 to March 2023), ISBN 978-92-9204-638-5.
[1344] « *élément ou groupe d'éléments appartenant à un réseau ou à un schéma d'information* » (article 2§12).
[1345] « *service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information* » (article 2§13).
[1346] « *ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance* » (article 2§14).

bien un accord de reconnaissance mutuelle du groupe des hauts fonctionnaires européens pour la sécurité des systèmes d'information (**SOG-IS**), mais de portée limitée [1347].

Mais **les « *fournisseurs de services de sécurité gérés* » étaient absents** des « *schémas européens de certification* ». Pourtant l'enjeu est de taille : l'ouverture d'un marché compétitif, par les multiples obligations de fond faite aux destinataires des textes, met en exergue la reconnaissance de la **compétence des prestataires de services de cybersécurité** !

2. Vers la certification européenne de compétence des « services de sécurité gérés » ?

Par nature, les organisations du secteur marchand qui proposent des prestations de service en cybersécurité doivent être des « *fournisseurs de confiance* ». Ceci *a fortiori* avec le développement des obligations des opérateurs publics et privés, donc l'élargissement du marché européen, source d'opportunité commerciales… comme d'ingérences.

Or, ces **« *fournisseurs de services de sécurité gérés* »** appartiennent à un « *secteur hautement critique* », et sont qualifiées d'« *entités essentielles* » ou « *importantes* » [1348].

***** Ce d'autant qu'ils ne sont pas moins exposés à des cyber-attaques que leurs clients du secteur public ou privé, cibles jusqu'alors primaires. Ils présentent même un risque particulier, « *du fait de leur grande intégration dans les activités des opérateurs* » [1349]. Cela suppose de leur part compétence, probité etc. **et leur propre sécurité pour éviter les risques systémiques de contamination**, accidentelle ou programmée.

***** En outre, ils sont censés s'intégrer dans la « *réserve de cybersécurité de l'Union Européenne* », dont la mise en place est un des buts de la proposition. Cette réserve doit être activée « *en cas d'incidents de cybersécurité importants et de grande ampleur* », pour **soutenir les mesures de réaction et de rétablissement capacitaire immédiat**. Or, cela appelle un processus de sélection des « *fournisseurs* » *(sic)* constituant cette réserve, laquelle sélection devrait tenir compte de leur certification en matière de cybersécurité.

Dès lors, l'enjeu en 2023 **est d'absorber dans le champ du droit européen en matière de certification de cybersécurité, ces services qui n'en relevaient pas** ; ceci sans préjudice du règlement n°765/2008, qui encadre aussi des activités d'accréditation et de surveillance [1350].

[1347] Cf. le *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates* version 3.0, janvier 1010 (texte et liste des Etats signataires sur le site de l'ANSSI).
[1348] Directive 2022/2555 préc.
[1349] Exposé des motifs (préalable aux considérants), page 2.
[1350] Règlement (CE) n°765/2008 du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) 339/93.

Introduite par la proposition de règlement de 2023, la notion de « ***services de sécurité gérés*** » découle donc directement de la notion de « *fournisseur de services de sécurité gérés* », portée par « NIS 2 ». Mais **la proposition de 2023 focalise ainsi sur la compétence.**

En effet, à la différence des produits, services ou processus TIC, ces services nécessitent de prévoir « *dans le cadre des objectifs de sécurité (...)* ***un très haut niveau de compétence, d'expertise et d'expérience*** *ainsi que les procédures internes appropriées* » (Consid 5, projet du 18 avril 2023). Cela justifie la proposition de modification du règlement (UE) 2019/881 [1351]. Si son texte ne contient que deux articles, l'article 1 contient 17 alinéas, avec nombre de subdivisions. Il n'est pas lieu ici de les passer en revue ; notons seulement que ce texte :

* définit le « ***service de sécurité géré*** », comme un « *service consistant à effectuer des activités liées à la gestion des risques en matière de sécurité, ou à fournir une assistance dans le cadre de ces activités, y compris la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil* » (article 1§2b).
En conséquence, il permet de bénéficier de la dérogation en droit pénal français pour les tests d'intrusion etc., *supra*. Mais la « réaction aux incidents » **n'inclut pas la pratique du *hackback*** privé, compte tenu de sa nature offensive et de son régime controversé, *infra*.

* prévoit la mise en place d'un « **schéma européen de certification de cybersécurité ».** Celui-ci est entendu comme un « *ensemble complet de règles, d'exigences techniques, de normes et de procédures* ***qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité*** *de produits TIC, services TIC, processus TIC* ***ou services de sécurité gérés spécifiques*** » (article 1§2a, sous 9).
Ainsi, la qualification de « *spécifiques* » associée aux services de sécurité gérés, suggère que le schéma européen couvre les services **examinés un par un dans l'éventail des services proposés**. Il pourrait donc ne pas être un éventail « complet » de services : cela imposera une vigilance quant aux prétentions, sur le marché, de l'entité qui revendique des certifications.

* prévoit la délivrance d'un « **certificat de cybersécurité européen** ». Il est défini comme un « *document délivré par un organisme compétent attestant qu'un (...) service de sécurité géré donné* ***a été évalué en ce qui concerne sa conformité aux exigences*** *de sécurité spécifiques* » précitées (article 1§2a, sous 11).
Or, nous avons vu que le service **était opérateur-dépendant autant que techno-dépendant.**

[1351] La proposition ne référence pas l'avis du CEPD : il en est saisi, mais ne l'a pas encore rendu à cette date.

Cela pose la question de la volatilité potentielle des compétences (donc des certifications !), **par *turn-over* d'une expertise très courtisée** (cf. le futur article 51bis [1352]). Ceci sans compter le **problème classique mais accru, des compromissions personnelles**, vecteur d'ingérences étatiques comme privées. L'introduction de systèmes dits d'« intelligence artificielle » dans la génération et maintenance adaptative de services de sécurité, pose encore d'autres questions.

* prévoit que le schéma européen de certification **peut préciser un ou des « *niveaux d'assurance* »** (au sens dans le texte de fiabilité de la prestation), y compris pour les services de sécurités gérés : « *élémentaire* », « *substantiel* », ou « *élevé* ». Leur détermination « *correspond au niveau de risque associés à l'utilisation prévue (...) en termes de probabilité et de répercussions d'un incident* » (article1§10, proposant de modifier l'article 52).
En conséquence, les organes d'assurance-risque pourraient rapidement moduler leur niveau de couverture **selon l'étendue de la garantie offerte** par « le » service de sécurité géré (puisque telle est l'échelle de raisonnement), selon les termes dans lesquels il aura été certifié.

Enfin, la boucle est bouclée avec l'implication de l'ENISA. Nous avons vu son champ de compétence déjà récemment étendu en 2019, il l'est encore plus par cette proposition de 2023.

En effet, l'ENISA devrait contribuer à l'établissement et au maintien du cadre européen de certification, favoriser le recours à la certification européenne (article 1§3), en surveillant les évolutions, recommandant des spécifications techniques, préparant des « schémas candidats », évaluant les schémas (article 1§4a), publiant les lignes directrices (article 1§4 b), facilitant l'établissement et l'adoption de normes européennes et internationales (article 1§4c) etc. **Il n'y a pas là de singularité en santé :** les « services de sécurité gérés » s'entendent a priori sans singularité sectorielle – à la différence des produits, processus et services TIC, *supra*.

[1352] Article 51bis, dont l'introduction est proposée par l'article 1§9 : il serait intitulé *Objectifs de sécurité des schémas européens de certification de cybersécurité.* Le projet dispose que *« Un schéma européen de certification pour les services de sécurité gérés est conçu de façon à réaliser **selon le cas, au moins les objectifs de sécurité suivants :*** a*) faire en sorte que les services de sécurité gérés soient fournis avec la compétence, l'expertise et l'expérience requises, y compris que le personnel chargé de fournir ces services possède un très haut niveau de compétence et de connaissances techniques dans le domaine spécifique**, une expérience suffisante et appropriée et la plus haute intégrité professionnelle**; b) faire en sorte que le fournisseur ait mis en place des procédures internes appropriées pour garantir que les services de sécurité gérés **sont fournis à tout moment à un niveau de qualité très élevé**;*

Dans ce contexte, ces derniers et les services de sécurité gérés qui auront été « *évalués conformément »* etc., doivent satisfaire ***« à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données*** *qui sont consultées, traitées, stockées ou transmises dans le cadre de la fourniture de ces services* » (article 1§5, sous 2).
Mais, au regard des obligations générales existantes en matière de protection des données, n'est-ce pour partie superfétatoire ? à moins de considérer que, **après l'institutionnalisation des compétences** (identification légale pour l'acquisition de caractères permanents)**, ces textes ouvrent une autonomisation** (soumission à des règles propres) **des procédures ?**

B. LA DYNAMIQUE INCERTAINE DES REGIMES PROCEDURAUX FACE AUX INGERENCES CYBER

Comme précédemment indiqué, ces considérations **ne sont plus propres à la problématique de l'atteinte à l'intégrité des STAD de santé** : nous élargissons une perspective que nous ne ferons qu'esquisser.

Toutes les ingérences dans un STAD ont un dénominateur commun : l'attaque est informatique ; son vecteur est généralement un réseau de télécommunication, mondial ou non. Après avoir évoqué les concepts de cyber sécurité, de cyber solidarité et de cyber résilience **désormais pourvus d'un large socle de droit commun européen**, nous relevons ici quelques interférences en droit interne, puis entre droit national et droit européen, en ce qui concerne la « *cyber défense* » qui relève du champ de souveraineté des Etats.

En France, la cyber défense relève de la Défense nationale [1353] ; elle est une compétence partagée entre les services de renseignement et l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), laquelle est désignée « *Autorité nationale de défense des systèmes d'information* » (art. L. 2321-1 Code défense) pour la protection de nos intérêts vitaux [1354].

En cas d'une telle cyber agression, « *les services de l'Etat peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques* ***nécessaires à la caractérisation*** *de l'attaque et à la* ***neutralisation de ses effets*** *en accédant aux systèmes d'information qui*

[1353] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, art.21 à 25
[1354] « *le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation* »

sont à l'origine de l'attaque » (art. L. 2321-2 al 1. Code Défense), ce qui nous conduit à questionner rapidement la congruence entre compétences administrative et judiciaire (1), règles nationales et jurisprudence européenne (2).

1. Esquisse du défi de l'articulation des compétences administrative et judiciaire

La loi qu'il est inutile de paraphraser, dispose que « *pour être en mesure de répondre aux attaques mentionnées au premier alinéa, les services de l'Etat déterminés par le Premier ministre peuvent détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du Code pénal,* ***en vue d'analyser leur conception et d'observer leur fonctionnement*** » (art. L. 2321-2, al 2 Code de la défense).

Neutraliser les effets d'une attaque (**on ne parle pas ici de neutralisation de l'attaquant**) suppose d'en observer le point de départ, et le mode de distribution jusqu'à sa cible.

* Mais pour cela, les services de l'Etat ne disposent finalement que de **peu d'outils en droit.** Ce sont majoritairement les articles L. 852 et suivants du Code de la sécurité intérieure (CSI), qui constituent l'essentiel de la boîte à outils de l'analyste qui opérera les premiers constats.

Or, ces articles (qui permettent par exemple l'interception d'une adresse IP suspecte), ont été initialement prévus par le législateur pour les atteintes aux intérêts fondamentaux de la Nation dans leur conception classique [1355]. L'article L. 811-3 CSI en liste les motifs de façon stricte. Paradoxalement, ces motifs **ne couvrent pas la prévention** des ingérences cyber, puisque l'on ne peut en préjuger du but de l'ingérence, même lorsqu'elle est établie.

Ainsi, dans l'art. L. 811-3 CSI, les seuls motifs autorisant le recours aux techniques par les services de renseignement pour but de prévention, sont (4°) la prévention du terrorisme (qualification qui pourrait englober certains types d'agression cyber mais pas toutes, nous l'avons vu) ; et (5°) la prévention de menaces critiques listées de façon restrictive [1356]. **Le législateur semble avoir considéré que la cyber n'était qu'un moyen technique**, dont la motivation procède soit du domaine de l'espionnage, soit du domaine criminel.

[1355] La création également en est récente, voir Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.
[1356] La liste du 5° est exhaustive, et vise la prévention « *a) Des atteintes à la forme républicaine des institutions; b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; 6° La prévention de la criminalité et de la délinquance organisées ; 7° La prévention de la prolifération des armes de destruction massive* ».

* En outre, le propre de l'action cyber, est qu'elle compromet pour son seul fonctionnement toute une série d'équipements (serveurs, ordinateurs, réseaux), ces compromissions connexes étant autant d'éléments constitutifs d'une infraction. Mais les infractions même pénalement constituées « en cascade » (ce qui est de fait fréquent), **ne sont pas *ipso facto* rattachables aux motifs légitimes d'action** tels que définis dans l'article L. 811-3.

Or, ces motifs **supposent la qualification spéciale d'une intention sous-jacente**, qui dépasse la seule caractérisation pénale au sens des articles 323-1 à 323-3 du Code pénal. Dès lors, le risque est fort que les organes de contrôle administratif (dont la Commission Nationale de Contrôle des Techniques de Renseignement) ou juridictionnel (Conseil d'Etat, Cour de cassation – voire le Tribunal des Conflits) soient seuls en charge de trancher ce qui doit relever de la police administrative ou judiciaire, dans un contexte de congruence que nous venons de voir relative, entre Codes de la défense et de la sécurité intérieure.

Agir en cyber défense (**caractérisation d'attaque pour la neutralisation d'effets**) ne relèverait-il que de la compétence judiciaire ? Loin de là, comme peuvent l'enseigner un nombre important d'attaques non attribuées, faute de pouvoir remonter à leurs auteurs, ou de pouvoir les traiter judiciairement lorsque le commanditaire ou l'attaquant lui-même est un Etat, nous l'avons vu.

* Par ailleurs, les équilibres recherchés spécialement par le Sénat français, lorsque la loi sur le renseignement y a été débattue en 2014, reposaient également sur le **caractère proportionnel des moyens mis à la disposition** des services et leur subsidiarité.

Dès lors, l'interception, par exemple d'une adresse IP pour documenter ou comprendre une attaque, n'est possible **qu'après avoir préalablement mis en œuvre une réquisition administrative** prévue à l'article L.851-1 permettant d'identifier l'utilisateur et de connaître des connexions réalisées depuis ou vers celle-ci.

Or, le délai de mise en œuvre n'est pas toujours compatible avec la rapidité de l'attaquant, ou avec les artefacts qu'il aimera laisser ici et là, pour masquer ses traces. Dès lors, il était nécessaire de disposer **d'une capacité à agir sur les communications internationales**, ce qui a été prévu en 2019 par les articles L. 854-1 à L. 854-9 du même code.

2. Esquisse du défi de l'articulation des règles entre droits nationaux et communautaire

Citons ici un autre point d'intérêt, non plus d'articulation administrative/judiciaire française, mais d'articulation nationale/européenne. Connaître un attaquant sur le plan télécom, suppose l'exercice d'un pouvoir de réquisition **auprès des opérateurs autorisés à opérer sur le territoire national**. Leur aptitude à répondre repose, en grande partie, sur les traces électroniques qu'ils conservent nécessairement pour motif de facturation.

Or, en Europe, cette facturation est le plus souvent mensuelle. Le code des télécommunications dans son article 10-13 prévoit *que les données techniques permettant d'identifier la source d'une connexion ou celles relatives aux équipements terminaux utilisés doivent être conservées pendant un an à compter de la connexion ou de l'utilisation des équipements terminaux.* Ces dispositions se trouvent certes renforcées pour certaines infractions, liées au terrorisme [1357] ; mais nul cyber ici non plus, dans les choix du législateur.

En outre, ce dispositif en soi perfectible donc, est bousculé par les décisions successives de la CJUE, tirées des affaires « *Digital Right* » [1358], puis « *Télé 2 Sveridge* » [1359], qui consacrent un **principe d'interdiction de conservation généralisée et indifférenciée** : le droit de l'Union s'oppose « *à une conservation généralisée et indifférenciée, **à titre préventif,** des données de trafic et de localisation aux fins de lutte contre la criminalité, quel que soit son degré de gravité* » [1360].

Or, si la capacité des Etats membres de l'Union à détecter et à relever le départ d'une attaque cyber, relève de leur aptitude à observer ce qui transite sur leurs réseaux, cette aptitude est intrinsèquement liée aux dispositifs nationaux de police administrative de chacun : **cela semble ainsi compromis par une orientation contraire du droit communautaire**.

[1357] Article 6, II de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[1358] CJUE, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland Ltd*.
[1359] CJCUE, C 203-15, 21 déc. 2016, *Tele2 Sverige AB*.
[1360] CJUE 6 oct. 2020, aff. C-511/18, C-512/18, C-520/18, *La Quadrature du Net et a.* Multiples commentaires et observations AJDA 2020. 1880 ; D. 2021. 406 note M. Lassalle ; *ibid*. 2020. 2262, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; AJ pénal 2020. 531 ; Dalloz IP/IT 2021. 46, obs. E. Daoud, I. Bello et O. Pecriaux ; Légipresse 2020. 671, étude W. Maxwell ; *ibid*. 2021. 240, étude N. Mallet-Poujol ; RTD eur. 2021. 175, obs. B. Bertrand ; *ibid*. 181, obs. B. Bertrand ; *ibid*. 973, obs. F. Benoît-Rohmer.

Suite à plusieurs décisions en avril 2021 du Conseil d'Etat [1361] (et en 2022 de la Cour de cassation, tirant les conséquences de la jurisprudence européenne [1362]), trois décrets ont été adoptés en octobre 2021 : le premier sur la politique générale de conservation des données de connexions [1363] ; le second afin de permettre l'identification d'une personne ayant créé un contenu en ligne [1364] ; le troisième décret, qui nous intéresse plus spécifiquement, en cas de « ***menace grave et actuelle*** » contre la sécurité nationale [1365].

Cette qualification appelle naturellement une réflexion approfondie quant à son champ, imminence, etc. tant elle est décisive, et pose la question du recoupement réaliste avec les enjeux de la prévention cyber.

Pour les infractions pénales, le Conseil d'Etat a lui même relevé en 2021 que « *la solution suggérée par la CJUE de conservation ciblée en amont des données* ***n'est ni matériellement possible, ni – en tout état de cause – opérationnellement efficace****. En effet, il n'est pas possible de pré-déterminer les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu où elle sera commise* » [1366]. Il n'est pas lieu ici d'entrer plus allant dans ces questions qui intéressent au premier chef les praticiens du droit pénal, plus que l'articulation des Codes de la défense et de la sécurité intérieure, dont la question de la congruence pour notre propos, se situe sur un terrain différent.

Pour la prévention de l'agression cyber (qui est en soi une infraction pénale, quelques en soient les motifs), dans le but rappelons-le d'en neutraliser les effets, notons seulement que dans l'espace européen, il semble que **seule l'analyse des atteintes déclarées ou observées (donc dans le champ judiciaire)** fasse en l'état consensus au plan européen. C'est ce qui semble pouvoir être inféré du renforcement de la politique de lutte voulue par le Conseil, et de l'accroissement des moyens d'Europol : **cela ne consacre que le volet strictement criminel, à volet presque exclusivement judiciaire.**

[1361] CE (en arrêt d'Assemblée), 21 avril 2021, n°393099, n°394922, n°397844, n°397851, n°424717, n°424718), publié au recueil Lebon.
[1362] Crim 12 juillet 2022, pourvois n°21-83.710 ; n° 21-83.820 ; n°21-84.096 ; n° 20-86-652 ; voir Nicaud B, « Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE », Dalloz 2022.
[1363] Décret n° 2021-1361 du 20 octobre 2021 relatif aux catégories de données conservées par les opérateurs de communications électroniques.
[1364] Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.
[1365] Décret n° 2021-1363 du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion.
[1366] Conseil d'Etat, communiqué : « Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité », 21 avril 2021.

Pour la connaissance et l'anticipation des atteintes cyber, un sursaut pourrait-il naître de la politique européenne de sécurité commune (PESC) ? Rejoindra-t-elle l'approche de l'OTAN, sur la reconnaissance conceptuelle des « affrontements hybrides » et leurs manifestations dans des champs d'importance nationale vitale – dont la santé, et l'intégrité des données qui s'y rapportent ?

SYNTHESE P2T2C2

Ce second chapitre restituait les résultats de notre recherche quant à la dynamique telle qu'exprimée en droit, des politiques des Etats membres de l'Union sous son égide, pour la garantie coordonnée face aux ingérences d'Etats tiers par voie de fait, que nous relevons ici spécialement dans le domaine des STAD de santé. La difficulté est double : technique pour réduire la vulnérabilité des systèmes et données en général ; politique, dans l'attribution de telles atteintes à des Etats utilisant des techniques voire des intermédiaires cybercriminels, ce qui marque un renouvellement des modes d'action, entre guerre froide et chaude.

* dans une première section, nous examinons la dynamique des ingérences a priori non attribuables dans les données de santé, en relevant la façon dont elles sont perceptibles et pistées. Nous relevons que les systèmes de traitement automatisés et les données sont en santé devenu des cibles privilégiées d'attaques, après n'en avoir été que victimes collatérales, et examinons la mise en place en santé de procédures de notification. Puis nous esquissons l'analyse des modes d'ingérence, rapportant tout à la fois l'emprunt d'outils de niveau étatique par des cybercriminels, et l'emprunt d'outils cybercriminels par des acteurs étatiques. Ces constats de fait, sans difficulté véritable de qualification pénale, introduisent une problématique ardue : l'attribution des ingérences, lesquelles soulèvent des problèmes souvent plus politiques que techniques ; ceci notamment en l'absence de conflit déclaré, et donc d'applicabilité du droit international public sur ses bases classiques, et l'assurabilité des dommages selon le fondement invoqué.

* dans une seconde section, nous examinons face à ces atteintes à la souveraineté, l'accélération de la recherche de garanties coordonnées, de façon générale mais avec une focale particulière sur le secteur emblématique de la santé. Nous y relevons l'extension toute récente par NIS2 des normes communes à la protection des infrastructures, dont

l'élargissement dans le champ de la santé de celle de qualification « hautement critique », et l'extension prévue des normes de protections en matière de tous produits connectés, qui nous conduit toutefois à relever l'autonomie juridique des dispositifs médicaux en la matière. A l'examen de la dynamique des normes succède l'examen de la dynamique des compétences, qui fait relever l'extension de la compétence des opérateurs dont notamment l'ENISA, mais laisse en suspend la question des régimes procéduraux hors droit commun de réponse aux ingérences cyber, conduisant à s'interroger sur la répartition des compétences et les règles de réaction, question d'actualité non publique.

SYNTHESE P2T2

Ce second titre avait pour objet l'analyse, toujours au travers du fil rouge de la donnée de santé, des dynamiques de recherche contemporaine par les Etats membres de l'Union, de garanties coordonnées contre les accès illicites d'Etats tiers notamment, aux données de santé. Notre recherche nous a conduit à distinguer deux types d'accès illicite, selon qu'ils se revendiquent d'une voie de droit, dont l'adéquation avec le droit européen doit alors être contrôlé ; ou selon qu'ils procèdent d'une voie de fait, qui se dissimule généralement sous la cybercriminalité avec laquelle elle se confond pénalement.

La question de la protection contre les accès illicites par voie de droit est posée par les cadres de transfert de données entre systèmes juridiques, lesquels transferts étant subordonnées au contrôle d'adéquation de l'ordre juridique de l'Etat de destination au regard des droits fondamentaux protégés par l'Union, mais aussi implicitement des intérêts souverains des Etats qui la composent. Dans ce champ, le contrôle d'adéquation a donné lieu à une série de contentieux et pourrait encore être soumis à la CJUE (un parlementaire français ayant en septembre 2023 décidé d'attaqué le nouveau cadre « DPF »), lequel a supposé une adaptation du droit fédéral américain et des mesures en cours dans le champ des activités de renseignement. Les enjeux économiques bilatéraux associés au transfert des données montrent l'ampleur de la dépendance réciproque, qui est plus une dépendance européenne en l'état pour les serveurs et les infrastructures, non sans poser de délicates questions de compétitivité à l'ère de l'IA.

La question de la protection contre les accès illicites par voie de fait est le second domaine emblématique de transformation pour la souveraineté des Etats membres et de l'Union. Ce champ ombrageux de compétence régalienne est le terrain d'adoption accélérée de normes et

de standards de protection d'infrastructures, de produits et de services, du fait de l'interconnexion et de la vulnérabilité immédiate des données et systèmes spécifiquement en santé.

CONCLUSION THESE

Cette rédaction a rendu compte du fil rouge de notre recherche sur ce thème transverse : la donnée de santé, du fait de sa place au carrefour des intérêts publics et des droits fondamentaux, dans une géopolitique aux moyens renouvelés.

Cette thèse était une fin en soi, du fait de l'intérêt de fond souligné en introduction ; mais aussi un prétexte pour des réflexions méthodologiques appliquées à des champs externes à cette seule rédaction. A nouveau, notre gratitude à notre directeur de thèse le Pr. Megerlin, pour son consentement à cette approche, et à notre méthode de travail, originales.

Notre recherche avait pour but de relever les dynamiques de la « donnée de santé » dans le champ de la souveraineté numérique : qui peut par là décrire, expliquer, prédire des états et tendances en santé, induire des comportements individuels et/ou populationnels, voire étatiques ? **que protéger donc en droit, comment ?** limitons nous à quelques points de base :

- en droit, il n'existe pas de définition opérante de la notion de « donnée de santé » : la définition existante depuis 2016 est tautologique, comme en témoigne le rajout jugé nécessaire dans la proposition de règlement EESD en 2022 ;
- en l'absence de définition opérante, il est nécessaire de conceptualiser des critères de qualification, que nous avons proposés ; mais aucun n'apparaît satisfaisant, des données passant par les mailles du filet du fait de leur origine ou usage externe ;
- l'extranéité de telles données au champ de protection renforcée ne les prive pas pour autant de la protection du droit commun européen des données personnelles, mais cela fait sous-estimer l'enjeu de leur signification spécifique ;
- en l'état, il n'existe pas de contentieux français de qualification des données de santé (quand la loi nationale s'applique seule) ; ni européen, car jusqu'alors, la donnée n'était pas une entité vouée à une circulation intracommunautaire intensive ;
- l'annonce de catégories « prioritaire » et « minimales » de données de santé, pour des utilisations « primaires » (données personnelles) ou « secondaires » (données

anonymisées) à l'échelle européenne, pourrait changer la donne, du fait, au-delà de la question des droits fondamentaux, de l'enjeu compétitif qui en résulte;

- la notion de « qualité » de la donnée introduite par la réflexion sur la régulation des utilisations secondaires est distincte des prétentions d'auteurs qui soutiennent, en matière de qualité de recherche observationnelle, la pertinence du droit français de la « recherche impliquant la personne humaine », dont la clarté à cet égard est en question ;
- la proposition de droit européen en 2022 use d'une subtilité pour attirer vers le champ de protection des données de santé, des données issues d'applications de « bien-être », ces dernières devant être enregistrées selon un droit spécifique pour abonder les bases de données de santé à usage primaire et secondaire ;
- le droit français a anticipé l'abondement possible de dossiers de données de santé par des technologies pourtant non médicales et leur dialogue, sous réserve de leur référencement dans un catalogue de services dont les critères ne sont, à cette date, pas encore posés ;
- en dépit de ses enjeux stratégiques en lien avec l'intelligence artificielle, la notion de « donnée synthétique », qui commence à se diffuser en santé, ne présente *quasi* pas d'occurrence dans les propositions de textes européens les plus avancés en la matière ;
- l' « anonymisation » des données personnelles et son irréversibilité supposée, sont un point critique déterminant de la confiance future dans le système européen, où les normes en gestation entendent permettre de massifier les données pour faciliter leur exploitation : cela les rend en fait et en droit accessibles à des algorithmes toujours plus performants ;
- d'autres points évoqués sur les questions d'ingérence de droit et de fait par des Etats tiers ne sont pas propres au STAD de santé ; ceux-ci sont ici une clef de réflexion et d'explication, du fait de leur dimension emblématique et des obligations spécifiques face aux risques de cyber agressions.

Notre recherche a ainsi rapporté et analysé le débordement de l'approche historique de régulation, du fait de la diversification des acteurs, techniques et usages, de la multiplication des sources de données et leur dissémination au sein des systèmes, de l'ébranlement de leurs catégories pourtant tout récemment fixées ; de la porosité des systèmes du fait d'interactions choisies ou non, des transferts internationaux et des risques spécifiques d'ingérences, notamment par des approches invasives et par les nouvelles puissances de calcul.

L'approche classique de la qualification de « donnée de santé » bute sur ces phénomènes ; nous en avons relevé les conséquences et le besoin, non de leur endiguement impossible, mais d'encadrement notamment préventif par une palette d'outils inédits.

Certains de ces outils viennent (fin 2022) d'être proposés au niveau européen ou sont parfois en gestation dans un sens intéressant dans ces champs régaliens, en matière d'infrastructures, de nouvelles qualifications (données, technologies, utilisations), de garanties contre les ingérence, par des cadres de transferts formalisés et les progrès communs en cyber sécurité et cyber résilience. Ils ont l'objet de réflexions en cours sur lesquelles nous ne nous sommes pas étendu.

D'autres réflexions nous semblent devoir être approfondies (problème des ré-identifications à la faveur des volumes massifiés ; défis des données synthétiques en santé pour les systèmes décisionnels notamment), dans une ère où la maîtrise technologique a cessé d'être l'apanage des Etats, et où la géopolitique s'est retendue avec des outils nouveaux.

Bibliographie indicative

Comme indiqué en introduction, le lecteur trouvera ici des références non systématiquement rapportées au bas des pages. Tel est le cas, lorsqu'elles ont pu éclairer le contexte de notre réflexion professionnelle, mais ne l'ont pas déterminée : dès le début de notre recherche, notre intention était en effet, plutôt qu'une méta-analyse (analyse d'analyses) de littérature, une analyse juridique et un **rapprochement de première main des textes-source** en situation.

Les propositions et projets de noprmes en discussion ne sont pas rapportés en bibliographie, du faite de leur nature, mais systématiquement en note de bas de page là où ils sont étudiés.

En contraste, des liens internet ou onglets de sites internet (comme ceux institutionnels) ne sont pas reproduits ici : ils ne figurent qu'en bas de page ; tous ont été recontrôlés en 2023.

Ouvrages, rapports institutionnels & parlementaires

Adair S, Hale M, Hartsein B et al. *Malware analyst's Cookbook*. Wiley. 2011.

Akman P, *The concept of abuse in EU competition law*, Hart Publishing, 2017.

Alla F, « Les déterminants de la santé », in *Traité de Santé publique*, Lavoisier éd. 2016, pp 15-18.

Allsopp W, *Advanced penetration testing*. Wiley, 2017.

ANSSI, *Maîtrise du risque numérique, l'atout confiance*, 2019.

ANSSI, *Panorama de la menace informatique*, 2021.

ANSSI, *Panorama de la menace informatique*, 2022.

Arouilla J, Ronfeldt D. *Networks and Netwars: the Future of Terror, Crime and Militancy*. Rand, 2001.

Arouilla J. *Bitskrieg, the new challenge of cyberwarfare. Polity, 2021.*

Arpagian N. *Frontières.com*. L'Observatoire, 2022.

Arpagian N. *La cybersécurité*. PUF, 2018.

Arutunyan A. *Hybrid Warriors, Proxies, Freelancers and Moscow's Struggle for Ukraine*. Hurst Publisher, 2022.

Audit B., *Droit international privé*, Economica, 3ème éd. 2001.

Austin G. *Cybersecurity in China: The next wave*. Springer. 2018.

Badouard R. *Le désenchantement de l'internet. Désinformation, rumeur et propagande*. FYP éditions, 2017.

Bellanger, P. *La souveraineté numérique*, Paris, Stock Ed. 2014.

Benkler Y, Faris R, Robert H. *Network propaganda: Manipulation, Disinformation, Radicalization in American Politics*. Oxford University Press.,2018.

Bévière-Boyer B., « Droit, intelligence artificielle et système de santé », in Bouteille-Brigant M. [dir.], *La personne face à l'intelligence artificielle*, IFJD, 2021.

Billois G, Cougot N. *Cyberattaques, les dessous d'une menace mondiale*. Hachette. 2022.

Bortzmeyer S, *Cyberstructure, l'Internet un espace politique*. C&F Editions, 2018.

Bothorel E., Combes S., Vedel R. « Pour une politique publique de la donnée », Rapport déc. 2020.

Boulard A, Favier-Baron E, Woillet S, *Le business de nos données médicales – enquête sur un scandale d'Etat* FYP éd., 2021.

Bouteille-Brigant M. [dir.], *La personne face à l'intelligence artificielle*, IFJD, 2021.

Bras P-L., Loth A., Rapport sur la gouvernance et l'utilisation des données de santé, 2022.

Brenner S, *Cyberthreats, the emerging fault line of the Nation State*. Oxford University Press. 2009.

Bruyère B., Les psychologues et le secret professionnel, Ed. Armand Colin, 2011.

Bryant W, *International Conflict and Cyberspace superiority*. Routledge, 2016.

Buchan, R. *Cyberespionage and international law*. Hart Publishing, 2018.

Buchanan B, *The Hacker and the state: The New Normal of Geopolitics*. Harvard University Press, 2020.

Buchanan, B. *The Cybersecurity Dilemna : Hacking, Trust and Fear Between Nations*. C Hurst Co Publishers, 2019.

Cardot, P. *Cybersouveraineté : mythe ou défi ?* Uppr Ed., 2016.

Carreau D, Haman A, Marrella F, *Droit international*, Pedone, 13ème éd., 2022.

Cattaruzza A, Danet D, Taillat S. *La cyberdéfense, politique de l'espace numérique*. Armand Colin ; 2023.

CEDH, Guide sur l'article 14 de la Convention européenne des droits de l'homme et l'article 1 du Protocole n°12 à la Convention – interdiction de la discrimination (2022).

Chaltiel F, *La Souveraineté de l'État et l'Union européenne, l'exemple français*, LGDJ, 2000.

Chavalarias D, *Toxic Data*. Flammarion, 2022.

Chesney R, Smeets M. *Deter, Disrupt, or Deceive, Assessing Cyber Conflict as an Intelligence Contest*. Georgetown University Press, 2023.

Choucri N, Clark D, *International Relations in the Cyber Age. The Co-Evolution Dilemma*. The MIT Press, 2019.

Clarke R, Knake R. *Cyberwar: the next Threat to National Security and what to do about it*. Ecco Press, 2010.

Clough J. *Principles of cybercrime*. Cambridge University Press, 2015.

CNIL, *Le corps, nouvel objet connecté*, Cahiers Innovation & Prospective n°02, mai 2014.

Coll., *Lexique de biopolitique. Les pouvoirs sur la vie* (trad. de l'italien), Érès, 2009.

Conseil d'Etat, *L'engagement de la responsabilité des hôpitaux publics* (dossier thématique), janv. 2015.

Conseil d'Etat, Loi bioéthique - Rapports et Etudes, 2018.

Conseil d'Etat, Rapport « Santé et protection des données », La documentation française, 2019.

Conway-Mouret H., Le Gleut R. « *Rapport Défense européenne, le défi de l'autonomie stratégique* », Sénat, 3 juillet 2019, n° 626 (2018-2019).

Cornu G., *Vocabulaire juridique, Quadrige/PUF, 13ème édition, 2020.*

Cour des comptes, « Les données personnelles de santé gérées par l'assurance maladie, une utilisation à développer, une sécurité à renforcer » Rapport 2016.

Cristiano F, Broeders D, Delerue F et al. *Intelligence artificielle et conflit international dans le cyberespace*. Taylor & Francis. 2023.

Delerue, F. *Cyberoperations and International Law*. Cambridge University Press. 2020.

DeNardis L, *The Internet in everything*. Yale University Press, 2020.

Dosse S, Kempf O, Malis C, *Cyberespace, nouveau domaine de la pensée stratégique*. Économica, 2013.

Dreyer E, *Droit pénal spécial*, LGDJ, 2020.

Dylstra J, Eugene S, Leigh M, *Cybersecurity myths and Misconceptions*. Pearson Education, 2023.

Egloff F. *Semi-State Actors in Cybersecurity*. Oxford University Press Inc, 2022.

ENISA, « Panorama des menaces », Rapport juill. 2023.

ENISA, Cybersecurity Threat Landscape Methodology, juil. 2022.

ENISA, *Foreign Information Manipulation and Interfrence (FIMI) and Cybersecurity – Threat Landscape*, déc. 2022, ISBN: 978-92-9204-606-4.

EO 14086 « *Enhancing Safeguards for United States Signals Intelligence Activities* », E.O. 14086 of Oct 7, 2022 ; FR doc. 2022-22531.

FBI, Cyber Division, Notification Private Industry, n° 20220912-001, 12 sept. 2022 (TJP :WHITE).

FDA, « Cybersecurity vulnerabilities of hospira symbiq infusion system » : FDA saf. comm. 2015

Freyssinet E, *La cybercriminalité en mouvement*. Hermes Science Publications, 2012.

Galeotti M, *The Weaponisation of Everything: A Field Guide to the New Way of War*. Yale University Press, 2022.

Gastineau P, Vasset Ph, *Armes de déstabilisation massive. Enquête sur le business des fuites de données*. Fayard, 2017.

Gergorin JL, Isacc-Dognin L, *Cyber, la guerre permanente*. Les éditions du Cerf. 2018.

Gonsalves R, « GANscapes: Using AI to Create New Impressionist Paintings » *Towards Data Science*, 2019.

GT « Article 29 », « Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques », février 2007, WP 131, point II.2.

HAS, « Accès précoce des médicaments : accompagnement des laboratoires », 2021.

HAS, « Autorisation d'accès précoce aux médicaments : doctrine d'évaluation de la HAS », 2021.

HAS, « Évaluer les dispositifs médicaux connectés, y compris ceux faisant appel à l'intelligence artificielle », 2022.

HAS, « Référentiel de bonnes pratiques sur les applications et les objets connectés en santé *(mobile Health ou mHealth) »,* 2016.

Haut Comité Juridique de la Place financière de Paris, « Rapport sur l'assurabilité des risques cyber », 28 janvier 2022.

Hecker M, Rid T, *War 2.0: Irregular Warfare in the information Age*. Praeger, 2009.

Henning L, *Unilateral Remedies to Cyber Operations*. Cambridge University Press, 2020.

Hubbard D, Seiersen R, *How to measure anything in cybersecurity risk*. John Wiley & Sons, 2023.

Hypponen M, *If it's smart, it's vulnerable*. Wiley, 2022.

Jamieson KH, *Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know*. Oxford University Press, 2020.

Jancczewsky L, Colarik A, *Cyber warfare and Cyberterrorism*. Information Science Reference, 2007.

Junien Cl., Priollaud N., *C'est votre sexe qui fait la différence*, Plon, 2023.

Kitchin R, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE, 2014.

Klimburg A, *The Darkening Web: The War for Cyberspace*. Penguin Press, 2017.

Lamy S, *Agora toxica*. Éditions du détour, 2022.

Laurent S-Y, *Conflits, crimes et régulations dans le cyberespace*. ISTE Group. 2021. vol.4.

Lemke C, *Ma Santé, mes données*, CPI éd., 2021.

Liang Q, Xiangsui W, *La guerre hors limites*. Les éditions du Cerf, 1999.

Libicki M, *Cyberdeterrence and Cyberwar*. RAND Project Air force, 2009.

Londsdale D. *The Nature of War in the Information Age*. Frank Cass, 2004.

Long M, Balladur E, Léotard F, *Livre Blanc sur la Défense*, Documentation française, 1994.

Longuet G, « Le devoir de souveraineté numérique », Rapport fait au nom de la commission d'enquête du Sénat, n° 7 tome I (2019-2020) - 1 octobre 2019.

Lutun A, *Le Big Data en santé, richesse et conditions d'accès*, thèse pour le doctorat en droit, Paris, 2021.

Maisnier-Boché L, Fasc. 945 : Données de santé à caractère personnel – Régime général, Jurisclasseur Communication, Lexis 360, 2023.

Latombe Ph, Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne », Rapport déposé à l'Assemblée nationale sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne », n° 4299 enregistré le 21 juin 2021.

Megerlin F, Fascicule 8-10 « Données de santé », *in* Traité de droit pharmaceutique Litec, Jurisclasseur LexiNexis, 2023.

Megerlin F, *Ordre public transnational et arbitrage international de droit privé – essai critique sur la méthode*, Thèse pour le doctorat en droit, université Paris II, PU Septentrion, 2000.

Mitnick K, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. John Wiley & Sons, 2005.

Morin-Desailly C*, Rapport d'information fait au nom de la commission des affaires européennes : « l'Union européenne, colonie du monde numérique ? »,* Rapport d'information n° 443 (2012-2013), 20 mars 2013.

Moussy H., *Les topographies médicales françaises des années 1770 aux années 1880 : essai d'interprétation d'un genre médical*, thèse de doctorat en histoire, Université Paris 1, 2003.

Parcu P.L., Monti G., Botta M., *Abuse of Dominance in EU Competition Law : Emerging Trends*, Edward Elgar Publishing, 2012.

Patino B, *Tempête dans le bocal, la nouvelle civilisation du poisson rouge*. Grasset et Fasquelle, 2022.

Payne K, *I, Warbot: The Dawn of Artificially Intelligent Conflict*. Hurst Publishers, 2021.

Pelroth N, *This is How they Tell me the World Ends: the Cyberweapons Arms Race*. Bloomsburry Publishing, 2021.

Perkovich A, *Understanding Cyber conflict: 14 analogies*. Georgetown University Press, 2017.

Petit N., *L'abus*, in Droit européen de la concurrence – Chapitre IV – Section III, Lextenso, 2018.

Porche I, *Cyberwarfare: An Introduction to Information-Age Conflict*. Artech House, 2019.

Raimondo L, *Les fondamentaux de la gestion de crise cyber*. Ellipses, 2022.

Rains T, *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd., 2020.

Rains T, Youngblood, TCISSP. *Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization*. Packt Publishing Ltd., 2023.

Rascagneres P, Larinier S, *Cybersécurité et Malwares. Détection, analyse et Threat Intelligence*. ENI. 2022.

Rid T, *Active Measures: The Secret History of Disinformation and Political Warfare*. Profile Books Ltd., 2020.

Roscini M, *Cyber Operations and the Use of Force in International Law*. Oxford University Press. 2014.

Salamon Y, *Cybersécurité et cyberdéfense : enjeux stratégiques*. Ellipses, 2020.

Sanger D, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. Crown, 2019.

Schmitt MN, Vihul L, *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge, Royaume-Uni. Cambridge university press, 2017.

Sejean M. *Code de la cybersécurité*. Lefevre Dalloz, 2022.

Sénat, Rapport d'information n°678 « La cybersécurité des entreprises – Prévenir et guérir : quels remèdes contre les cyber virus ? », 10 juin 2021.

Sénéquier A., *Géopolitique de la santé*, Eyrolles 2023.

SGDSN, *Revue stratégique de cyberdéfense*, 12 février 2018.

Singer PW, Brooking ET, *LikeWar: The Weaponization of Social Media*. Mariner Books, 2019.

Steffens T, *Attribution of Advanced Persistent Threat*. Springer Vieweg, 2020.

Van Puyvelde D, Brantly A, *Cybersecurity. Politics, Governance and Conflict in Cyberspace*. Polity, 2019.

Volkoff V, *La désinformation : arme de guerre*. L'Age d'homme, 2004.

Articles de doctrines & notes de jurisprudence

Accenture, « Losing the Cyber Culture War in Healthcare: Accenture 2018 Healthcare Workforce Survey on Cybersecurity ».

Accoce P, « Secrets et défense médicale - Chefs d'Etat et dirigeants s'efforcent de tout savoir sur la santé de leurs pairs. Et de ne rien laisser paraître de la leur », *in* L'Express, 23 juin 1998.

Adams J, Hillier-Brown FC, Moore HJ et al. « Searching and synthesising 'grey literature' and 'grey information' in public health: critical reflections on three case studies ». Syst Rev. 2016 Sep 29;5(1):164

Aker S.D, Knudsen J, Ahmadi D.M, « The Wireless challenge : security and safety for medical devices and Hospitals ». *Biomed Instrum technol*, mai 2013, 208-211.

Alberto I.R., Alberto N.R., Ghosh A.L., Jain B. et al, « The impact of commercial health datasets on medical research and health-care algorithms », Lancet Digit Health, mai 2023, vol 5, 288-294.

Armstrong DG, Kleidermacher DN, Klonoff DCet al., « Cybersecurity regulation of wireless devices for performance and assurance in the age of « medjacking ». *J Diabetes Sci Technol*. 2016 Mar; 10(2): 435–438.

Arora A. et A, « Synthetic data in health care : a widening legal loophole », *The Lancet,* 23 avril 2022 *;* vol. 399, issue n° 10335, p 1601-1602.

Aungst TD, Clauson KA, Misra S, Lewis TL, Husain, (2014), I. How to identify, assess and utilise mobile medical applications in clinical practice. Int J Clin Pract ; 68(2):155-62.

Bannelier K. et Christakis T., *Cyberattaques – Prévention-Réactions : Rôles des États et des acteurs privés*, *Les Cahiers de la Revue Défense Nationale*, Paris, 2017.

Bannelier K., Christakis T., « Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la Revue Stratégique de cyberdéfense de la France et le projet de loi ACDC aux Etats-Unis », *Rev. Stratégique* 2017 n°117, pp 99-118.

Bardford L., ABoy M., Liddell K., « Standard contractual clauses for cross-border transfers of health data after *Schrems II », Journal of Law and the Biosciences*, 2021 Jun 21;8(1):lsab007.

Barrett B, « Petya Ransomware: What You Need to Know » 27 juin 2017, *Wired*, https://www.wired.com/story/petya-ransomware-what-you-need-to-know.

Bates M, « Tracking Disease: Digital Epidemiology Offers New Promise in Predicting Outbreaks » IEEE Pulse. 2017 Jan-Feb;8(1):18-22.

Baumfeld A., Reynolds, R. Caubel P., Azoulay L., Dreyer N.A., « Trial designs using real-world data: The changing landscape of the regulatory approval process », Pharmacoepidemiol Drug Saf. 2020 1201- 1212.

Bellamy F.D., « US data privacy laws to enter new era in 2023 », Reuters, 12 janvier 2023.

Bender JL, Yue RY, To MJ, Deacken L, Jadad AR. « A lot of action, but not in the right direction: systematic review and content analysis of smartphone applications for the prevention, detection, and management of cancer ». J Med Internet Res 2013 ;15(12):e287.

Bensoussan-Brulé V, « Focus : le traitement juridique et judiciaire des cyberattaques », site internet cabinet Bensoussan, mai 2021.

Bernier A., Molnàr-Gàbor F., Knoppers B.M., « The international data governance landscape » J Law Biosci. 2022 Apr 4;9(1):lsac005.

Beyan O., Choudhury A., Van Soest J et al., « Distributed Analytics on Sensitive Medical Data: The Personal Health Train ». *Data Intelligence* 2020 ;2 (1-2): 96–107.

Biden J.R, « Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities », 7 oct. 2022 (non autrement référencé, site maison Blanche).

Bolaños L.A., Xiao D., Ford NL. *et al.*, « A three-dimensional virtual mouse generates synthetic training data for behavioral analysis », *Nat Methods* 2021 ;18, 378–381.

Bories C, « Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point », Rev. dr. homme, 2014 (6) n°5, 1-13.

Bossi-Malafosse J., « Les nouvelles règles d'accès aux bases médico-administratives », Dalloz IP/IT 2016/3, 61-64.

Boulos M., Kwan M.-P. El Emam K. Chung A., Richardson S. et D., « Reconciling public health common good and individual privacy : new methods and issues in geoprivacy », in Intern. Jl. Of Health Geographics vol. 21, 2022.

Bowen C, « WannaCry, Petya and MEDoc: lessons for healthcare », SC Media, 9 août 2017.

Bradford L., Aboy M., Liddell K., « International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection », *Journal of Law and the Biosciences*, jan-jun 2020, Volume 7, Issue 1, 1-33.

Bradford L., Aboy M., Lidell K., « Standard contractual clauses for cross-border transfers of health data after *Schrems II* », *Journal of Law and the Biosciences*, Jan-Jun 2021,Vol 8, Issue 1, 1-36.

Buin, Y. « Normopathie : un mode d'existence ? », Raison présente, 2019/1, 103-108.

Burroni G., « L'influence de la finalité sur la qualification juridique des données de santé », Rev int. dr. éco 2022/3, pp 63-76.

Buzatu A-M, « 15 - Advanced Persistent Threat Groups Increasingly Destabilize Peace and Security in Cyberspace », in *Cyber Pease, Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge U Press, 2022.

Caire G., « Vauban, la Défense et la cohésion de l'économie nationale », Innov. 2008/2 n°28, 149- 175.

Campagne d'attaque du mode opératoire APT31 : description, contre-mesures et code – CERT-FR. (2021) https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/

Cardinal R.N., Moore A., Burchell M., Lewis J.R., , « De-identified Bayesian personal identity matching for privacy-preserving record linkage despite errors: development and validation », *BMC Med Inform Decis Mak*. (2023 May 5).

Cartwright AJ., « The elephant in the room: cybersecurity in healthcare ». *J Clin Monit Comput*. 2023 Apr 24;1-10.

Cattan J, « La mise à disposition des données de santé », Droit administratif n° 5, mai 2016,15-22.

Charpak Y., Chaix Couturier C., Danzon M., « Demander un titre de séjour pour raisons de santé : que sait-on des systèmes de santé des pays d'origine ? » in Trib. De la Santé 2017/4 n°57, 97-106.

Chen A., Chen D, « Simulation of a machine learning enabled learning health system for risk prediction using synthetic patient data » Sci Rep 2022 Oct 26;12(1):17917.

Chen, R.J. Lu M.Y, Chen T.Y. *et al.* « Synthetic data in machine learning for medicine and healthcare », *Nat Biomed Eng* 2021 **5**, 493–497.

Chevrier R., Foufi V., Gaudet-Blavignac C., Robert A., Lovis C., « Use and Understanding of Anonymization and De-Identification in the Biomedical Literature: Scoping Review ». *J Med Internet* 2019 May 31 ; 21(5):e13484.

Church P, Linklaters LLP, "EU & US – The new EU-US data privacy Framework : Third time lucky ?" (2023) https://www.linklaters.com/en/insights/blogs/digilinks/2023/july/eu-and-us--the-new-eu-us-data-privacy-framework--third-time-lucky

Cimino V, « APT31 : le groupe de hackers affilié à l'État chinois s'attaque à la France » in Le Siècle Digital, 23 juill. 2021.

Clemente JD, « Medical Intelligence », Jl of U.S. Intelligence Studies, vol 20 n°2, 2013, pp 73-78.

Cluzel-Metayer, D. « Les données de santé, ou le défi d'un partage sous haute protection », Actes du colloque 40ème anniversaire de l'AFDS, Rev. dr. san. soc. 2022, 149-158.

Cohen K, « Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data », FTC blog, 11 juillet 2022.

Coll., « Comprendre la souveraineté numérique », *Cahiers français*, nº 415, mai-juin 2020

Coll., Dossier « *Quel est l'état de santé de nos chefs d'Etat ? »* Jeune Afrique (2017) https://www.jeuneafrique.com/dossiers/quel-est-letat-de-sante-de-nos-chefs-detat/

Collet L, « Pénurie de médicaments et stocks de sécurité en France : fondement juridique », Bull ANM 2023, 207, pp 136-141.

Conolly C., « The US Safe Harbor - Fact or Fiction? » Privacy Laws & Business International, n°96, déc. 2008, 4-18.

Conseil d'Etat, communiqué : « Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité », 21 avril 2021.

Cook D.A., Triola M., « *Virtual patients: a critical literature review and proposed next steps* », *Medical Education*, 2009, vol. 43, nº 4, p. 303–311.

Cook SE, Palmer LC, Shuler FD, « Smartphone mobile applications to enhance diagnosis of skin cancer: A guide for the rural practitioner ». W V Med J 2015 ;111(5):22-8.

Courage C., « Qualification du dispositif médical : quand les activimètres permettent d'affiner les critères de qualification » (note sous CE 10 février 2020, n° 421576), Rev. dr. et santé 2020, n°97, 981-983.

Crichton C, « L'intelligence artificielle dans la révision de la loi bioéthique », Actualité Dalloz, IP/IT et communication, 16 sept 2021.

Crichton C., « L'intelligence artificielle dans la révision de la loi bioéthique », Dalloz Actu, 16 sept. 2021.

Cyranoski D, « China's massive effort to collect its people's DNA concerns scientists » Nature, 7 juill. 2020.

Dang A., « Real-World Evidence: A Primer », Pharmaceut Med. 2023 Jan;37(1):25-36.

Davis S., Ssemaganda H., Koola J. *et al.*, « Simulating complex patient populations with hierarchical learning effects to support methods development for post-market surveillance ». *BMC Med Res Methodol* 2023 ; 23, 89 ;

Debies E., « L'ouverture et la réutilisation des données santé : panorama et enjeux », RDSS 2016, p. 697-709 ;

Defranoux L, « Fichage génétique en Chine : l'Amérique se réveille » *in* Libération, 22 févr. 2019.

Del Sesto, R. W., Jr, Spies, A., & Guo, J. « How to comply with the new EU-US data privacy Framework »
2023. *www.morganlewis.com*. https://www.morganlewis.com/pubs/2023/07/how-to-comply-with-the-new-eu-us-data-privacy-framework

Deloitte Luxembourg. *Adequacy decision on the EU-US data privacy framework*. (2023). https : //www2.deloitte.com/lu/en/pages/investment-management/articles/adequacy-decision-eu-us-data-privacy-framework.html

Demailly A, « Health data: an introduction to the synthetic data revolution », (Exploratory research), Resolving Pharma, 2021.

Deroudille A et Fatah A, « L'extraterritorialité du RGPD dans le contexte du "Cloud Act" », *RUE 2019*, p. 442.

Desabie J. « L'Insee entreprend d'automatiser le répertoire des personnes », Écon & Stat. 1970, nº 10

Desrosières, (2018), ″Pour une sociologie historique de la quantification. L'argument statistique", Presses de l'École des mines 2008, p. 10-11).

Dilmegani, C. « What is synthetic data ? use cases & ; benefits in 2023 ». *AIMultiple* 2023 https://research.aimultiple.com/synthetic-data/

Dinechin (de), O. « Les poussées d'un droit à la santé », 37-45 in dossier « Droit à la santé », *in* revue Projet 2008/3 (n°304), pp 35-75.

Diogenes Y, Ozkaya E, *Cybersecurity. Attack and Defense Strategies: Counter modern threats and emply state of the art tools and techniques to protect your organization*. Packt Publishing, 2019.

Dodeh S., « Du dossier médical personnel au dossier partagé - Vers un dispositif de médiation documentaire », les Cahiers du numérique 2016, 1/2 pp 31-50.

Dubuis A., « L'article 14 de la directive 2011/24/UE sur le réseau « santé en ligne » : Quel contenu pour quelle application ? », *La santé connectée et "son" droit : approches de droit européen et de droit français, 2017.*

Dumont G.-F., La Covid19, facteur de recompositions géopolitiques, Analyses de population & avenir 2021/1 (vol 24), pp 1-13.

Dupré R., « Les cas de fraude aux certificats de vaccination se multiplient », Le Monde 7 août 2021.

El Emam K ., Jonker E., Arbuckle L., Malin B, « A systematic review of re-identification attacks on health data » PlusOne, 2011;6(12):e28071 (avec erratum « Correction: a systematic review of re-identification attacks on health data » PlosOne, 2015).

Elkam K., Hoptroff R., « The Synthetic Data Paradigm for Using and Sharing Data » Executive Update (Cutter Consortium), Data Analytics & Digital Technologies Executive Update 2019 Vol. 19, n°6, pp 1-10,

ENISA *Threat landscape: Health Sector* (January 2021 to March 2023), ISBN 978-92-9204-638-5. https://www.enisa.europa.eu/publications/health-threat-landscape

Fallery B., « La plateforme de données de santé Health Data Hub » Revue française de gestion 2021/4, pp 141-159.

Farr, C., & Levy, A. « The Trump administration is forcing this health start-up that took Chinese money into a fire sale », 2019, 4 avril. CNBC. https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html

Farrell H, « Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement », Cambridge University Press, 15 avril 2003.

Faure-Mutian V (groupe d'études « Assurance »), Rapport à l'Assemblée Nationale dédié à la Cyber assurance, octobre 2021 (non autrement référencé).

Favret JM, « L'Intégration européenne et la France : quelques réflexions sur la divisibilité de la souveraineté », *RDP 1999*, pp. 741-1764.

Feathers T., Fondrite-Teitler S., Waller A., Mattu S. « Facebook Is Receiving Sensitive Medical Information from Hospital Websites, Pixel Hunt, 2022.

Finlayson S., Bowers J.D., Ito J., Zittrain J. et al, « Adversarial attacks on medical machine learning - Emerging vulnerabilities demand new conversations » Science, 22 mars 2019, vol. 363 issue 6433,1287-1289.

Fombeur P., « Le secret médical partagé », in *Actes du colloque Santé et protection des données*, La documentation française, 2020.

Foster J, *Digital influence mercenaries, profits and power through information warfare*. US Naval Institute Press. 2022.

Franklin JM, Schneeweiss S. « When and How Can Real World Data Analyses Substitute for Randomized Controlled Trials ? » Clin Pharmacol Ther. 2017 Dec. ;102(6):924-933.

Fraser N, Plan F, O'Leary J, Cannon V, Leong R, Perez D, Shen C.E, Rapport Fire Eye, « APT41: A Dual Espionage and Cyber Crime Operation » 7 août 2019, https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

Frost J-H, Massagli M-P., « Social Uses of Personal Health Information Within PatientsLikeMe, an Online Patient Community: What Can Happen When Patients Have Access to One Another's Data », J Med Internet Res. 2008 May 27;10(3):e15.

Gatel M., Quentin D., *Rapport d'information (…) sur le sujet de l'autonomie stratégique de l'Union européenne,* 16 déc. 2021, n°4822.

Gaumont-Prat H., « Aspects éthiques de l'informatisation des données de santé dans la société de l'information », D. 2001, p. 1432.

Ghorbani A., Natarajan V., Coz D. & Liu Y. *Proceedings of the Machine Learning for Health Neur IPS Workshop* (eds Dalca, A. V. et al.) 2020, 155–170.

Ginot L, Kirschen B, Laporte A, « Mise en place d'une poliuqe publique de santé des mignrants », Santé publique 2018/5, pp. 611-616.

Gisel L, « Le droit de la guerre impose des limites mêmes aux cyberattaques », CICR.org. 17 janv. 2013.

Gonzales A, Guruswamy G, Smith SR, « Synthetic data in health care: A narrative review », A narrative review. PLOS Digit Health 2023 Jan 6;2.

Gonzalez R, Thompson J, « Sanctions Recent Developments in U.S. Sanctions: Russia Sanctions, OFAC Enforcement Trends, and Compliance Lessons Learned 2023 », ICLG, 30 sept. 2022.

Guiffard J, « Menace dans le cyberespace : qu'est-ce qu'une APT et pourquoi s'en soucier ? », plateforme *Expressions*, Institut Montaigne, 7 juin 2023.

Guillemain H. et Hanafi N., « Pour une histoire des données médicales - XVIIe-XXIe siècle », in Dossier « Données médicales », Rev. Histoire, médecine et santé (11) Hiver 2022. pp 31-46.

Gupta S*, «* Implantable medical devices-cyber risks and mitigation approaches ». *Cybersecurity in Cyber- Physical Systems workshop*.

Hamel T. « Pandémie Covid-19 : leçons pour le bioterrorisme », Sécurité globale 2020/4, pp 5-42.

Greenberg A, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, 2019.

Groupe Pandoras. *Cybersécurité - méthode de gestion de crise*. VA-Ed., 2021.

Henrard JCl, « Les données de santé et leur utilisation », *Santé Publique*, vol. 34, no. 3, 2022, pp. 333-334.

Hoffman W., Levite A.E. « Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace ? », Rapport pour Carnegie Endwment for international Peace, 14 juin 2017.

Howard-Jones N*, « Les bases scientifiques des conférences sanitaires internationales, 1851-1938 », Chronique OMS,* 1974, 28.

Hradec J., Craglia M., Di Leo M., De Nigris S., Ostlaender N., Nicholson N. (2022), « Multipurpose synthetic population for policy applications », EUR 31116 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-53478-5 (online), doi:10.2760/50072 (online), JRC128595, ;

Hussain M, Al-Haiqi A, Zaidan AA, Zaidan BB, Kiah ML, Anuar NB, *et al.*, « The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations ». Comput Methods Programs Biomed 2015;122(3):393-408.

IQVIA, Institute for Human Data Science. « The Growing value of digital health » 2017 ; https://regresearchnetwork.org/wp-content/uploads/the-growing-value-of-digital-health.pdf

Jeanneney J, « *« Le recours aux intentions du législateur face aux énoncés normatifs ambigus »,* Droit et Philosophie, 2018, vol. 9.

Jeong, S. Yoo, Y.H. Kim, W.H. Shim, « De-Identification of Facial Features in Magnetic Resonance Images: Software Development Using Deep Learning Technology », *J Med Internet Res.* 2020 Dec 10;22(12):e22739.

Juillard-Condat B, Tribaudeau L, Taboulet F, « Accès précoce et compassionnel : quel impact de la réforme en matière de sécurité sanitaire et d'accessibilité ? » RGDM 2022, n°9, 347-374.

Juillard-Condat B, Tribaudeau L, Taboulet F, « Articulation entre accès précoce et l'accès de droit commun aux médicaments : quels impacts peut-on attendre de la réforme de 2021 ? » RGDM n°10, 9-28

Kempf, O. « *La France face au numérique : une souveraineté rénovée ?* », *Rev. Int. Strat*. nº 110, février 2018, p. 109-117.

Kerouedan D, « Diplomatie de la santé mondiale », Santé publique 2013/3, p 253 (éditorial).

Kerouedan D, Pletschette M, « Historique des politiques et de l'architecture institutionnelle de la coopération sanitaire mondiale », in *Traité de la Santé publique*, Lavoisier éd. 2016, pp 614-626.

Kervasdoué (de) J, « Palmarès des hôpitaux du « Point » : les raisons profondes de la censure » *in* Le Point, 10 juillet 2023.

Kim K, Shin Y, Lee J, Lee K. « Automatically Attributing Mobile Threat Actors by Vectorized ATT&CK Matrix and Paired Indicator ». Sensors (Basel) 2021 ; 29;21(19):6522.

Koenig G, Rapport « Mes data sont à moi », Génération Libre, 2018.

Kononowicz A., Woodham L.A., Edelbring S., Stathakarou N, Davies D, Saxena N, Tudor Car L, Carlstedt-Duke J, Car J, Zary N., « Virtual Patient Simulations in Health Professions Education: Systematic Review and Meta-Analysis by the Digital Health Education Collaboration ». *J Med Internet Res.* 2019 Jul 2;21(7):e14676.

Kuo N, Polizzotto M.N., Finfer S., *et al.* « The Health Gym: synthetic health-related datasets for the development of reinforcement learning algorithms ». *Sci Data* 2022, 9, 693;

Labrique AB, Vasudevan L, Kochi E, Fabricant R, Mehl G., « Health innovations as health system strengthening tools: 12 common applications and a visual framework ». Glob Health Sci Pract 2013;1(2):160-71.

Lajarge E., Debiève H., Nicollet Z., « Évolution de la définition de la santé publique » Sant. pub. 2013, 13-40.

Lalanne Berdouticq A.-M., « La politique des indicateurs : usages politiques et scientifiques des indices d'aptitude militaire (France – Grande-Bretagne, 1914-1923), Histoire, médecine et santé 2022 (11), pp 105-122 ;

Lambert K., Barry P., Stokes G, « Risk management and legal issues with the use of social media in the healthcare setting », J Healthcare Risk Management 2012, 23 avr.

Laude A, « Le secret médical partagé », in Santé et protection des données, en TR4 du Colloque du Conseil d'Etat (2017) , La documentation française 2019, 110-116.

Launois R, Ethgen O, « Contrats de risk-sharing : choix des schémas d'étude et des critères de jugement », Ann. Pharm. Fr. n°5, 2013, pp. 346-357.

Le Cun Y, Bengio Y, Hinton G, « Deep learning » *Nature* 2015 ; 521, p. 436-444.

Le Gal Fontes C, Leguelinel G, « De l'importance des données de vie réelle en matière de fixation des prix des médicaments », RGDM 2017, 281-.

Le Gal Fontes C, Rage Andrieu V, « Hébergement des données de santé », Sem Jur. Entreprises 2011 n°9, 1184.

Le Person X, « Usages et discours de la maladie dans l'art de la négociation politique (…) (1585) », *in* Belmas E et Michel MJ (dir.), *Corps, santé, société. Actes du colloque de Paris du 12-13 décembre 2002*, Paris, Nolin, p. 155-172.

Lee P, Bubeck S, Petro J, « Benefits, Limits, and Risks of GPT-4 as an AI Chatbot for Medicine », N Engl J Med 2023; 388:1233-1239.

Legros P, « L'impératif de sécurité des données de santé, de la nécessité technique à l'obligation juridique », introduction au cahier spécial, RIDE 2022/3 pp 13-37.

Lenatti M, Paglialonga A, Orani V et al. « Characterization of Synthetic Health Data Using Rule-Based Artificial Intelligence Models ». IEEE J Biomed Health Inform. 2023 Jan 13; Doi: 10.1109/JBHI.2023.3236722 ;

Lévy M-L, « *Le numéro INSEE : de la mobilisation clandestine (1940) au projet Safari (1974)* », (2000), Dossiers & Recherche, Ined nº 86, p. 23-34

Lippi G, Mattiuzzi C, Cervellin G, « Google search volume predicts the emergence of COVID-19 outbreaks ». Acta Biomed. 2020 Sep 7;91(3):e2020006.

Liss J, D. Peloquin, M. Barnes, B.E. Bierer, « Demystifying *Schrems II* for the cross-border transfer of clinical research data », *Journal of Law and the Biosciences*, July-December 2021Vol 8, Issue 2.

Losing the Cyber Culture war in Healthcare : Accenture 2018 *Healthcare Workforce Survey on Cybersecurity*. (s. d.). https://www.slideshare.net/secret/2bnzxgIzzSTxD4

Makady A, de Boer A, Hillege H, Klungel O, Goettsch, « What Is Real-World Data? A Review of Definitions Based on Literature and Stakeholder Interviews ». *Value Health* 2017;20(7):858-865.

Makady A, Ham RT, de Boer A, Hillege H, Klungel O, Goettsch W, « Policies for use of real-world data in health technology assessment : a comparative study of six HTA Agencies ». *Value Health* 2017;20(4):520-32

Makady A, van Veelen A, Jonsson P, Moseley O, D'Andon A, de Boer A, et al, « Using real-world Data in Health Technology Assessment practice: A comparative study of five HTA agencies ». Pharmacoeconomics 2018;36(3):359-68.

Malin B, « A computational model to protect patient data from location-based re-identification », Artif Intell Med; 2007 ;40(3):223-39.

Mallory C., Chin MG., Lee JC. « Legal Penalties for Physicians Providing Gender-Affirming Care », JAMA 2023;329(21):1821-1822.

Marks M, « Emergent Medical Data: Health Information Inferred by Artificial Intelligence » - 11 UC Irvine L. Rev. 995 (2020-2021) 995 et s.

Martinez J, Tonon C, « La gouvernance des données de santé: leçons de la crise du Covid-19 en Europe, en Chine et aux États-Unis», *Études de l'Ifri*, Ifri, juillet 2021.

Martuscelli C, « How China could choke EU supply of medicines - Europe relies on China for the production of certain key drugs such as antibiotics », Politico, 24 mai 2023.

MASCF, « Les cybercriminels s'attaquent aux professionnels de santé », site MASCF, 15 juin 2020.

Maslow A, « A Theory of Human Motivation », *Psychological Review*, nº 50, 1943, p.370-396.

Mason M, « Biosupremacy: Big Data, Antitrust, and Monopolistic Power Over Human Behavior », *UC Davis Law Review,* juin 2021, 513.

Mason M, « Emergent Medical Data: Health Information Inferred by Artificial Intelligence » - 11 *UC Irvine L. Rev.* mai 2021, 995.

Mason M., Haupt C.E, « AI Chatbots, Health Privacy, and Challenges to HIPAA Compliance ». JAMA. 2023;330(4):309-310.

Maurer T, *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018.

Mayaux L, « Assurance et ordre public : à la recherche d'un critère », RGD Ass, 2008 n°3.

McCoy TH Jr, Hughes MC, « Preserving Patient Confidentiality as Data Grow Implications of the Ability to Reidentify Physical Activity Data », JAMA Network Open 2018;1(8):e186029 ;

Megerlin F, « Intelligence artificielle en santé et responsabilité civile : quelques interactions entre catégories », *Cadre légal des projets d'e-santé*, Editions législatives, Paris, 2019, 140-145.

Megerlin F, Pinilla E, Huriet Cl, « Etudes observationnelles et données de santé « par destination » : quelles protections en droit ? » Rev Gen Dr Méd 2021 (PDP), 151-164.

Megerlin F, Pinilla E, Huriet Cl, « Recueil de données sur les médicaments en accès précoce : quel lien avec la recherche 'impliquant' les personnes humaines ? » Rev Gen Dr Méd 2022 (PDP), 375-388.

Megerlin F, **«** Technologies de santé : vers l'achat de « résultats » ? Rev. dr. san. soc. Dalloz 2022, Hors série, Actes du 40ème anniversaire de l'AFDS – Paris La Sorbonne, 135-147.

Megerlin F, Lhoste F, **«** LFSS 2023 et 'Médicaments de Thérapie Innovante' : consécration du contrat de résultat ? » Rev Gen Dr Méd 2023 (PDP), 259-266.

Megerlin F, Pinilla E, Huriet Cl, « Règlement européen de 2021 sur l'évaluation des technologies de santé : place des données de 'vie réelle' ? » Rev Gen Dr Méd 2023 (PDP), 281-294.

Megerlin F, Roche Th, Huriet Cl, Faut-il sauver le droit de la recherche « impliquant » la personne humaine ? Rev Gen Dr Méd 2024 (PDP), à paraître.

Megerlin F, « La donnée de santé « électronique » et le droit européen : tautologie, pléonasme, levier ? », Rev Gen Dr Méd 2024 (PDP), à paraître.

Megerlin F, Lhoste F, « Droit européen et « qualité » des données de santé pour les utilisations secondaires. *Quid* des données synthétiques ? », Rev Gen Dr Méd 2024 (PDP), à paraître.

Mitchell C., Ordish J., Hall A., «Genomic Medicine and research: how does the GDPR apply ? », 2020, *phgfoundation.org*.

Moore S.M., D.R. Maffitt, K.E. Smith et al., « De-identification of Medical Images with Retention of Scientific Research Value ». *Radiographics*. 2015 May-Jun;35(3):727-35.

Moquet-Anger M.-L., « Professions et professionnels de santé », in Actes du Colloque de l'AFDS, n° spécial hors série Revue de droit sanitaire et social 2022, 99-108.

Morlet-Haïdara L, « Le système national des données de santé et le nouveau régime d'accès aux données », RDSS 2018, p. 91-106.

Morlet-Haïdara, « L'*empowerment* du patient et l'Espace Numérique de Santé « Mon espace santé », JDASM 2023 (n°36), pp 33-44.

Morley J, Cowls J, Taddeo M, Floridi L, « Public Health in the Information Age: Recognizing the Infosphere as a Social Determinant of Health ». J Med Internet Res. 2020 Aug 3;22(8):e19311.

Mosa AS, Yoo I, Sheets L., « A systematic review of healthcare applications for smartphones ». BMC Med Inform Decis Mak 2012;12:67.

Movshovitz-Attias Y., Kanade T., Sheikh Y, *Eu*r*ope*an *Confer*en*ce on Computer Vision,* 2016, 202–217.

Mullins C.D., Whicher D., Reese E.S. et Tunis S., « *Generating Evidence for Comparative Effectiveness Research Using More Pragmatic Randomized Controlled Trials: », PharmacoEconomics* 2010, vol. 28, nº 10, p. 969–976

Na L, Yang C, Lo C-C, Zhao F, Fukuoka Y, Aswani A., « Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning ». JAMA Netw Open 2018 ;1(8):e186040.

Nabat Y, « Données de santé : entre permissivité juridique, biopolitique et néolibéralisme », AOC, 2 mars 2021.

Naidoo, P., Bouharati, C., Rambiritch, V., Jose, N., Karamchand, S., Chilton, R., & Leisegang, R. « Real-world evidence and product Development : opportunities, challenges and risk mitigation ». *Wiener Klinische Wochenschrift*, 2021, *133*, 15-16.

National Cyber Security Centre britannique, Rapport « WannaCry ransomware outbreak » (https://www.ncsc.gov.uk/report/wannacry-ransomware-outbreak).

Nerbonne S., « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? » Legicom 2009, n°42, pp 37-46.

Netter E., « La portabilité, un droit à inventer ? », Dalloz IP/IT 2020, pp.352-357.

Nevejeans P., « Le corps souffrant et ses enjeux diplomatiques », *in* Bull. Centre de recherches du château de Versailles, 2016.

Nguyen B., Castellucia C, « Techniques d'anonymisation tabulaire : concepts et mise en œuvre », Bull. sté inform. Fr 20 avril 2020 ; n°5, pp 23-41.

Nicaud B, « Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE », Dalloz 2022.

Nik-Ahd F., De Hoedt A., Butler C. et al. « Prostate Cancer in Transgender Women in the Veterans Affairs Health System, 2000-2022 ». JAMA 2023 Jun 6;329(21):1877-1879.

Oxley T., Mocco J., Majidi S. et 13 autres co-auteurs, « Large-Vessel Stroke as a Presenting Feature of Covid-19 in the Young », *Engl N. J Med* 2020; 382:e60.

PatientsLikeMe secures $ 100M, partners with health data company (5 janvier 2017). MobiHealthNews. https://www.mobihealthnews.com/content/patientslikeme-secures-100m-partners-health-data-company-icarbonx

PatientsLikeMe, FDA explore how patient-generated data could help (23 août 2018). MobiHealthNews. https://www.mobihealthnews.com/content/patientslikeme-fda-explore-how-patient-generated-data-could-help-event-reporting

Pencina M, Goldstein B, D'Agostino R (2020 23 avril).) : « Prediction Models - Development, Evaluation, and Clinical Application », N Engl J Med. 2020 Apr 23;382(17):1583-1586.

Perrot J-C, « L'âge d'or de la statistique régionale (an IV-1804) », Annales historiques de la Révolution française, 224, 1976, p. 215-276.

Pezzali G, Espesson-Vergeat B, « Cyberattaque des objets connectés dans le secteur de la santé : quelle protection des fabricants et des utilisateurs ? », FIDAL, 20 nov. 2017.

Ping H, Le Pichon S, Reichmann T., Tingyang Z. *Transcultural dictionnary of Misunderstandings - European and Chinese Horizons*, Ed. Cent mille milliards, Paris, 2023.

Pinilla E, Megerlin F, « De la donnée de santé par qualification de la loi, à la donnée de santé « par destination », Rev. gén. dr. méd 2018 (PDP), 99-112.

Pinilla E, Bordas P, Megerlin F, « Le juge européen et les services dématérialisés des professions réglementées : quelle pharmacie à l'aube du Digital Market Act ? » Rev Gén Dr Méd 2021 (PDP), 175-185.

Pinilla E, Megerlin F, « La donnée de santé « synthétique » en droit européen : un objet virtuel non (encore) identifié », Rev. Gén. Dr. Méd. 2024 (PDP), à paraître.

Plaiasu M, Alexandru D, Nanu C, « Physicians' legal knowledge of informed consent and confidentiality. A cross-sectional study » ; BMC Med Ethics 2022 Sep 16;23(1):93.

Pon D. Coury A, « Accélérer le virage numérique », Rapport final de la stratégie de transformation (09/2018).

R. Porcher, « Grand ménage de printemps chez Doctolib », Rev. dr. santé janv. 2023 (111), 10-11.

Pouvourville (de) G., Armoiry X., Lavorel A., Bilbault P. et al., « Données et preuves en vie réelle dans l'évaluation des technologies de santé : dans quels cas sont-elles complémentaires, substitutives, ou les seules sources de données par rapport aux essais cliniques ? » Ther. 2023 Vol 78 (1), 66-80.

Py B, *Le secret professionnel,* L'Harmattan, 2005.

Quemener M, Ferry J, *Cybercriminalité : défi mondial et réponse*. Economica, 2007.

Quesard C, M et M. *Les guerres de l'information à l'ère numérique*. Presses Universitaires de France, 2021.

Rabesandratana T., « European data law is impeding studies on diabetes and Alzheimer's, researchers warn », *Science*, nov. 20, 2019.

Rabiolo A, Alladio F, Morales E, McNaught AI et al., « Forecasting the COVID-19 Epidemic by Integrating Symptom Search Behavior Into Predictive Models: Infoveillance Study » J Med Internet Res. 2021 Aug 11;23(8):e28876.

Rachidi I, « Europol met en garde contre la vente de faux certificats PCR négatifs », *Euractiv*. 2 févr. 2021.

Raghunathan TE, Synthetic data, Annual Review of Statistics and Its Application 2021;8, 129-140.

Rose RV, Kumar A, Kass JS, « Protecting Privacy: Health Insurance Portability and Accountability Act of 1996, Twenty-First Century Cures Act, and Social Media ». Neurol Clin. 2023 Aug;41(3):513-522.

Rozier M, Scroggins S, Loux T, Shacham E, « Personal Location as Health-Related Data: Public Knowledge, Public Concern, and Personal Action », Value Health 2023 May 24:S1098-3015(23)02614-1 ».

Sadare O., Melvin T., Harvey H. *et al.,* « Can Apple and Google continue as health app gatekeepers as well as distributors and developers? » *Nature Digit. Med.* 2023 6, 8.

Sampieri-Teissier N, Camman C., Livolsi L, « La supply chain santé est aussi une affaire d'Etat », Fevue française de gestion 2020/8, pp. 127-137.

Sanger D, Perlroth N, « Hospitals Wrestle With Unprecedented Cyber Assault », The New York Times 28 juin 2017, https://www.nytimes.com/2017/06/28/technology/ransomware-hospitals-wanna-cry-attack.html.

Sankar P ; Mora S., Mers J.F. Jones N.L. « Patient perspectives of medical confidentiality: a review of the literature », J Gen Intern Med 2003 Aug;18(8):659-69 ;

Santillana M, Zhang DW, Althouse BM, Ayers JW, « What can digital disease detection learn from (an external revision to) Google Flu Trends? » Am J Prev Med. 2014 Sep;47(3):341-7.

Sariyar M., Schlünder I., « Reconsidering Anonymization-Related Concepts and the Term "Identification" Against the Backdrop of the European Legal Framework », Biopreserv Biobank 2016 ; 14(5): 367–374.

Sauer F., « Les grandes étapes de l'Europe du médicament », Rev. d'histoire de la pharmacie 2014, LXII, n°381, 61-74.

Schillinger D, Baron RJ, « Health Communication Science in the Balance », *Jl Am Med Ass.* Publié en ligne le 31 juillet 2023 (doi:10.1001/jama.2023.14763).

Schmidt H., Gostin L.O., Williams M. A., « The Supreme Court's Rulings on Race Neutrality Threaten Progress in Medicine and Health » JAMA. 2023;330(11):1033-1034.

Schweikart SJ, « Should Immigration Status Information Be Considered Protected Health Information ? » AMA J Ethics. 2019 Jan 1;21(1):E32-37.

Seibert J.A., Perry J., Gichoya J.W., Kirby J. et al., « Report of the Medical Image De-Identification (MIDI) Task Group, Best Practices and Recommendations ». *ArXiv [Preprint],* avril 2023.

Shah N, « Thriving Apple Watch & Apple Health Ecosystem Advancing Digital Intelligent Healthcare », 21 juillet 2022, Blog, sur le site counterpoint, vérifié janv. 2023.

Sicard D, « Les perspectives de la médecine préventive et prédictive », RFAP 2005/1(n°113), pp 121-125.

Simon G.E., Shortreed S.M., Cloey R.Y. et al., « Assessing and Minimizing Re-identification Risk in Research Data Derived from Health Care », *EGMS* (Wash.DC) 2019 Mar 29;7(1):6.

Skoze-Pellet V.,*Les cyberattaques étatiques et la notion d'agression en droit international*, Mémoire de Master 2, U. Aix Marseille, Droit. 2018. dumas-02089316.

Smith A., Lambert P., Rutherford MJ, « Generating high-fidelity synthetic time-to-event datasets to improve data transparency and accessibility ». *BMC Med Res Methodol* 2022 ; 22, 176.

Roche Th, Lauria C. « Loi Jardé, le chantier continue encore et toujours : publication de deux nouveaux arrêtés » ; Blog sciences du vivant (2020), Delsol Avocats.

Sterling, B. (2008, 24 juin). The end of theory : the data deluge makes the scientific method obsolete. *WIRED*. https://www.wired.com/2008/06/the-end-of-theo/

Suarez-Lledo V, Alvarez-Galvez J. (2021), Prevalence of health misinformation on social media: systematic review. *J Med Internet Res.* 2021 Jan 20;23(1):e17187.

Sullivan. J. *Privacy matters*. « European commission adopts new adequacy decision for EU-US data flows Privacy Matters » 2023, 15 septembre. https://blogs.dlapiper.com/privacymatters/european-commission-adopts-new-adequacy-decision-for-eu-us-data-flows/

Sutner S, « Cyberattack on Medical Devices Shows Healthcare Industry's Vulnerability », TechTarget 11 juillet 2017, https://searchhealthit.techtarget.com/news/450422835/Cyberattack-on-medical-devices-shows-healthcare-industrys-vulnerability.

Taillat S., « Un mode de guerre hybride dissymétrique ? Le cyberespace », éditions Institut de Stratégie Comparée, 2016 (n°111), p. 89-106.

Tanner, A. E. « For sale : your medical records ». *Scientific American*, 2016 *314*(2), 26-27. https://doi.org/10.1038/scientificamerican0216-26

Teller M, « La régulation des données de santé : entre intérêt général et intérêts particuliers », introduction au cahier spécial, RIDE 2022/3 (t 26), p5.

Terrier M, « De faux *pass* sanitaires créés via une faille de sécurité en Europe », Huffpost, 29 oct. 2021.

The SAMD regulatory landscape in the US and Europe. (s. d.). RAPS, 2021. https://www.raps.org/news-and-articles/news-articles/2021/8/the-samd-regulatory-landscape-in-the-us-and-eu-1

Thelisson E., « la portée du caractère extraterritorial du règlement général sur la protection des données », Rev. int. dr. éco. 2019/4 t 26, 501-533.

Theodos K, Sittig S. « Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply ». Perspect Health Inf Manag. 2020 Dec 7;18(Winter):1l.

Tirard S (*dir*), Dossier « Données médicales », Rev. Histoire, médecine et santé, Hiver 2022 (11).

Trister A., « The Tipping Point for Deep Learning in Oncology » JAMA Oncol. 2019;5(10):1429-1430.

Troia V, *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*. Sybex Inc., 2020.

Tucker A., Wang Z., Rotalinti Y. *et al.* « Generating high-fidelity synthetic patient data for assessing machine learning healthcare software ». *npj Digit. Med.* 2020, 147.

Wan C., Jones D.T, « Protein function prediction is improved by creating synthetic feature samples with generative adversarial networks. *Nat Mach Intell* 2020, **2**, 540–550.

Wang Y, McKee M, Torbica A, Stuckler D, « Systematic Literature Review on the Spread of Health-related Misinformation on Social Media », Soc Sci Med. 2019 Nov;240:112552.

Wang Z, Yin Z, Argyris Y.A, « Detecting Medical Misinformation on Social Media Using Multimodal Deep Learning », IEEE J Biomed Health Inform. 2021 Jun;25(6):2193-2203.

Wellington K., « Cyberattacks on medical devices and hospital networks : legal gaps and regulatory solutions ». *Santa Clara High tech*. 2013 vol 30.

Wessel L. « Scientists concerned over US plans to collect DNA data from immigrants », *Nature*, News 7 oct. 2019.

Wilson CS, « Dissenting Statement of Commissioner Christine S. Wilson Policy Statement on Breaches by Health Apps and Other Connected Devices », Matter n° P205405, 15 sept. 2021.

Wyrd C., Gruson D., « Renseignement et santé », Rev. déf. nat. 2021/7 (n°842), pp 83-89.

Xia W., Liu Y., Wan Z., Vorobeychic Y. et al. « Enabling realistic health data re-identification risk assessment through adversarial modeling », *J Am Med Inform Assoc*. 2021, Mar 18.

Yaloz, C. R. « Conformité au RGPD : obligation de moyen ou de résultat ». *Euro Legal Counsel Group* (2019) https://elc-paris.com/conformite-au-rgpd-obligation-de-moyen-ou-de-resultat/

Yasini M, Marchand G. « Toward a use case-based classification of mobile health applications ». Stud Health Technol Inform 2015; 210:175-9.

Yetisen AK, Martinez-Hurtado JL, da Cruz Vasconcellos F, Simsekler MC, Akram MS, Lowe CR, « The regulation of mobile medical applications ». Lab Chip 2014;14(5):8 33- 40.

Yeung A, Tosevska A, Klager E, Eibensteiner F *et al.*, « Medical and Health-Related Misinformation on Social Media: Bibliometric Study of the Scientific Literature ». J Med Internet Res. 2022 Jan 25;24(1):e28152.

ZDNet, « NotPetya ransomware attack: What is it, how it started, who is responsible and more » (2017), https://www.zdnet.com/article/notpetya-ransomware-outbreak-chaos-reigns-supreme-in-ukraine/.

Zhang Z., Yan C., Malin B., « Membership inference attacks against synthetic health data » Jl Biomed. Inform. 2022, 103977.

Université de Strasbourg

Erwan PINILLA

Données de santé, dynamiques et enjeux de souveraineté

Résumé

Cette recherche a pour but de relever les dynamiques de la « donnée de santé » dans le champ de la souveraineté numérique : qui peut par là décrire, expliquer des situations, prédire des tendances, induire des comportements individuels et/ou populationnels, voire étatiques ? Que protéger donc en droit, comment ? Nous rapportons et analysons le débordement des approches historiques de régulation, du fait de la diversification des acteurs, techniques et usages ; de la multiplication des sources de données et leur dissémination ; de l'ébranlement de catégories juridiques pourtant récemment fixées ; de la porosité des systèmes du fait d'interactions choisies ou non, dont les ingérences étrangères. En conséquence, nous analysons l'avènement accéléré d'outils inédits au niveau européen, dans des champs traditionnellement régaliens en matière d'infrastructures cyber, de qualifications (données, technologies, utilisations), et de garanties mutuelles contre les ingérences étatiques. D'autres défis nous semblent devoir être approfondis (ainsi la ré-identification ; les données synthétiques), dans une ère où la maîtrise technologique a cessé d'être l'apanage des Etats, et où la géopolitique s'est retendue avec des outils nouveaux.

Données de santé – Souveraineté – Numérique – Droit – Ingérence – Cyber – France – Union Européenne

Abstract

Aim of this research is to identify the dynamics of "health data" in the field of digital sovereignty: who can use it to describe and explain situations, predict trends, and induce individual and/or population, or even States, behaviours ? What is – and should be legally protected, and how ? We here report on and analyze the overflowing of historical approaches to regulation, due to the diversification of players, techniques and uses ; the multiplication of data sources and their dissemination, the shaking of legal categories despite their recent establishment ; the porosity of national and joint systems, due to conventional or agressive interactions. As a result, we analyze the accelerated advent of new rules at European level in traditionally regalian fields of cyber infrastructure, qualifications (data, technologies, uses), and mutual guarantees against interferences. Other challenges call for in-depth insight (such as reidentification & synthetic data), in an era where for long technological domination is no more a prerogative of States, and where geopolitics has been extended by new tools and practices.

Health data – Sovereignty – Digital – Law – Interference – Cyber – France – European Union

Ecole doctorale des sciences juridiques | ED 101
Université de Strasbourg